Advances in Economics, Business and Management Research, volume 188
Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021)

Information Threats in the Context of Hybrid War

Nataliia Svyrydiuk * 1 [0000-0001-9772-1119], Yaroslav Likhovitskyy 2 [0000-0002-8537-2676], Pavel Polián 3 [0000-0002-3258-0340]

[1]*State Scientifically Research Institute of the Ministry of Internal Affairs, Kyiv, Ukraine*
[2]*Uzhhorod National University, Ukraine*
[3]*Akademie HUSPOL, Czech Republic*
** S_N_P_@ukr.net*

ABSTRACT

The paper, based on empirical data on the spread of hybrid threats in the field of civil security, taking into account the risk-oriented approach, examines hybrid threats related to the informative environment. The risks of spreading of this group of hybrid threats have been assessed. There are some of them that are characterized by the highest level of risk. The focus is on quantifying ability / vulnerability of the civil security system to counter hybrid information threats. Using the constructed model of linear regression, the risk of spreading the hybrid threat "influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust" was assessed, indicators of ability to prioritize risk reduction were identified, their vulnerability according to the level of assessment and the corresponding forecast is made to reduce the level of risk of spreading of a certain hybrid threat.

***Keywords**: hybrid threats, informative environment, capability, vulnerability, risk assessment, linear regression.*

1. INTRODUCTION

Hybrid threats in the system of contemporary security of society occupy one of the most important places. This is especially important for countries where external aggression or other forms of armed conflict are in the active phase. The security situation requires raising awareness of hybrid informaton threats and the ability to effectively counter their spread [1]. Modern risk management involves the analysis and monitoring of both key threats and factors that form the mechanisms for effective response to such threats, formation of a system of resilience to threats, management decisions to increase the ability to counter hybrid threats, avoid vulnerable components in security, etc.

2. RESEARCH ANALYSIS

The study of hybrid threats, justification of measures to counter them, is the study subject of many researchers, in particular: Arzumanyan R. [2], Gbur Z. [3], Korystin O. [4], Magda E. [5], Martyniuk V. [6], Predborsky V. [7], Rusnak I. [8] and others. But the reality of hybrid threats to Ukraine requires, above all, applied scientific analysis and formation of reasonable research theories, implementation in practice.

3. THE PURPOSE OF THE PAPER

Based on a risk-oriented approach to assess information hybrid threats in the civil security sector, analyze [9] the factors that determine the effectiveness of countering hybrid threats, form a system of indicators of capability / vulnerability [10] that correlate with information hybrid threats and affect risk reduction. their spread. To build, based on regression analysis [11], a model for forecasting the spread of information hybrid threats subject to enhanced key capabilities and reducing the risk of system vulnerabilities of counteraction to information hybrid threats.

4. THE MAIN MATERIAL

Investigating hybrid threats in the field of civil security, scientists of the State Research Institute of the Ministry of Internal Affairs of Ukraine, on the basis of up-dated theoretical developments, have introduced methodological principles for assessing the spread risks of hybrid threats [1]. A risk-based approach has been used to assess both threats and indicators of ability / vulnerability of the system to counter these hybrid threats. In addition, generalized groups of hybrid threats in the civil security sector have been identified, as hybridization can extend to all areas of public relations. One of the key groups of hybrid threats in the field of civil security is *hybrid threats related to the informative environment* [12, 13].

Of the total array [1] of identified hybrid threats in the field of civil security, 25 hybrid threats are associated with the information environment, some of which (11) are shown in Table 1 with a certain level of risk.

Graphical representation of the risk rating of the spread of information hybrid threats (Figure 1) forms a vision of some of the most significant *hybrid threats related to the informative environment.*

Using approaches based on the reflection of risk limits, significant threats, in the range of 50-60%, are highlighted in orange, and less significant (40-50%) - in yellow and (less than 40%) in green.

Thus, the level of risk of spreading significant *hybrid threats related to the informative environment* is as follows:

stimulation and encouragement of citizens in border regions to obtain a second citizenship contrary to the legislation of Ukraine - 53.33%;

creation and support of political projects in order to shake the socio-political situation, discredit the state leadership, etc. - 51.36%;

aggressor control of content in areas close to hostilities and border areas - 51.04%.

