CYBERWARFARE POLIHEURISTIC APPROACH OF NATION-STATE EXPANSION

Horatiu MOGA[*], Cristian ISTRATE[**]

[*]CNIF-MFP, Braşov, Romania (horatiu.moga@gmail.com)
[**]National Defense University "Carol I" (Bucharest, Romania
(cristian.i.istrate@gmail.com)

DOI: 10.19062/1842-9238.2019.17.2.5

Abstract: *The article aims to provide a way of researching the mechanisms of nation state expansion by using economic means and cyberwarfare. The justification for such a study is dictated by the international dynamics of rewriting the various international agreements between states and their reordering by using means of a hybrid nature that include economic tools, cyberwarfare, mass communication and of course, military techniques. To study these mechanisms of expansion when it comes to the already established superpowers as well as the ascending powers, we rely on the theory of hegemonic war proposed by Robert Gilpin and the foreign policy paradigm issued by Alex Mintz. The specific matrix of decision-making mechanisms will be built on ~~in~~ the evaluation of share rates ~~to~~ via a qualitative-quantitative hybrid approach meant to bring additional value to the market of security studies on ~~of~~ cyberwarfare, which currently encompasses purely rationalist research only. The present approach is not intended as an exhaustive outlook, but rather as a first step towards a larger study, as its purpose is to introduce new and revolutionary ideas in the cyberwarfare research of international relations.*

Keywords: *decision matrix, foreign policy management style, decision rules*

1. INTRODUCTION

The research aims to present a model of the expansion of a nation-state based on the hegemonic theory of Robert Gilpin [1] but adapted to the poliheuristic analysis of cyberwarfare [2]. The theory of hegemonic war by ~~of~~ Robert Gilpin is part of the family of theories of offensive realism and deals with internal and external modalities that make possible the expansion or over-expansion of a state actor depending on economic costs and good governance / internal corruption [1]. In order to develop Gilpin's idea, he considers that the expansion and over-expansion of a state (that is, the economically unsustainable expansion leading to its failure) are determined by three internal economic costs (cost for national security; cost for private and nonmilitary public; cost for productive investment) and the level of corruption or good internal governance. These elements are tight in what we called the "Gilpin Test". All these elements are in agreement with the poliheuristic paradigm that will study the part of cyberwarfare that considers that the foreign policy is dependent on the internal state of the state actor [2] and therefore also on the four variables mentioned above. The research aims to explain cyberwarfare not as a singular element in the arena of international relations but as an intrinsic element of the process of military, economic, cultural, etc. expansion of a state actor.

In the specialized literature, attempts are made to define the new field of human cyber-existence. There are researches that define a new modality of virtual political system [3], trying to adapt the classical paradigms or to propose new paradigms of approach [3]. Most of these studies call for the rational choice paradigm, which has a multitude of limitations in all areas and therefore in cyberwarfare. That is why this study proposes an alternative of bounded rationality based on the poliheuristic paradigm [2]. The limits of the rational paradigms that currently dominate cyberwarfare research are largely explained in a myriad of research [4] that take into account the computer engineering side but neglect the part of prejudice that governs human decision most of the time. That is why the poliheuristic paradigm comes to fill this void.

This research aims to present a way of researching the expansion of a state actor that uses, besides the classical means and cyberwarfare approaches, taking into account also the prejudice system that governs the executive power of a state and which gives it the necessary confidence in the expansionist actions of the policy. external. The article makes an introduction to the poliheuristic paradigm and its elements in the methodology section and in the results section it makes some recommendations that can help the reader to carry out a practical analysis of an expansion of a nation-state based on cyberwarfare. The research will present the way in which using qualitative-quantitative hybrid methods for predicting statistical indicators [5] and the logical relationships between them, the specific decision rates are determined regularly from the decision-making matrix.

