

Methods for Assessing Threats to Criminological Security

Daria Prokofieva-Yanchylenko * [0000-0001-6458-5536]

National Security and Defense Council's of Ukraine Inter-Service Research Center into Combating Organized Crime Problems, Kyiv, Ukraine

* *d.pr.yanchylenko@gmail.com*

ABSTRACT

Modern society is a "society of risk", and crime - its institutional practice. The permanent existence of criminal threats to all spheres and objects of national security of Ukraine, the causes and conditions that give rise to crime and related challenges, presupposes the existence of an integrative component of national security - criminological security. It is impossible to achieve an ideal state of criminological security, because it is impossible to get rid of the corresponding threats completely. At the same time, it is possible to achieve a state of criminological security when crime and its individualized manifestations (criminal offenses), although they will affect society, the level of this influence will be socially acceptable. Maintaining a socially acceptable level of criminological security can best be achieved through risk management, which has long been an integral tool not only for business projects or disaster prevention, but also for planning the life of society in all its spheres in terms of sustainable development. The key to successful application of risk management methodology is effective assessment of threats to criminological security. This research proposes a heuristic methodology for assessing and certification of relevant threats, which is designed to provide forecasting of the dynamics of their development, as well as modeling and support of decisions in the field of crime prevention.

Keywords: *criminological security, threat to criminological security, risk of criminological security, risk management.*

1. INTRODUCTION

Given the wide range of views on criminological security [1-7], it should be defined as an integrative component of national security and the state of its objects (individual, society and state), including their protected values, individual rights and freedoms, material and spiritual values of society, the constitutional order, sovereignty and territorial integrity of the state, etc.), which characterizes their ability to maintain their systemic qualities and relationships, to function stably, to develop progressively and to be less vulnerable [8] to criminal threats and related challenges.

From the «risk point of view», a crime is a "catastrophic event" that changes the state of the system. All complex self-organizing systems are characterized by complex causal relationships, when one event (cause) can cause a number of changes ("avalanche") that will affect the system as a whole. The so-called "avalanche processes" are characterized by asymmetry of causes and effects, and some causal factors are probabilistic for an outside observer. Completion of the "avalanche of

changes" determines the transition to a new state of equilibrium of the system and can be significantly delayed compared to the original event [9-11]. The probability of committing a crime is on the verge of determined and probable behavior, therefore, it is advisable to use in criminological security risk [12] management methodology.

The risk of criminological security should be defined as the probability [13] of realization of a criminal threat and the potential possibility of the system (object) to suffer losses as a result of its implementation. Such risk can be analyzed and assessed systematically, introducing its assessment as a mandatory element of state anti-crime policy. The results of risk assessment give an idea of the level of public danger and can serve as a guide for the legislator in addressing issues of criminalization or decriminalization of an act, as well as the separation of crimes from other offenses. "Feedback" between risks and threats [14] can ensure the implementation of the most effective mechanism for countering threats to criminological security - through risk management.

At the heart of the concept of socially acceptable level of criminological security, and accordingly - acceptable risk of criminological security is the differentiation of risk levels at different stages of its manifestation [15], as well as the understanding that risk is not static and unchanging, but a controlled parameter. need to be managed. In this case, the impact can be exerted only on the identified, analyzed and assessed risk.

The initial stage of identification, analysis and risk assessment of criminological security is the assessment of threats that cause the relevant risks (an appropriate method is proposed in this treatise).

The article is organized as follows: in section 2, an overview of scientific developments related to the research; section 3 describes the problem statement; section 4 reflects the details of the proposed solution; in section 5 the conclusion on results of research is given.

2. RELATED RESEARCH

The principles of using risk management methodology in counteracting crime are the subject of scientific interest for many scientists.

According to R. Clark, who used a risk-oriented situational approach in crime prevention, a crime is more likely to be committed if the vulnerability of its victim is clearly defined, there is a clear purpose of the illegal act, there are certain characteristics that contribute to its commission [16]. The application of an eventological approach, which combines the features of actuarial and clinical approaches to risks [17], allows us to consider the risks of criminological security not only for the individual who performs a certain action (realizes a criminal threat), but also for third parties who may be harmed by criminal action. The notion of criminological security risk under such conditions may cover not only the potential impact of intentional unlawful encroachments, but also accidental events, unlawful acts committed through negligence, and so on.