Less significant from the given list of hybrid threats by the level of risk is determined by the threat: *influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at*

reducing trust – 38,6%. At the same time, it is worth paying attention to a more detailed analysis of the risk level assessment of this threat, not by the average value, but by the distribution of expert assessments within the whole scale (0-100%) (Figure 2).

Despite the fact that the average value when assessing the risk of spreading a hybrid threat: *influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust*, – it is received 38.6%, expert assessment, according to the distribution on the whole scale, 30% of experts see risk assessment at a level above 50%. This indicates the need for additional control over the identified threat and its relevance in modern conditions.

Table 1. Risk assessment of the spread of hybrid threats

Hybrid threats related to the informative environment	**№TA**	**Risk, %**
Creation and support of political projects in order to shake the socio-political situation, discredit the state leadership, etc.	ta3	**51,36**
Stimulation and encouragement of citizens in border regions to obtain a second citizenship contrary to the legislation of Ukraine	ta4	**53,33**
Inciting certain segments of the population to civil disobedience and making economic and political demands	ta28	**41,10**
Aggressor control of content in areas close to hostilities and border areas	ta39	**51,04**
Provocative activity of an aggressor-controlled media resource by concealing the ultimate beneficiary	ta40	**48,14**
Promotion of aggressive destructive narrative against bodies and employees of the Ministry of Internal Affairs system through information media	ta41	**41,37**
Influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust	ta42	**38,60**
Influence of the Ministry of Internal Affairs on the reduction of trust in the political elite in the state	ta42.4	**43,59**
Influence on the consciousness of the population in order to discredit the authorities, bodies and employees of the Ministry of Internal Affairs	ta44	**49,15**
Influence on the population on discrediting the government, the system of the Ministry of Internal Affairs through the use of inform.-psychologist. operations	ta44.1	**43,38**
Influence on the population through information campaigns on artificial polarization and radicalization of society	ta44.4	**44,62**

Continuing the analysis, it is important to assess the capacity of the civil security system to reduce the risk of the spread of *hybrid threats related to the informative environment.* It is used indicators, aimed at assessing the capabilities that characterize the effectiveness of the civil security system in combating hybrid threats [1]. The assessment is based on a risk-based approach and takes into account both the probability of effectiveness level and the impact on countering hybrid threats.

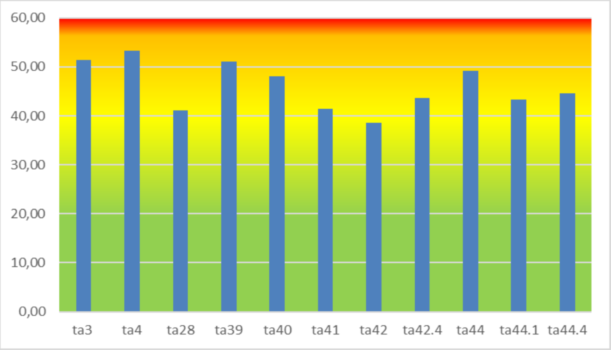

Figure 1 Rating of hybrid threats related to the informative environment

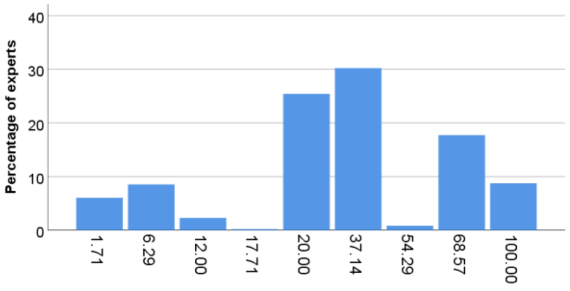

Figure 2 Influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust

Total 152 indicators were used to characterize the effectiveness of the civil security system in counteracting hybrid threats [1]. Hypothetically, some of them are characterized by some statistical relationship with individual hybrid threats and may directly or indirectly affect the reduction of risk of spreading the threat. In order to confirm this hypothesis, we built a model of linear regression (using SPSS statistics) by the method of STEPWISE where the dependent variable used a hybrid threat TA42 - *influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust* (Figure 3).