2. METHOD

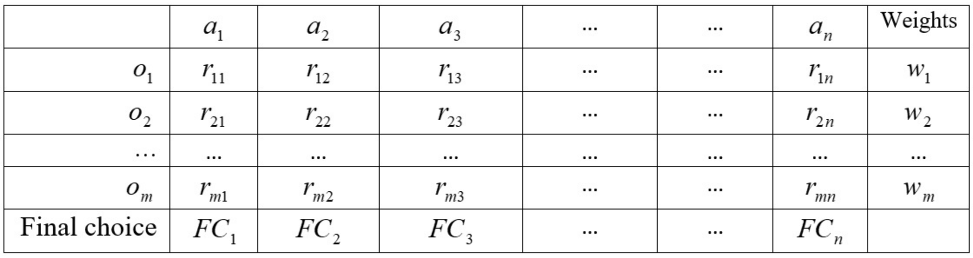
The article makes in the methodology part a presentation of the poliheuristic paradigm together with the elements that characterize it. The reason for which the poliheuristic paradigm was chosen is the widespread idea among researchers in international relations and the analysis of foreign policy that the internal state of the state actor actually determines its behavior and the result of foreign policy [2] and not just the international political system.

Poliheuristic Approach – the poliheuristic paradigm is part of the family of models of foreign policy analysis initiated by the work of Graham Allison, "The Essence of Decision" [6]. This approach was proposed by Israeli political scientist Alex Mintz as a synthesis approach between schools of cognitive psychology and paradigms of rational choice [...], considering that the decision is based on "cognitive short-cuts heuristics." The approach is called poliheuristics because it considers that any decision is a synthesis between several "cognitive short-cuts heuristics". Other defining characteristics of this paradigm are the two-stage decision and the non-compensatory principle of choice between several options. The decision in the first stage is based on bias (ie "heuristics cognitive short-cuts"), and in the second stage on rational approaches. Thus, the decision process through the prejudices of the first stage eliminates a spectrum of opinions that the decision maker would could be considered in the case of a rational approach. That is why the decision-making approach is bounded rationality. The decision analysis tool is the decision-making matrix, based on the principle of the non-compensatory decision. *This principle considers it important for each decision maker to establish a hierarchy of the objective-result dimensions of this matrix, which simplifies the decision-making process* [2]. The most important of the dimensions of the decision matrix is the internal state system, which contains the supreme constraint [2]. The first stage in eliminating unacceptable dimensions, and in the second stage in establishing the decision rules. The research calls on data collected by Council on Foreign Relations in the bank entitled Cyber Operations Tracker which contains sources about motivated or accidental attacks, on which elements of the actor took place respectively his reaction but also to other sources mentioned in the results section.

Cyber Operations Tracker contains data on cyberwarfare incidents from 2005 to date and allows the results section to explain how to calculate the rates in the poliheuristic decision matrix based on statistical indicators such as the intensity of a particular type of cyber attack the economic costs of the "Gilpin Test" of the expansion of a state actor and its indicator of good governance. Regarding the problem of the rates in the decision matrix that explains the hierarchy of actions taken by a state actor in the enlargement process, a variety of evaluation modalities are presented in the specialized literature. The originality of this article is the use of qualitative-quantitative predictive hybrid methods.

The first element is to establish the model of management in foreign policy – in this first stage, the foreign policy management model is identified, focused on one person, group or several decision groups [7]. The next step in the first step of the decision is to establish the model (s) of "cognitive short-cuts heuristics" bias that according to Mintz fall into the following forms [2]: B01. "Focusing on short-term benefits rather than longer-term problems"; B02. "Preference over preference"; B03. "Locking on one alternative"; B04. "Wishful thinking"; B05. "Post-hoc rationalization"; B06. "Relying on the past"; B07. "Focusing on a narrow range of policy options rather than on a wide range of options"; B08. "Groupthink" B09. "Overconfidence; over-estimating one's capabilities and underestimating one's capabilities"; B10. "Ignoring critical information; denial and avoidance"; B11. "Focusing on only part of the decision problem"; B12. "Turf battles leading to suboptimal decisions"; B13. "Lack of tracking and auditing of prior decisions and plans"; B14. "Polyheuristic bias"; B15. "Shooting from the hip"; B16. "Polythink" B17. "Group polarization effect". The second stage of the first step of the two-stage decision process will focus on establishing the critical objective-outcome dimensions of the decision matrix and rejecting the dimensions that offer unacceptable results. Establishing the hierarchy of critical dimensions will be made based on the principle of noncompensatory decision and B01-B17 bias. A decision matrix has a table appearance in which the lines represent the critical dimensions of the objectives respectively of the results $o_1, \ldots, o_m$ followed by the decisive actor and the columns are the actions carried out by him $a_1,...,a_m$ $a_1, \ldots, a_n$ (see Table 1). According to the principle of non-compensating decision from the analysis of the facts of the state actor there is a hierarchy of critical objectives $o_1,...,o_m$ $o_1, \ldots, o_m$ for an action a_i date of the rates values $r_{1i},...,r_{mi}$, practically, there are no two goals with the same importance.