In general, foreign experience in the use of risk management methodology in counteracting crime is quite rich, especially at the stage of risk assessment. It is advisable to take into account the practice of such scientific institutions as the Rutgers Center for Public Safety (USA, New Jersey), models of corruption and other risks, existing methods of risk assessment and management, in particular, the so-called "maximum" approach to systematize criminal threats, as well as the risks caused by them. A practical result of the Rutgers Institute's research was the development of the RTM (Risk Terrain Modeling) methodology, a model of territorial risk that analyzes the relationship between historical data on crimes committed in different parts of the city and the characteristics of these places [18; 19; 20].

The risk-oriented approach is successfully used not only in the research of domestic mercenary and violent crimes, but also to assess the threats of corruption. For example, in the article by A. Greykar and A. Sidebottom "Corruption and Control: An Approach to Reducing Corruption", the authors explore the feasibility of using preventive measures to eliminate or reduce corruption opportunities and argue that the environment plays a causal role in shaping corruption [21].

Some aspects of interdisciplinary risk management methodology are used in Ukraine to combat migration and customs offenses (for example, fiscal authorities use an automated risk analysis and management system, the main tool of which are risk profiles aimed at controlling certain characteristics of goods), money laundering, to solve certain tasks of preventing corruption offenses. The practice of threat assessment has been introduced into the system of prevention, response and cessation of terrorist acts. However, in general, this experience has not yet become universal.

3. STATEMENT OF THE PROBLEM

The implement of the risk management methodology into the practice of counteracting crime should be preceded by the development of theoretical and legal bases for assessing the threats of criminological security on the basis of existing and tested achievements of risk in comparison with the needs of law enforcement. According to Yu. Antonyan, "... if criminologists do not have their own theoretical basis, then its practical recommendations will be far-fetched, unfounded. In other words, the deeper the theoretical research, the more valuable and useful will be for practice proposals and recommendations made on the basis of theory" [22]. To this end, a method of quantitative and qualitative assessment of threats to criminological security is proposed.

4. THE PROPOSED SOLUTION

The proposed solution is based on the use of a heuristic approach, in which an important role is played by expert assessment, which determines the subjective probability of threats to criminological security and forms a set of factors that determine criminological security. These factors are evaluated in internal units (points), followed by the derivation of the final score and its interpretation.

Assessment is carried out by identifying threats to criminological security, analytical processing of information about such threats and determining their level.

4.1. Threats Identification

In order to identify threats to the criminological security of the analysis is subject to: operational information; information received in the form of appeals

of citizens and officials, inquiries of people's deputies of Ukraine, reports of crimes; official statistics characterizing the peculiarities of the criminal situation and security environment; results of monitoring of open information sources.

In order to increase the accuracy of the analysis results, the primary information is subject to preliminary assessment for reliability.

An indicative list of threats to criminological security is determined by the National Security Strategy of Ukraine, the Criminal Code of Ukraine, the Strategy for Combating Organized Crime, etc. Threats to criminological security should be investigated at all stages of their deployment.

Methods for identifying threats to criminological security may include: research of "checklists", structuring information using departmental classifiers, building a "threat tree", forming templates of typical threats, building models of the system (objects) of state security to identify their vulnerabilities and more.

The description of the threat to criminological security includes a description of the sphere of national security to which the threat relates, the source (initiator) of the threat, the addressee (goal) of the threat, the manifestations of the threat, the expected consequences of the threat.

4.2. Analytical Processing of Information about Threats to Criminological Security

Analytical processing of information on threats to criminological security provides awareness of the nature of the threat and provides initial data to determine the level of such threats.

Analytical processing of information on threats to criminological security includes qualitative and quantitative assessment of threats (Threats - Th), including the consequences of their implementation, related factors and associated with the implementation of the threat of probabilities, according to certain parameters.

The following parameters are subject to evaluation: probability of threat realization (P_{th}), threat relevance (Rel); threat dynamics (Dyn); harm of consequences (H); security environment in the context of threat realization (Env).

The following parameters are used to assess the probability of threat realization: the reality of the threat; recurrence of the threat; influence on the process of realization of the threat of control measures; probability of influence of unpredictable factors.

The following parameters are used to assess the relevance of the threat: development potential; adaptability; scale; latency; the possibility of inspiration

or nourishment from abroad; social danger; the possibility of corruption; impact on the deterioration of the criminal situation; impact on the deterioration of the socio-political situation; profitability for the initiator; additional parameters Rel_n (if applicable).

