Bulletin of the *Transilvania* University of Braşov – Special Issue
Series VII: Social Sciences • Law • Vol. 11 (60) No. 1 - 2018

POLIHEURISTIC APPROACH OF HYBRID WARFARE ACTIONS BASED ON INFORMATION WARFARE CANONIC STRATEGIES

H. MOGA[1] A.M. BOLBORICI[2] E.V. CONSTANTINESCU[3]

Abstract: *This research aims to provide a poliheuristic approach of the decisions that form the foundation of hybrid war acts which have a strong component of informational war. Through hybrid war we understand an interstate conflict modality in which the aggressor state denies involvement and uses military engagement means specific to low-intensity or non-military means. This research insists on the involvement of the means of informational warfare within hybrid military means of both military and non-military nature. The purpose of this research is to evaluate the impact of informational war means, which are considered intrinsic to hybrid war means on the various areas of society targeted by the hybrid war. The instrument with which the evaluation is carried out is the poliheuristic decision matrix.*

Key words: *poliheuristic approach, hybrid war, decision matrix, interstate conflict.*

1. Introduction

This research aims to treat the concept of hybrid warfare with the help of the informational warfare strategies. It also aims to assess the consequences of the hybrid warfare on the national cyber infrastructure. The theoretical device of this phenomenon is a poliheuristic paradigm. In this article the hybrid warfare unfolds between two states – one is the aggressor state called Challenger respectively the aggrieved state identified by the term Defender. Following the introductory section, we will define the important concepts of this research.

[1] Transilvania University of Braşov, Centre "Advanced Research on Mechatronics", horatiu.moga@gmail.com
[2] Transilvania University of Braşov, ana.bolborici@unitbv.ro
[3] Transilvania University of Braşov, Centre "Advanced Research on Mechatronics", e.valentinaconstantinescu@yahoo.com

The poliheuristic paradigm was created by Israeli researcher Alex Mintz as a way of unifying cognitive-type approaches with rationalist approaches (Mintz, 2010). Regarding the poliheuristic paradigm, the deciding actor passes a *two-stage process in making decisions*:

a. The decision-maker simplifies the complex information he receives on the basis of cognitive shortcuts, his experiences, various historical analogies known to him, long-term (mood) or short-term (emotion), focusing on the critical dimensions of the decision, and rejecting the irrelevant (Mintz, 2002, pp.1-11).
b. In the second stage, the decision-maker will focus only on the critical dimensions of the consequences and will rationally evaluate his alternatives only by aiming at maximizing gains, minimizing risks and costs (Mintz, 2002, pp.1-11) using the rational choice paradigm.

In this research, we will treat the hybrid warfare in the perspective of András Rácz (Rácz, 2015, pp.57-82), describing it as a three-phased warfare: preparatory phase, attack phase, stabilization phase; the hybrid warfare must abide to the following conditions:

a. Military superiority of Challenger state;
b. Weak central power and security of Defender state;
c. Lasting, regionally-concentrated dissatisfaction with the central government of Defender state;
d. Presence of Challenger state speaking minority as source of legitimacy claim Challenger state actions;
e. Strong media presence of Challenger state both in the Defender state and abroad;
f. Strong Logistics of Challenger state actions;

The tool by which the Challenger implements the three phases defined by András Rácz is *information warfare* and its target is the Defender's national cybernetic infrastructure. By the concept of national cybernetic infrastructure we understand the set of servers and clients along with the information transfer between them (cables, optic fibers, radio antennas) that are found within the boundaries of a nation-state (Moga, 2016, pp 97-104). Thus, through information warfare, we understand the actions of "action to deny, exploit, corrupt, or destroy" from the Challenger, developed against the national cybernetic infrastructure of the Defender, with the intention and ability to prevent such action on their own national cybernetic infrastructure. The purpose of information warfare as an instrument in the hybrid warfare is the destruction of critical cyber infrastructure components: servers, clients, and the information transfer systems.

2. Theoretical Aspects

In terms of areas of applicability, the poliheuristic paradigm deals mainly with national security issues and foreign policy analysis, economic issues, internal policy issues, etc (Mintz, 2005, pp. 94–98). For analysis specific to the foreign policy area we can mention:

a study on Turkey's foreign policy on the issue of Cyprus (Erciyas, 2014), (Sula, 2011), the study of military coalitions and alliances (Park, 2010), research on general political crises (James, 2005, pp. 31–54) or on political crises (Ye, 2007, pp. 317–344), etc. For evaluations of the poliheuristic paradigm and comparative analysis of its performances and limitations when compared with other paradigms, or for its ability to absorb concepts specific to international relations and foreign policy, we can recall research regarding: the foreign policy decisions in autocratic regimes (Kinne, 2005, pp. 114–128), Arab-Israeli conflicts (Beckerman-Boys, 2014, 225–242), the issue of bureaucrats in opposition to the ballot box (Christensen, 2004, pp. 69-90), the traditional analysis of the foreign policy decision versus the poliheuristic one (Dacey, 2004, pp. 38-55), Predictive and Political Positions (Brulé, 2008, pp. 266-293), etc.