Table 1. Poliheuristic decision matrix to a state decision-maker.



	a_1	a_2	a_3	...	...	a_n	Weights
o_1	r_{11}	r_{12}	r_{13}	...	...	r_{1n}	w_1
o_2	r_{21}	r_{22}	r_{23}	...	...	r_{2n}	w_2
…	...	...	...	...	...	...	...
o_m	r_{m1}	r_{m2}	r_{m3}	...	...	r_{mn}	w_m
Final choice	FC_1	FC_2	FC_3	...	...	FC_n	

Actions / Alternatives - represents the behavior of foreign policy of the state actor that can have a wide spectrum from military, economic, cyberwarfare, radio-electronic or cooperation actions.

Dimensions - after the elements of the first step of the foreign policy process have been established, it is necessary to establish the critical dimensions of the decision matrix.

These may be elements of foreign policy that have a smaller significance than those of internal politics such as the size of the cyber power index [8] or the five-ring model [9] or other models proposed by other authors [2].

Of course, at least one of the dimensions must be linked to the internal political system as considered by Mintz. *Implications* - are explanations specific to each critical dimension produced by a certain action of the poliheuristic decision matrix. *Ratings* - are numerical values assigned to each critical dimension depending on its specific involvement in a particular action. Rate values can range from -10 (very bad) to +10 (very good), critical dimensions have values between 0 and +10. *Weights* - follow the non-compensatory decision principle and the foreign policy management criterion and explain the hierarchy of critical objectives pursued by a political actor. They have values between 0 and +10.

Example: For this study we use the Council on Foreign Relations Cyber Operations Tracker database [10]. It monitors cyber-attacks activities from around the world from 2005 to the day on four dimensions of each state or non-state actor: Civil society, Government, Military, Private sector (economic). Of course, for non-state actors they do not cover all four dimensions. In this study we will consider all four critical dimensions. Cyber actions developed by a state or non-state actor are the following [10]: 1. Distributed Denial of Service - flooding a server with data packets from its clients, so that it can no longer work; 2. Espionage - the ability of an actor to extract useful information from a computer without the owner's approval; 3. Defacement - changing the content of a web content or account from a computer without the consent of its owner; 4. Data Destruction - the ability to use malware to make a malfunctioning computer or destroy the data it contains; 5. Sabotage - the ability to use malware to remove a system from a critical infrastructure controlled by that computer; 6. Doxing - the activity of identifying on the Internet information about a particular individual or collective actor and making it public with evil intentions against it.

Table 2. Example of poliheuristic decision matrix to a state decision-maker based on Cyber Operations Tracker of Council on Foreign Relations

	DDOS	Espionage	Defacement	Data Destruction	Sabotage	Doxing	Weights
Civil society	r_{11}	r_{12}	r_{13}	r_{14}	r_{15}	r_{16}	w_1
Government	r_{21}	r_{22}	r_{23}	r_{24}	r_{25}	r_{26}	w_2
Military	r_{31}	r_{32}	r_{33}	r_{34}	r_{35}	r_{36}	w_3
Private sector	r_{41}	r_{42}	r_{43}	r_{44}	r_{45}	r_{46}	w_4
Final choice	FC_1	FC_2	FC_3	FC_4	FC_5	FC_6	

Determining the decision rules – after establishing the positive and negative rates from the first stage and excluding the non-critical dimensions (those with negative rates), we will move to the second stage in which, based on the rational choice paradigm, the decision rules of the actor will be established. In the following we will present some decision rules [2] that can be based on a decision based on the principle of the non-compensatory decision and the hierarchy of the objective-result critical dimensions. Of these, the most important is as we have outlined above the internal political system.