Using the results of linear regression, the optimal dependence of the hybrid threat was determined *influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust* from the variables characterizing efficiency of activity of civil safety bodies concerning counteraction to hybrid threats (Table 2). Thus, the key predictors of regression analysis are:

- RS44 - The level of personal resilience of the staff of the bodies of the Ministry of Internal Affairs to the perception of misinformation;
- RS51 - Compliance of professional training with the requirements of practice at the level of initial (basic) training;
- RW1 - Imperfect regulatory and legal support for the activities of the system of the Ministry of Internal Affairs;
- RW2 - Discrediting the reform of the bodies of the Ministry of Internal Affairs by individual employees;
- RW9 - Insufficient level of professional training at the managerial level.

```
REGRESSION
  /DESCRIPTIVES MEAN STDDEV CORR SIG N
  /MISSING LISTWISE
  /STATISTICS COEFF OUTS R ANOVA
  /CRITERIA=PIN(.05) POUT(.10)
  /NOORIGIN
  /DEPENDENT TA42
  /METHOD=STEPWISE Rs1 Rs2 Rs3 Rs4 Rs5 Rs6 Rs7
Rs8 Rs9 Rs10 Rs11 Rs12 Rs13 Rs14 Rs15 Rs16 Rs17
Rs18 Rs19 Rs20 Rs21 Rs22 Rs23 Rs24 Rs25 Rs26 Rs27
Rs28 Rs29 Rs30 Rs31 Rs32 Rs33 Rs34 Rs35 Rs36 Rs37
Rs38 Rs39 Rs40 Rs41 Rs42 Rs43 Rs44 Rs45 Rs46 Rs47
Rs48 Rs49 Rs50 Rs51 Rs52 Rs53 Rs54 Rs55 Rs56 Rs57
Rs58 Rs59 Rs60 Rs61 Rs62 Rs63 Rs64 Rs65 Rs66 Rs67
Rs68 Rs69 Rs70 Rs71 Rw1 Rw2 Rw3 Rw4 Rw5 Rw6
Rw7 Rw8 Rw9 Rw10 Rw11 Rw12 Rw13 Rw14 Rw15
Rw16 Rw17 Rw18 Rw19 Rw20 Rw21 Rw22 Rw23 Rw24
Rw25 Ro1 Ro2 Ro3 Ro4 Ro5 Ro6 Ro7 Ro8 Ro9 Ro10
Ro11 Ro12 Ro13 Ro14 Ro15 Ro16 Ro17 Ro18 Ro19
Ro20 Ro21 Ro22 Ro23 Ro24 Ro25 Ro26 Ro27 Ro28
Ro30 Ro31 Ro32 Ro33 Ro34 Ro35 Ro36 Ro37 Ro38
Ro39 Ro40 Ro41 Ro42 Ro43 Ro44 Ro45 Ro46 Ro47
Ro48 Ro49 Ro50 Ro51 Ro53 Ro54 Ro55 Ro56 Ro57.
```

Figure 3 Syntax of linear regression of the threat "*influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust* " (TA42)

One predictor of RS44 has a negative value, and therefore with increasing level of its assessment, the risk of spreading the threat will tend to decrease. Other predictors with the same sign in the linear regression model, and therefore will affect the threat with a direct relationship: increasing the level of predictor evaluation will affect the increase of the specified threat.

Table 2. Linear regression model of the "influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust"

Factor^{a}					
Model	Unstand factors		Standard factors	т	P value
	B	Std. Err.	Beta		
(Constant)	13,886	3,333		4,188	0,000
RS44	-0,154	0,051	-0,160	-3,110	0,000
RS51	0,290	0,055	0,277	5,396	0,000
RW1	0,105	0,037	0,128	2,776	0,006
RW2	0,131	0,034	0,177	3,830	0,000
RW9	0,141	0,035	0,180	4,020	0,000

- RS51 - Compliance of professional training with the requirements of practice at the level of initial (basic) training;

- RW1 - Imperfect regulatory and legal support for the activities of the system of the Ministry of Internal Affairs;

- RW2 - Discrediting the reform of the bodies of the Ministry of Internal Affairs by individual employees;

- RW9 - Insufficient level of professional training at the managerial level.