In Mintz's point of view, the poliheuristic paradigm, in order to deduce the way a decision-maker makes a particular choice, one must go through two stages in which the *two-stage process in making decisions* is integrated:

1. The author proposes the design of the poliheuristic decision matrix with all its specific elements: alternatives or actions, dimensions of the results, the implications of the dimensions specific to each alternative, the rates of each dimension for an alternative;
2. The second stage involves defining decision-making relationships involving a two-stage process in making decisions in order to establish a hierarchy of alternatives from the most favorable to the least favorable.

Designing the poliheuristic decision matrix of the decision-maker leader – contains several elements that define it as a tool for analyzing the actions it can take in order to evaluate the results it can reach based on the dimensions of these results. The ratio between dimensions and each alternative is defined by the rate.

Alternatives – represent conflict or cooperative behaviors, which the decision-maker may adopt. For example, in the case of an escalating conflict, Mintz adopts four alternative actions (Mintz, 2005, pp. 94-98): Do Nothing, Apply Sanctions, Containment, Use Force.

Dimensions – defines results indicators that operate the results of the alternatives. It also bears the name of the criteria. For example, quoting (James, 2004, pp. 31–54), Mintz proposes to reach the dimensions: political, military, economic, and diplomatic (Mintz, 2005, pp. 94-98).

Ratings – is the way the decision maker determines the importance of a particular dimension for a given alternative/action. If the dimension is not critical, it will get values between -10 and -1. If the size is critical for the wo-stage process in making decisions, it will get values between 0 and +10. Alternatives with non-critical values will be excluded from the decision matrix, with critical value alternatives determining the implications and decision-making relationships that define the two-stage process in making decisions.

Implications – consist of explanations or descriptions of the consequences of each alternative for each dimension (Mintz, 2010, pp.87-93). For a unitary treatment of a

large number of implications, the authors recommend treating the implications with the rational choice paradigm as elements specific to the second stage of the two-stage process in making decisions.

Defining of decision making relationships – in several papers ways of making decisions for actors with bounded rationality are presented such as *bounded rationality and intuitive decision making* or *fast and frugal decision making* (Lau, 2006, pp.12-20). It is also the use of rates with the decider *bounded rationality and intuitive decision making* which determines how decisions are made for the rational choice paradigm (Mintz, 2002, pp.1-11). In literature, several non-compensatory decision rules are used, such as Conjunctive Decision Rule (CON), Disjunctive Decision Rule (DIS), Elimination-by-aspect (EBA) Decision Rule, Lexicographic (LEX) Decision Rule (Mintz, 2010, pp.35-38).

3. Results

The informational warfare strategies mentioned in the title of the research are specific to military intelligence (Rácz, 2015, pp. 57-82). They were then extended to the field of cyber-attacks with rational approaches. In this study we will integrate the field of security studies of the poliheuristic paradigm based on bounded rationality and intuitive decision making with the *two-stage process in making decisions.* That is why the first step in shaping the concept of hybrid warfare is to build the poliheuristic decision matrix, and the second is to establish the rules of decision. For a broader description of the canonical strategies of the informational warfare, the reader can study the works (Poisel, 2013, pp. 107-121).

Alternatives – are comprised in this research of the five canonical strategies of the informational warfare defined below (Poisel, 2013, pp.107-121):

a. *Denial of information/passive denial* – this type of action consists in the defragmentation by Defender of certain features of the equipment that make up the critical cyber infrastructure (switches, routers, and computers) and which cannot be used in a cybernetic attack by the Challenger state.
b. *Disruption and destruction/active denial* – is based on the insertion of false information of the Challenger State into the national cyber infrastructure of the Defender, thus causing dysfunctions or damage to the latter.
c. *Deception and mimicry* – insertion of false information into the Defender's national cybernetic infrastructure by Challenger, so that the Defender's cyber defense equipment cannot separate the false information from the Challenger state.
d. *Subversion* – is the process of inserting information from the state of Challenger into the cyber infrastructure of the Defender State that will trigger its self-destruction.

e. *Exploitation* – is the process by which the Challenger State gathers information on the critical infrastructure of the Defender so the Challenger is more effective in the future situation assessment of the Defender.