For the calculation of average weights, the formula below is used:

$$\overline{w_j} = \frac{1}{n} \cdot \sum_{i=1}^{n} r_{ij} \qquad (1)$$

After we have established the hierarchy of objectives for each dimension according to biases B01-B17, from the most important to the least important, we will associate the values of the average weights from the highest in value to the lowest in value (to be consistent with the hierarchical order of the objectives resulting from B01-B17 biases and *cognitive consistency, cognitive inconsistency, cognitive dissonance of the state actor* [2]). Then with the help of the relation (2) we establish the relevant rates for the hierarchical system of objectives of the state decision maker.

$$\max(r_{ik}, w_i) = \begin{cases} r_{ik}, r_{ik} \geq w_i \\ 0 \end{cases} \tag{2}$$

For the calculation of the final choice option of each action we define by the relation (3) the option as below in which only the rates that exceed the weight of the objectives are summed and prove that the respective action is viable to reach the proposed objectives.

$$FC_k(r_{1k}, r_{2k}, ..., r_{mk}, w_1, w_2, ..., w_m) = \sum_{i=1}^{m} \max(r_{ik}, w_i) \tag{3}$$

The methods of calculating the rates will be discussed in the results section. As limitations, this research does not take into account the evaluation of the external conditions for limiting the expansion of the state actor defined by Gilpin: increasing costs of political dominance, loss of economic and technological leadership [1].

3. RESULTS

In the specialized literature, the purely rationalist approach is widespread. By this approach we consider a step forward in the process of knowledge of cyberwarfare which proposes an alternative approach that wants to bring the process of analysis closer to the reality of the research object. In order to deepen research in calculating the rates of the specific poliheuristic decision matrix, **the first element is to establish the management model in foreign policy**, we call on the qualitative and quantitative hybrid study methodology of the international events proposed by Sokolowski and Banks [5] which takes place in three stages: 1. A historical research of the study event; 2. Investigation of the event through statistical indicators; 3. Defining a quantitative predictive system for modeling statistical indicators and predicting the evolution of the event. Validate approaches through qualitative and quantitative comparisons that describe the event being investigated. As we stated in the introduction to this article, the phenomenon of cyberwarfare is not a singular one but we consider it an intrinsic one of the expansion of military, economic, cultural, etc. nature of a state actor. That is why in this research we approach the flexible or massive expansion model exhibited by authors such as Robert Gilpin [1], Jack Snyder [11], Paul Kennedy [12]. That is why we use the "Gilpin Test" in the research of the decision of flexible or massive expansion / over-expansion of a state actor. Gilpin explains this phenomenon through five internal conditions defined according to: cost for national security c_{CNS}; cost for private and nonmilitary public c_{CPNP}; cost for productive investment c_{CPI} and the level of corruption or good internal governance. The five conditions are the following [13]:

GT1. The gross domestic product suffers from a great decrease

$$\frac{\Delta c_{GDP}}{\Delta t} \downarrow < 0 \tag{4}$$

GT2. Military expenditures rise too sharply compared to the other two costs

$$\frac{\Delta c_{CNS}}{\Delta t} >> \frac{\Delta c_{GDP}}{\Delta t} \ AND \ \frac{\Delta c_{CNS}}{\Delta t} >> \frac{\Delta c_{CPNP}}{\Delta t} \ AND \ \frac{\Delta c_{CNS}}{\Delta t} >> \frac{\Delta c_{CPI}}{\Delta t} \tag{5}$$