At the same time, it is extremely important to take into account the real situation in the model. In our version, it is an assessment of vulnerability or ability of the civil security system to reduce the risks of the spread of hybrid information threats. According to the study [1], the level of risk relative to the predictors indicated in the model (Table 2) is characterized mainly by vulnerability (Figure 4). Predictors RW1, RW2, RW9 in their content are already vulnerabilities as they are assessed as "weaknesses" and identified with a negative content.

One predictor of RS44 has a negative value, and therefore with increasing level of its assessment, the risk of spreading the threat will tend to decrease. Other predictors with the same sign in the linear regression model, and therefore will affect the threat with a direct relationship: increasing the level of predictor evaluation will affect the increase of the specified threat.

At the same time, it is extremely important to take into account the real situation in the model. In our version, it is an assessment of vulnerability or ability of the civil security system to reduce the risks of the spread of hybrid information threats. According to the study [1], the level of risk relative to the predictors indicated in the model (Table 2) is characterized mainly by vulnerability (Figure 4). Predictors RW1, RW2, RW9 in their content are already vulnerabilities as they are assessed as "weaknesses" and identified with a negative content.

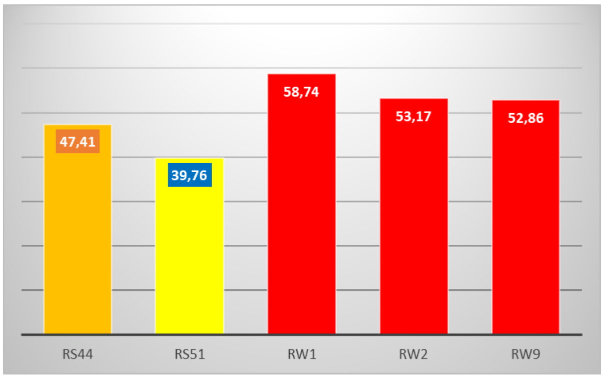

Figure 4 Risk Assessment largest predictors

Therefore, predictors RS44 and RS51, although positive in nature, are estimated to be more vulnerable as less than 50%. This opinion is proved experimentally by using limit levels based on matrix analysis [1].

Taking into account the level of vulnerability by key predictors and using a linear regression model, the risk of spread *influences on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust* (Figure 5).

Model and forecast	Coeff	P value	**Rating %**	
(Constant)	13,886	0,000		
RS44	-0,154	0,000	47,41	-7,280920591
RS51	0,290	0,000	39,76	11,5234602
RW1	0,105	0,006	58,74	6,144196434
RW2	0,131	0,000	53,17	6,98138524
RW9	0,141	0,000	52,86	7,438466821
TA42		**RA = 38,64 %**		

Figure 5 Risk assessment of using of "*influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust*" (TA42)

Given the current state of vulnerability of the civil security system in counteracting a particular hybrid threat, based on the predictors specified in the linear regression model, the real level of spread risk *influences on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust* (38,69 %) is slightly higher than its estimate based on an integrated indicator of likelihood and consequences (38,6 %).

Therefore, the considered model of linear regression forms bases for the forecast of risk reduction *influences on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust* provided increasing the capacity of the civil security system to counter hybrid information threats (Figure 6):

Coefficient	P value	Rating +/-20%	
13,886	0,000		
-0,154	0,000	67,41	-10,35239099
0,290	0,000	39,76	11,5234602
0,105	0,006	38,74	4,05219901
0,131	0,000	33,17	4,355323461
0,141	0,000	32,86	4,624063938
RA = 28,09 %			

Figure 6 Forecast of the risk influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust if changing vulnerabilities by 20%

5. CONCLUSIONS

Thus, based on assessment of the spread risks of *hybrid threats related to the informative environment*, the most significant threats:

stimulation and encouragement of citizens in border regions to obtain a second citizenship contrary to the legislation of Ukraine – 53,33%;

creation and support of political projects in order to shake the socio-political situation, discredit the state leadership, etc. – 51,36%;

aggressor control of content in areas close to hostilities and border areas – 51,04%.