Dimensions – is based on Colonel Warden's approach. He proposed a model of conceiving an enemy state through five concentric rings (Warden III, 2017):

1. The central ring is made up of the political power of the sovereign state, in our case, the Defender. We will name this dimension Government.
2. The following two rings are the 'organic essential ring' and 'the ring of the infrastructure' respectively. The ring of organic essential elements generally contains raw materials (utilities, hydrocarbons, wood-based resources) and elements of first necessity (money, water, food). The ring of the infrastructure consists in the processing capability and the transport routes. These two rings will together build the 'Economy' dimension.
3. The fourth ring consists in the population and the public opinion in the online space and has the Social Networking and Social Media dimension.
4. The fifth ring is the military dimension, which will be named Military.

Ratings – are values of scores between 0 and 10 that the analyst will apply for each action to the impact of a specific dimension. In the three tables below we define the decision matrices that the Challenger will develop through the five canonical strategies of the informational warfare on the four dimensions of the Defender's national cyber infrastructure. We are further interested in developing a way of calculating rates based on the number of servers destroyed by Challenger in the Defender's national cybernetic infrastructure through one of the five canonical strategies of the informational warfare.

Preparatory phase Table 1

	passive denial	active denial	deception and mimicry	subversion	exploitation
Government	r_{11}^{PPh}	r_{12}^{PPh}	r_{13}^{PPh}	r_{14}^{PPh}	r_{15}^{PPh}
Economy	r_{21}^{PPh}	r_{22}^{PPh}	r_{23}^{PPh}	r_{24}^{PPh}	r_{25}^{PPh}
Social Network and Social Media	r_{31}^{PPh}	r_{32}^{PPh}	r_{33}^{PPh}	r_{34}^{PPh}	r_{35}^{PPh}
Military	r_{41}^{PPh}	r_{42}^{PPh}	r_{43}^{PPh}	r_{44}^{PPh}	r_{45}^{PPh}
Final Choice	FC_1^{PPh}	FC_2^{PPh}	FC_3^{PPh}	FC_4^{PPh}	FC_5^{PPh}

Attack phase Table 2

	passive denial	active denial	deception and mimicry	subversion	exploitation
Government	r_{11}^{APh}	r_{12}^{APh}	r_{13}^{APh}	r_{14}^{APh}	r_{15}^{APh}
Economy	r_{21}^{APh}	r_{22}^{APh}	r_{23}^{APh}	r_{24}^{APh}	r_{25}^{APh}
Social Network and Social Media	r_{31}^{APh}	r_{32}^{APh}	r_{33}^{APh}	r_{34}^{APh}	r_{35}^{APh}
Military	r_{41}^{APh}	r_{42}^{APh}	r_{43}^{APh}	r_{44}^{APh}	r_{45}^{APh}
Final Choice	FC_1^{APh}	FC_2^{APh}	FC_3^{APh}	FC_4^{APh}	FC_5^{APh}

Stabilization phase Table 3

	passive denial	active denial	deception and mimicry	subversion	exploitation
Government	r_{11}^{SPh}	r_{12}^{SPh}	r_{13}^{SPh}	r_{14}^{SPh}	r_{15}^{SPh}
Economy	r_{21}^{SPh}	r_{22}^{SPh}	r_{23}^{SPh}	r_{24}^{SPh}	r_{25}^{SPh}
Social Network and Social Media	r_{31}^{SPh}	r_{32}^{SPh}	r_{33}^{SPh}	r_{34}^{SPh}	r_{35}^{SPh}
Military	r_{41}^{SPh}	r_{42}^{SPh}	r_{43}^{SPh}	r_{44}^{SPh}	r_{45}^{SPh}
Final Choice	FC_1^{SPh}	FC_2^{SPh}	FC_3^{SPh}	FC_4^{SPh}	FC_5^{SPh}

r_{ij}^{XPh} - represents line rate i and column j in one of the three phases of the hybrid warfare.

If

i = 1, then the canonical strategy of the Challenger is passive denial;

i = 2, then the canonical strategy of the Challenger is denial;

i = 3, then the canonical strategy of the Challenger is deception and mimicry;

i = 4, then the canonical strategy of the Challenger is subversion;

i = 5, then the canonical strategy of the Challenger is exploitation.

j = 1, then the magnitude of the consequences of the Challenger actions on the Defender's national cyber infrastructure is Government.

j = 2, then the magnitude of the consequences of the Challenger actions on the National Defender's cybernetic infrastructure is Economy.

j = 3 then the magnitude of the consequences of Challenger actions on Defender's national cybernetic infrastructure is Social Network and Social Media.

j = 4 then the magnitude of the consequences of the Challenger actions on the Defender's national cybernetic infrastructure is Military.