Assessing the dynamics of the threat requires determining the number of manifestations of the threat to criminological security for the current period (Dyn_1) and for the previous period (Dyn_2), which is determined for the needs of the study (1 year, 3 years, 5 years, 10 years, etc.).

To assess the danger of the consequences of the threat to criminological security, the following parameters are used: probability of consequences (P_{cons}); critical consequences.

The following parameters are used to assess the probability of consequences: the reality of the consequences; recurrence of cases of consequences; impact on the process of occurrence of the consequences of control measures; probability of influence of unpredictable factors.

The following parameters are used to assess the risk of consequences: criticality of adverse consequences (C) - human casualties; damage to health; property damage; criminalization of public administration, etc.; adequacy of means to minimize harm (M - measures to prevent and minimize harm or prevent its occurrence; measures to compensate for harm); "Price" of means to minimize harm (Mpr - costs of preventive activities, law enforcement, regulatory activities, etc.; restrictions on the rights and freedoms of citizens; restrictions on economic development of the country; restrictions on information development of the country, etc.).

The assessment of the security environment in the context of the threat is based on the SWOT methodology, where St - strengths, O - opportunities, W - weaknesses, Ch - challenges, which is used instead of "threat" (T) in the traditional methods). The factors selected for the study are assessed in terms of the extent to which they contribute to or hinder the realization of the threat to criminological security or the occurrence of its negative consequences.

When carrying out a qualitative (quantitative-qualitative) assessment, it should be taken into account:

- the realization of the threat to criminological security can have multiple consequences and affect a significant number of diverse goals;

- not every threat to criminological security as a result of its implementation causes consequences that can be measured in absolute statistical terms;

- the realization of the threat to criminological security may have insignificant adverse consequences in the short term at the same time with a high probability of their occurrence, or vice versa - significant adverse consequences

at the same time with a low probability of their occurrence. At the same time, both options for realizing the threat can have a significant negative cumulative effect in the long run.

The processing of the results of analytical processing of information on threats to criminological security is carried out using a relative tribal assessment scale: 1 - low level; 2 - intermediate level; 3 - high level. All parameters (for each studied threat) are evaluated in points from 1 to 3, after which their arithmetic mean value is calculated for each parameter separately, which is simplified by rounding to integers in the direction of a larger indicator.

Parameters for which the definition of indicators is based on statistical data characterizing the features of the security environment (information on the number of manifestations of the threat, the number of cases of adverse effects, etc.) are evaluated in points from 1 to 3 by the previous division into three groups: intermediate level (I); the indicator for the studied parameter is at the average level, ie in the range of the arithmetic mean value of the number of relevant manifestations / cases +/- 15% of this value (II); the indicator for the studied parameter is above the average level (III).

Parameters for which the definition of indicators is based on qualitative or quantitative-qualitative assessment, in particular, involves the assessment of probability, are evaluated in points from 1 to 3 according to the expert group.

In the absence of information that allows to determine the indicator of the relevant parameter with sufficient clarity, it is estimated as average.

When assessing the criticality of consequences if a certain type of adverse effects may occur in the case of a threat and is directly causally related to its implementation, but is not the main type of probable consequences, the level of damage is assessed as average.

The "cost" of harm minimization means not only the cost of law enforcement or protective measures and means, but possible restrictions or violations of human and civil rights and freedoms, which are expected to lead to the necessary measures to minimize potential harm. For all parameters, it is not the actual indicators (for example, the actual insufficient funding of law enforcement) that are assessed, but the indicators that are sufficient to prevent or minimize the damage. The high price of harm minimization means, thus, neutralizes the indicator of the parameter "harm minimization means", at the same time increasing the risk of consequences.

To assess the dynamics of the threat, a comparison of the number of manifestations of the threat to criminological security in the current period with the number of manifestations of the corresponding threat in the previous period is used.

The dynamics are estimated in points from 1 to 3 according to the results of a preliminary comparison of quantitative indicators as: positive, if there is a decrease in

the number of manifestations of the threat compared to the previous study period by more than 5% (I); stable if there is a constant number (in the range of +/- 5%) manifestations of the threat compared to the previous study period (II); negative if there is an increase in the number of threats compared to the previous study period by more than 5% (III).

In determining the relevance of threats to criminological security, the critical consequences of their implementation, the "price" of minimization, security environment in the context of the implementation of threats by the expert group can use additional parameters due to the specifics of specific threats.