Of the general list of indicators (152) that characterize the effectiveness of the law enforcement system in combating hybrid threats, 5 of them are characterized by the greatest impact on the threat «*influence on the consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust*». Risk assessments are characterized by system vulnerabilities, but affect the risk level of a particular threat in different ways.

Based on the linear regression model, a forecast of reducing the risk of spreading the hybrid threat *"influence on consciousness of employees of the system of the Ministry of Internal Affairs, by discrediting, aimed at reducing trust"* was built, taking into account the level of vulnerability assessment of the civil security system.

REFERENCES

[1] Kovalchuk, T. Korystin, O. and Svyrydyuk, N. (2019), "Hybrid threats in the civil security sector in Ukraine", *Nauka i pravooxorona*, vol. 3 (45), pp. 69-79, DOI: 10.36486/np.2019308

[2] Arzumanyan, R.V. (2011), "Defining war in the 21st century", *Obzor XXI ezhegodnoy konferentsii po strategii Instituta strategicheskih issledovaniy Armeyskogo voennogo kolledzha*, 6-8 aprelya 2010, Erevan, 48 p.

[3] Gbur, Z.V. (2018), "Actual hybrid threats to economic security of Ukraine", Investitsiyi: praktyka ta dosvid, vol. 7/2018, pp. 97-99.

[4] Korystin, O.Y. Katamadze, G.S. Nekrasov, V.A. Mel‘nyk, V.I. and etc. (2021), *Fiscal Security of Ukraine – Threats, Risks, Vulnerabilities: Strategic vision*, Vidavnichij Dim, Gelvetika, LLC, Kherson, Ukraine iн

[5] Mahda, YE.M. (2014), "Hybrid warfare: the essence and structure of the phenomenon", *Mizhnarodni vidnosyny: Seriya "Politychni nauky"*, vol. 4, available at: http://journals.iir.kiev.ua/index.php/pol_n/article/view/2489

[6] Martynyuk, V. (2018), *Hibrydni zahrozy v Ukrayini i suspil'na bezpeka. Dosvid YES i skhidnoho partnerstva* [Hybrid threats in Ukraine and social security. The experience of the EU and the Eastern Partnership], Kyiv, Ukrainian, 106 p.

[7] Predborskyy, V.A. (2014), "Hibrydna" war as a reflection of the laws of society of independent modernization", *Formuvannya rynkovykh vidnosyn v Ukrayini*, № 10, pp. 13-18.

[8] Rusnak, I.S. (2015), "Ukraine's military security in the light of reforming the security and defense sector", *Nauka i oborona*, vol. 2, pp. 9-14.

[9] Hua-Gang Yu, Gao-Ming Huang and Jun Gao (2010), "Nonlinear Blind Source Separation Using Kernel Multi-set Canonical Correlation Analysis", *International Journal of Computer Network and Information Security*, vol. 2, no.1, pp.1-8, DOI: 10.5815/ijcnis.2010.01.01

[10] Sonali Sharma and Shilpa Mahajan (2017),"Design and Implementation of a Security Scheme for Detecting System Vulnerabilities", *International Journal of Computer Network and Information Security,* vol. 9, No. 10, pp. 24-32, DOI: 10.5815/ijcnis.2017.10.03

[11] Mohamed Zaim Shahrel, Sofianita Mutalib and Shuzlina Abdul-Rahman (2021), "PriceCop–Price Monitor and Prediction Using Linear Regression and LSVM-ABC Methods for E-commerce Platform", *International Journal of Information Engineering and Electronic Business*, vol. 13, No. 1, pp. 1-14, DOI: 10.5815/ijieeb.2021.01.01

[12] Korystin, Oleksandr and Svyrydiuk, Nataliia (2021), “Activities of Illegal Weapons Criminal Component of Hybrid Threats”, *Proceedings of the International Conference on Economics, Law and Education Research (ELER)*, vol. 170, 22 March, pp. 86-91, DOI:10.2991/aebmr.k.210320.016

[13] Korystin, Oleksandr and Svyrydiuk, Nataliia (2021), “Formation of security competences in law enforcement activities”, *Nauka i Pravookhorona,* vol. 1 (51), pp. 191-198, DOI: 10.36486/np.2021.1(51).20