For the exponent of the rate if *X = P* refers to the initial phase of the hybrid warfare preparatory phase. If *X = A* is the second attack phase and if *X = S* is the last stabilization phase.

Next, to determine the rate value, we need to determine the number of servers destroyed by a Challenger's certain canonical strategy in the Defender's national infrastructure. We will use some previous studies explaining how this is done using a computer-specific concept (Moga, 2016, pp. 97-104). Stages of identifying servers in Challenger's national cybernetic infrastructures include the following stages (Moga, 2015, pp 383-390):

1. Determination of DNS servers and their IP addresses in all four dimensions of the Defender: Government, Economy, Social Network and Social Media and Military;
2. Determination of IP addresses and address ranges in all four dimensions of the Defender: Government, Economy, Social Network and Social Media and Military;
3. Determination of the active servers within each IP range in all four dimensions of the Defender: Government, Economy, Social Network and Social Media and Military;
4. Determination of open ports on each server in all four dimensions of the Defender: Government, Economy, Social Network and Social Media and Military;
5. Determination of the services specific to each server in all four dimensions of the Defender: Government, Economy, Social Network and Social Media and Military.

In this way we determine the difference in the number of pre-and post-attack servers Δn_{ij}^{XPh} (Moga, 2017, pp. 364-370), from a certain dimension of Defender's Critical Cyber Infrastructure that is specific to a certain canonical strategy of Challenger to the value of the function rate with the following formula:

$$r_{ij}^{XPh} = f\left(\Delta n_{ij}^{XPh}\right)$$

The decision-making relationship in this study is considered to be the sum of the rates on the critical dimensions for a given action. In this study we consider all four of the dimensions critical and the decision relationship is given by the computed relation of the final choice for a given canonical strategy.

$$FC_j^{XPh} = \sum_{i=1}^{4} r_{ij}^{XPh}$$

Implications – in this case the implications are explanations or meanings of the ways in which actions influence each dimension of the decision matrix. András Rácz (Rácz, 2015, pp. 57-82) considers in his research that the efficiency of Russia's action in Ukraine is based on three elements:

1. The element of surprise
2. Denial of formal involvement
3. Attackers indistinguishable from civilians

As a result of the above-mentioned author's conclusions, denial of formal engagement and "attackers indistinguishable from civilians" are the most appropriate elements.

Therefore, these two types of strategies will have maximum scores of 10 on each of the four dimensions in the decision matrix of the preparatory phase. So the decision-making relationships are $FC_1^{PPh} = FC_2^{PPh} = 40$

And other relationships of final choice have values that tend to zero.

$$FC_3^{PPh} = FC_4^{PPh} = FC_5^{PPh} \longrightarrow 0$$

In the second phase of attack, the conditions for the hybrid warfare as a process require "military superiority of the Challenger State", "strong logistics of Challenger state actions", "presence of Challenger state minority as a source of legitimacy, the weak central power and the security of the Defender's state, "lasting, regionally-concentrated dissatisfaction with the central government of the Defender State", have the use of exploitation and subversion. These strategies have the role of destroying the central and military power of the Government and Military dimensions. So for the two dimensions the rates will get 10 and zero values for the remainder of the second decision matrix. So for the second decision matrix, the final choice relationships are:

$$FC_3^{APh} = FC_4^{APh} = FC_5^{APh} = 20$$

And other relationships of final choice have values that tend to zero.

$$FC_1^{APh} = FC_2^{APh} \longrightarrow 0$$

As an implication for the third one in which the Challenger State is pursuing the consolidation of new political and military powers, the *passive denial* and *active denial* strategies will again be used to ensure "strong media presence of the Challenger State both in the Defender state and abroad". This involves social networking and social media dimensions for the two strategies and scores 10 and zero for the rest. So in this case, the final election relationships have the following values:

$$FC_1^{SPh} = FC_2^{SPh} = 10$$

$$FC_3^{SPh} = FC_4^{SPh} = FC_5^{SPh} \longrightarrow 0$$

The weighting approach and the calculation of the final selection functions are strictly indicative. For a concrete calculation of alienation and defense policies, researchers have to take into account many more elements.

4. Conclusion and Future Works

The research of the hybrid warfare is strictly limited to its cybernetic dimension. The novelty of the hybrid warfare concept still suffers from deficiencies, and therefore the lack of mature literature has rendered impossible the maturity of the operationalization of this concept. Adoption of the viewpoint on hybrid warfare was made from theoretical rationale that allows the rapid implementation of the concepts of information warfare and the poliheuristic paradigm. The authors do not claim to have clarified an important and up-to-date theme, but they have just opened a new path in the field of security research and new threats to European and NATO states. Research is to be deepened in the future and extended to predictive models such as LAMP, AHP, Delphi, or event-driven scenarios, maintaining the poliheuristic core of research.