GT3. Gross domestic product has a lower growth than non-military public and private expenditures

$$\frac{\Delta c_{CPNP}}{\Delta t} >> \frac{\Delta c_{GDP}}{\Delta t}; \tag{6}$$

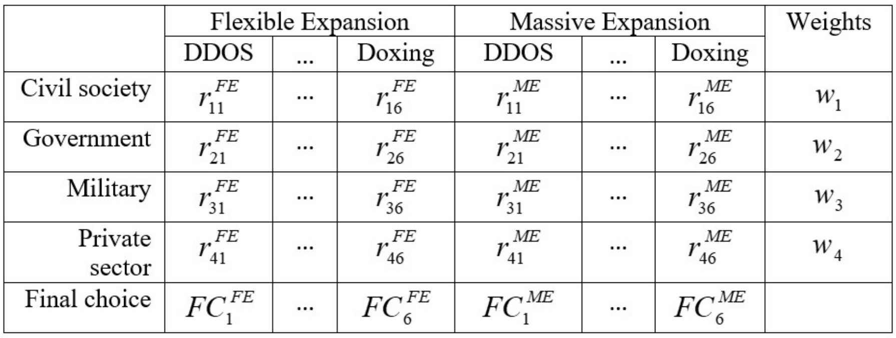
GT4. Innovative investments being lower than the other two military and non-military costs, the structural change of the type of economy cannot be achieved because

$$c_{CPI} < c_{CPNP} \text{ AND } c_{CPI} < c_{CNS} \tag{7}$$

GT5. High degree of corruption depending on the global indicator of good governance or the perception of corruption.

For the study of the compound phenomenon of expansions of a nation-state composed of cyberwarfare, we propose a polyurethane matrix below in which the two types of flexible expansions (which do not satisfy the Gilpin test) and the massive ones (which satisfy the Gilpin test) are paired with the six types of cyberwarfare strategies proposed by the Cyber Operations Tracker of Council on Foreign Relations. The critical dimensions remain the same as in Table 2. (FE = Flexible Expansion, ME = Massive Expansion).

Table 3. Cyberwarfare poliheuristic approach of nation-state expansion based on “Gilpin Test”



	Flexible Expansion			Massive Expansion			Weights
	DDOS	...	Doxing	DDOS	...	Doxing	
Civil society	r_{11}^{FE}	...	r_{16}^{FE}	r_{11}^{ME}	...	r_{16}^{ME}	w_1
Government	r_{21}^{FE}	...	r_{26}^{FE}	r_{21}^{ME}	...	r_{26}^{ME}	w_2
Military	r_{31}^{FE}	...	r_{36}^{FE}	r_{31}^{ME}	...	r_{36}^{ME}	w_3
Private sector	r_{41}^{FE}	...	r_{46}^{FE}	r_{41}^{ME}	...	r_{46}^{ME}	w_4
Final choice	FC_1^{FE}	...	FC_6^{FE}	FC_1^{ME}	...	FC_6^{ME}	

The poliheuristic decision matrix is shown in Tabel 3 above. After identifying the B01-B17 biases, the dimensions of the decision matrix, the actions we carry out a historical analysis of the expansion event combined with cyberwarfare and we identify as statistical indicators mentioned above: investments in economic innovation for the private sector dimension, military expenses for the military dimension, non-military public and private expenditures for the civil society dimension, the indicator of good governance for the government dimension, and the GDP for establishing the type of flexible or massive expansion if the conditions of GT1-G5 are verified. In the second stage of the decision to establish the decision rules, before applying the relations (1), (2) and (3) we calculate using a qualitative-quantitative type predictive approach of the post-event statistical indicators, knowing them. those pre-event through time series, neural networks, or other learning machines. The indicators used are: indicator of good governance from the World Bank [14], military expenses / non-military public and private expenses / investments in economic innovation / GDP from the CROSS-NATIONAL TIME-SERIES DATA ARCHIVE data bank [15]; cyber indicator of the number of attacks of the Cyber Operations Tracker of Council on Foreign Relations […].