4.3. Determination of the Level of Threats to Criminological Security

Determining the level of threats to criminological security is carried out by calculating the quantitative indicators obtained from the evaluation of the parameters listed above. Summary indicators of the corresponding parameters are calculated as follows:

a) the probability of threat:

$$P_{Th} = \sum_{n=1}^5 P_5 \tag{1}$$

the urgency of the threat:

$$Rel = \sum_{n=1}^x Rel_n \tag{2}$$

threat dynamics:

$$\begin{aligned} Dyn_i &= Dyn_2 - Dyn_1 \\ | Dyn_i > 0,05 \times Dyn_2 &\Rightarrow Dyn = 1 \\ | Dyn_i \cong \pm 0,05 \times Dyn_2 &\Rightarrow Dyn = 2 \\ | Dyn_i \leq - 0,05 \times Dyn_2 &\Rightarrow Dyn = 3 \end{aligned} \tag{3}$$

b) the probability of adverse effects (harm):

$$P_{cons} = \sum_{n=1}^5 P_5 \tag{4}$$

critical adverse effects (harm):

$$C = \sum_{n=1}^x C_n \tag{5}$$

adequacy of means to minimize harm or prevent its occurrence:

$$M = \sum_{n=1}^3 M_3 \tag{6}$$

"Price" of means of minimizing harm:

$$M_{pr} = \sum_{n=1}^x M_{pr_n} \tag{7}$$

danger of consequences:

$$H = \frac{C \times M_{pr}}{M} \tag{8}$$

c) security environment in the context of threat realization:

$$St = \sum_{n=1}^x St \in Env_n \tag{9}$$

$$O = \sum_{n=1}^x O \in Env_n \tag{10}$$

$$W = \sum_{n=1}^x W \in Env_n \tag{11}$$

$$Ch = \sum_{n=1}^x Ch \in Env_n \quad (12)$$

$$Env = \frac{St \times O}{W \times Ch} \quad (13)$$

$$| Env[6: 9] \Rightarrow Env = 3$$

$$| Env[2: 5] \Rightarrow Env = 2$$

$$| Env[0,11: 1] \Rightarrow Env = 1 \quad (14)$$

d) the level of threat:

$$Th = \frac{P_{th} \times Rel \times H \times Dyn}{Env} \quad (15)$$

The indicator of the level of threat, taking into account the given rating scale is in the range from 0.33 to 81 points; in the case when the specified indicator is less than 1 point, it is rounded to 1 point: **Th** [1:81].

The results of determining the level of threats to criminological security are aggregated by regions and / or by areas of national security with the calculation of the arithmetic mean of the indicators for each threat. Based on the consolidated indicators, threats are clustered by the level of: critical - if the level of threat in the region (at the operational service facility) is from 60 to 81 points; high - if the level of threat in the region (at the operational service facility) is from 39 to 59 points; medium - if the level of threat in the region (at the operational service facility) is from 18 to 38 points; low - if the level of threat in the region (at the operational service facility) is from 1 to 17 points.

Based on the results of the assessment, a passport is formed for each identified and assessed threat, in which the data of analytical research are summarized. Passports of identified and assessed threats are used to form a consolidated passport ("portfolio") of threats to criminological security.

When certifying threats to criminological security of a transnational nature, the parameters that characterize the security environment are analyzed and evaluated in the context of global trends in the implementation of relevant threats, as well as trends in their implementation in countries bordering Ukraine.

5. CONCLUSION

This msterial proposes a method of assessing threats to the criminological security of Ukraine, aimed at predicting the dynamics of their development, as well as modeling and supporting decisions in the field of crime prevention.

The assessment is carried out in three stages, by identifying threats to national security, analytical processing of information about such threats and determining their level. Based on the results of the assessment, a passport is formed for each identified and assessed threat, in which the data of analytical research are summarized. Threat passports and their totality -

"threat portfolio" - should be reflected in the program documents that implement the concept of criminological security risk management.