References

Beckerman-Boys, C. (2014). Third Parties and the Arab-Israeli Conflict: Poliheuristic Decision Theory and British Mandate Palestine Policy. *Foreign Policy Analysis*, Vol. 10, No. 3, pp. 225-242.

Brulé, D. J. (2008). The Poliheuristic Research Program: An Assessment and Suggestions for Further Progress. *International Studies Review*, Vol. 10, No. 2, pp. 266-293.

Christensen, E.J., Redd, S.B. (2004). Bureaucrats versus the Ballot Box in Foreign Policy Decision Making An Experimental Analysis of the Bureaucratic Politics Model and the Poliheuristic Theory. *Journal of Conflict Resolution*, Vol. 48, No. 1.

Dacey, R., Carlson, L.J. (2004). Traditional Decision Analysis and the Poliheuristic Theory of Foreign Policy Decision Making. *Journal of Conflict Resolution*, Vol. 48, No.1.

Erciyas, O. (2014). *Turkish Foreign Policy towards the Cyprus Crises of 1964, 1967, and 1974: A Poliheuristic Perspective*. Available at: http://www.thesis.bilkent.edu.tr/0007086.pdf. Accessed: 7th October 2017.

James, P., Zhang, E. (2005). Chinese Choices: A Poliheuristic Analysis of Foreign Policy Crises, 1950–1996. *Foreign Policy Analysis*, Vol. 1, No. 1, pp. 31-54.

Kinne, B. J. (2005). Decision Making in Autocratic Regimes: A Poliheuristic Perspective. *International Studies Perspective,* 6, pp. 114-128.

Lau, R. R., Redlawsk, D. P. (2006). *How Voters Decide Information Processing during Election Campaigns*. Cambridge: Cambridge University Press.

Mintz, A., DeRouen Jr., K. (2010). *Understanding Foreign Policy Decision Making.* Cambridge: Cambridge University Press.

Mintz, A. (2002). *Integrating Cognitive and Rational Theories of Foreign Policy Decision Making.* Palgrave Macmillan.

Mintz, A. (2005). Applied Decision Analysis: Utilizing Poliheuristic Theory to Explain and Predict Foreign Policy and National Security Decisions. *International Studies Perspectives*, Vol. 6, pp. 94-98.

Moga, H., Boscoianu, M., Ungureanu, D., Lile, R. and Erginoz, N. (2015) Massive Cyber-Attacks Patterns Implemented with BDI Agents. *Applied Mechanics and Materials*. Vol. 811, pp. 383-389,

Moga, H., Boscoianu, M., Ungureanu, D., Sandu, F. and Lile, R. (2016). Using BDI Agents in Flexible Patterns for Cyber-Attacks over Electrical. *Applied Mechanics and Materials*, Vol. 841, pp. 97-104.

Moga, H., Boscoianu, M., Ungureanu, D., Sandu, F. and Boboc, R. (2017). Refined Concepts of Massive and Flexible Cyber Attacks with Information Warfare Strategies. *Journal of Communications,* Vol. 12, No. 6., pp. 364-370

Park, J. G. (2010). *Poliheuristic Theory and Alliance Dependence: Understanding Military Coalitions*. Available at: http://oaktrust.library.tamu.edu/bitstream/handle/1969.m1/ETD-TAMU-2010-05-7709/PARK-DISSERTATION.pdf?sequence=2. Accessed: 19th September 2017.

Poisel, R. A. (2013). *Information Warfare and Electronic Warfare Systems, Artech House Power Infrastructures*. Norwood, Massachusetts: Artech House.

Rácz, A. (2015*). Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*. Available at: https://storage.googleapis.com/upi-live/2017/01/fiiareport43.pdf. Accessed: 15th September 2017.

Sula, I. E. (2011). *Where is the Anchor Now? A Poliheuristic Analysis of Turkish Foreign Policy in the AKP Period*. Available at: http://www.thesis.bilkent.edu.tr/0005030.pdf. Accessed: 11th October 2017.

Warden III, J. A. (2017). *The Enemy as a System*. Available at: http://www.ciar.org/ttk/mbt/strategy.Warden.enemy-as-a-system.html. Accessed: 19th October 2017.

Ye, M. (2007). Poliheuristic Theory, Bargaining, and Crisis Decision Making. *Foreign Policy Analysis*, 3, pp. 317-344.