$$r_{ij}^{cyber}(\Delta N) = k, k \cdot \frac{N_{Max} - N_{Min}}{10} \le \Delta N \le (k+1) \cdot \frac{N_{Max} - N_{Min}}{10}, k = \overline{1{,}9} \tag{8}$$

$$r_{ij}^{non-cyber}(\Delta c) = K, K \cdot \frac{c_{Max} - c_{Min}}{10} \le \Delta c \le (K+1) \cdot \frac{c_{Max} - c_{Min}}{10}, K = \overline{1{,}9} \tag{9}$$

$$r_{ij}^{X} = \begin{cases} r_{ij}^{cyber} \\ r_{ij}^{cyber} \cdot \alpha_{ij} + r_{ij}^{non-cyber} \cdot (1 - \alpha_{ij}), \alpha_{ij} \in (0{,}1); X = \overline{FE, ME}\text{,} \\ r_{ij}^{non-cyber} \end{cases} \tag{10}$$

Where r_{ij}^{X} is the final rate in the decision matrix used in relations (1) - (3); r_{ij}^{cyber} is a rate assessed based on quantitative predictions of cyber attacks from the Cyber Operations Tracker of Council on Foreign Relations database; and $r_{ij}^{non-cyber}$ is the rate resulting from the quantitative prediction of any type of economic cost or indicator of good governance; parameter α_{ij} further noted α for simplicity is a subunit and positive percentage parameter and is considered to be known in advance and can be analyzed based on previous case studies using the hybrid methodology proposed by Sokolowski and Banks by analyzing historical events.

Thus he decides whether for a particular type of cyber attack in a type of mass or flexible expansion, cyber operations or economic mechanisms or good governance were more important. The rates of the decision-making poliheuristic matrix are defined by the relations (8) - (10) above, and the rate variant is decided from the analysis of past facts that are the basis for the prediction of future actions. If the decision was purely economic or cyber, one opts for the rate that results only from the economic cost specific to the size of Civil society, Military, Private sector. For the Government dimension we use the indicator of good governance and for the cyber rate the number of attacks on a certain dimension. If one takes the analysis of the facts both the cost / governance and cyber parameters, the parameter α is used which is also used in the prediction, considering it a constant. *Thus, after establishing the rates, the second step is determined* **determining the decision rules** *and applying the relations (1) - (3) to establish the hierarchy of the final decisions of the actions of the state actor.*

This research brings as novelty the involvement of international statistical parameters in the calculation of decision rates as a possibility to evaluate the cognitive consistency [...] of the decision maker in foreign policy actions using the hybrid evaluation method of international events proposed by Sokolowski and Banks. This is a novelty besides the models of decision rules proposed by Mintz of conjunctive, disjunctive or elimination type by aspect [2].

The results presented based on the use of World Bank statistical indicators, CROSS-NATIONAL TIME-SERIES DATA ARCHIVE, Cyber Operations Tracker of Council on Foreign Relations and relations (1) - (3) and (8) - (10) present a flexible approach which is extendable to other areas of foreign policy research and security studies and management operations in general. Compared to other approaches to the analysis of foreign policy, which involve establishing decision rates only based on the analysis of historical facts [5], which can mix the analysis of the biases of the political actors with the researcher's biases, the approach proposed by us by calling on statistical indicators and operationalizing their objectives by indicators, these disruptive factors are largely removed. By the approach proposed in this research in the analysis of a certain action, one can establish the ratios that were the basis of the decision of an actor by establishing a percentage for the variable α which explains the importance that the decision maker gave to a certain objective in the hierarchy of objectives and the importance of prejudice from the list B01-B17 that were the basis of that option. The poliheuristic analysis used to analyze the foreign policy decision that accompanies the expansion policy of a nation state using cyber means goes beyond the purely rationalist approach which dominates the specialized analysis for the most part today, presenting a revolutionary approach through the appeal of the decision in two stages, to the list of biases B01-B17 proposed by Mintz and the decision-making matrix as alternatives to options based purely on game theory. According to the hybrid approach of the events proposed by Sokolowski and Banks and applicable in the evaluation of the rates, we obtain a high percentage of their evaluation in the most objective construction of the decision of a state political actor based on international statistical indicators. As we exemplify above, the approach presented in this research has the greatest flexibility and applicability in areas such as international relations and foreign policy, economic policies, security studies, management operations in general, etc.