REFERENCES

- [1] Avanesov, G.A. (2006), *Concept and essence of criminological security*, Moskow, Russia, 495 p.
- [2] Artemov, A.V. and Kleimenov, M.P. (2004), "Foresight of criminological security", *Bulletin of Omsk University. Series: Law*. No. 1. pp. 113-115.
- [3] Babaev, M.M. (2009), "Criminological security as a conceptual basis and the main goal of criminal policy", *Aktual'nyye problemy ugolovnoogo prava, kriminologii, zakonodatel'stva i pravoprimereniya* [Actual problems of criminal law, criminology, legislation and law enforcement], materialy nauchno-prakticheskogo seminaru pamyati professora, doktora yuridicheskikh nauk, zasluzhennogo deyatelya nauki Rossiyskoy Federatsii A.S. Mikhlin [materials of a scientific and practical seminar in memory of Professor, Doctor of Law, Honored Scientist of the Russian Federation A.S. Mikhlin], October 20, 2008. Moskow, Russia, pp. 28-41.
- [4] Gorshenkov, G.G. (2009), *Anti-criminal security of the person*. Stavropol, Russia, 447 p.
- [5] Pleshakov, V.A. (2013), "Fundamentals of the theory of criminological security", *Aktual'nyye problemy teorii i praktiki protivodeystviya prestupnosti v sovremennoy Rossii* [Actual problems of the theory and practice of combating crime in modern Russia], materialy Mezhdunarodnoy nauchno-prakticheskoy konferentsii [materials of International scientific and practical conference], Moscow, Russia, pp. 65-75.
- [6] Skulish, C.D. and Prokofieva-Yanchylenko D.M. (2012), *Doctrine of criminological security: background and genesis*, Kiev, Ukraine, 252 p.
- [7] Shabanov, S.G (2001), *Criminological security of corporations and its forecasting*, Omsk, Russia, 155 p.
- [8] Sonali Sharma (2007), "Design and Implementation of Malware Detection Scheme", *International Journal of Computer Network and Information Security*, Vol. 10, No.8, pp. 58-66, 2018.DOI: 10.5815/ijcnis.2018.08.07
- [9] Vitlinskiy, V.V. (2003), "Conceptual ambush of riskology in financial activity" *Finansy Ukrayiny*, №3. pp. 3-9.
- [10] Zhdanov, Yu.A. (1976), "Trigger causality", *Voprosy filosofii*, No. 6. pp. 87-92.

- [11] Nekrasov, A.I. (1988), “Features of the manifestation of the transitivity of the causal links of historical events”, *Philosophical problems of modern natural science*, Issue 67, p. 100.
- [12] Alexandros Deligiannis and Charalampos Argyriou (2020), “Designing a Real-Time Data-Driven Customer Churn Risk Indicator for Subscription Commerce”, *International Journal of Information Engineering and Electronic Business*, Vol. 12, No. 4, pp. 1-14. DOI: 10.5815/ijieeb.2020.04.01
- [13] Arvind Panwar, Achin Jain and Manish Kumar (2016), “A Novel Probability based Approach for Optimized Prefetching”, *International Journal of Information Engineering and Electronic Business*, Vol. 8, No. 5, pp. 60-67. DOI: 10.5815/ijieeb.2016.05.08
- [14] Gururaj, H.L. Swathi, B.H. and Ramesh, B. (2018), “Threats, Consequences and Issues of Various Attacks on Online Social Networks”, *International Journal of Education and Management Engineering*, Vol. 8, No. 4, pp. 50-60. DOI: 10.5815/ijeme.2018.04.05
- [15] Martsynkovsky, D.A. Basic principles and methodology of risk management: Concept of acceptable risk, available at: www.rusregister.ru/upload/iblock/78b/part-2.pdf.18.
- [16] Clarke, R. (1995), “Situational crime prevention”, *Crime and Justice. Building a Safer Society: Strategic Approaches to Crime Prevention*, Vol. 19, pp. 91-150.
- [17] Richard V. Ericson “Ten uncertainties of risk-management approaches to security”, available at: www.ccja-acjp.ca/en/cjc/cjc/cjc4893.html
- [18] John Lea (2001), “Crime as governance: reorienting criminology, available at: <https://web.archive.org/web/20150307043033/http://www.bunker8.pwp.blueyonder.co.uk/misc/crimgov.htm>
- [19] Kaplan, Stanley and B. John Garrick (1981), “On The Quantitative Definition of Risk”, *Risk Analysis*, Vol.1, pp.11-27.
- [20] Leslie, W. Kennedy and Erin Gibbs Van Brunschot (2009), *The Risk in Crime*. 192 p.
- [21] Graycar, A. and Sidebottom, A. (2012), “Corruption and control: a corruption reduction approach”, *Journal of Financial Crime*, Vol. 19 (4), pp. 384-399.
- [22] Antonyan, Yu. M. (2004), *Criminology*, Selected lectures. Moskow, Russia, 448 p.