CONCLUSIONS

In the researches that dominate the study of international relations of the dominant cyberwarfare are the rationalist theses, which try to highlight only focus on the end-result but neglect the internal constraints of the state actor but also his prejudices that can affect a rational decision and as a result can affects a good quality analysis.

That is why the logical step was to call for an approach such as foreign policy analysis, in our case the poliheuristic paradigm [2], to overcome these impediments. Thus, we appealed to the poliheuristic paradigm for the deep study that it offers to the decision maker's prejudices and the two-stage approach that allows the introduction of quantitative type calculations in the second stage of the study. Thus, our research has taken a step forward by integrating the qualitative-quantitative hybrid approach proposed by Sokolowski and Banks in evaluating the rates underlying the hierarchy of final decision rules.

Our research has presented how biases can influence the decision by reordering according to the hierarchy of the objectives that it has and the model to influence the order of the final decision rules specific to the second stage of decision. Thus, through the proposed approach, the researcher can get closer to the cognitive mechanisms underlying the decision and the cognitive inconsistency or inconsistency that Mintz speaks of [2]. As important contributions we can name the implication of a qualitative-quantitative hybrid approach for evaluating the rates of a decision matrix by using common factual-historical analysis in establishing the hierarchy of biases and quantitative predictive models such as time series and complementary analysis mechanisms. The novelty of this article in the field of cyberwarfare security studies is represented by the internal constraint that the state system can bring to achieving the foreign policy objectives and limiting the decision-makers' vision due to their own biases. The applications can be counted besides the classic ones in the studies of security and the foreign policy can be extended to the researches in variants domains of the management or of the different economic and social policies. About the limits of the research the most important is probably the interference between the historical approach from the beginning of the qualitative-quantitative hybrid analysis and the operationalization of the concepts by the researcher. Something that has to be treated very carefully and checked several times. As a future activity we intend to improve the limitation mechanism mentioned above and the possibility of an objective approach of the α parameters in the decision rules.

REFERENCES

[1] Robert Gilpin, *War and Change in World Politics*, Cambridge University Press; 1983;

[2]Alex Mintz and Karl DeRouen Jr, *Understanding Foreign Policy Decision Making*, Cambridge University Press, 2010;

[3] Craig B. Greathouse, *Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?*, in Cyberspace and International Relations Theory, Prospects and Challenges, Jan-Frederik Kremer and Benedikt Müller (Eds.), Springer; 2014;

[4] Lina Eriksson, *Rational Choice Theory: Potential and Limits*, Palgrave Publisher, 2011;

[5] John A. Sokolowski and Catherine M. Banks, *Modeling and Simulation for Analyzing Global Events,* Wiley Publisher 2009;

[6] Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis*, Pearson Publisher; 2 edition, 1999;

[7] Margaret G. Hermann: *Assessing Leadership Style: a Trait Analysis*, 1999, Available at https://socialscience.net/docs/LTA.pdf;

[8] Horațiu Moga, Andrei Luchian, Razvan Boboc, Poliheurisitc Approach of Cyberwarfare Based on Cyber Power Index, *AFASES 2019*, pp. 28-38;

[9] John A. Warden III: *The Enemy as a System*, http://www.ciar.org/ttk/mbt/ strategy.Warden.enemy-as-a-system.html;

[10] *** Cyber Operations Tracker Council on Foreign Relations, https://www.cfr.org/interactive/cyber-operations;

[11] Jack Snyder, *Myths of Empire: Domestic Politics and International Ambition*, Cornell University Press, 2013;

[12] Paul Kennedy, *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000,* Publisher: Vintage, 1989;

[13] Horatiu Moga, Mircea Boscoianu, Delia A. Ungureanu, Florin D. Sandu, and Razvan Boboc, Refined Concepts of Massive and Flexible Cyber Attacks with Information Warfare Strategies, *Journal of Communications Vol. 12, No. 6, June 2017,* pp. 364-370;

[14] *** World Bank, https://info.worldbank.org/governance/wgi/;

[15] *** CROSS-NATIONAL TIME-SERIES DATA ARCHIVE, https://www.cntsdata.com/.