

UDC 004.056(045)

DOI:10.18372/1990-5548.89.21475

Valentyn Dokil

DYNAMIC MODEL FOR ASSESSING THE RECOVERABILITY OF AN INFORMATION AND COMMUNICATION SYSTEM IN SUPPORT OF CAPABILITY ASSESSMENT OF THE CYBER FORCES OF THE ARMED FORCES OF UKRAINE

National Defence University of Ukraine, Kyiv, Ukraine

E-mail: v.dokil.kkb@gmail.com ORCID: 0000-0002-6321-0940

Abstract—The article addresses dynamic assessment of the recoverability of an information and communication system after cyber impact in support of capability assessment of the Cyber Forces of the Armed Forces of Ukraine. The purpose of the study is to develop a dynamic model that represents system degradation, primary recovery, and controlled return of components to the protected operating state, and to form a normalized indicator for scenario comparison. The research method combines a three-state S–A–R system of differential equations, a conservation law for normalized states, a piecewise-constant description of cyber-impact intensity, numerical integration using an adaptive Runge–Kutta method, and scenario analysis. The model distinguishes components in the protected state, affected components, and components that have completed primary recovery but are still returning to normal operation. The integral recoverability indicator combines the final protected-state level, the maximum degradation depth, and normalized recovery time. A numerical example and four illustrative scenarios were used to examine model behaviour under weak, baseline, intensive, and enhanced-recovery conditions. The calculations show that an increase in cyber-impact intensity deepens degradation and prolongs recovery, whereas higher primary-recovery and controlled-return rates reduce the maximum affected share and shorten the time required to reach the specified operating threshold. In the baseline scenario, the maximum affected share is approximately 0.244, the recovery time is about 6.80 h, and the integral indicator is about 0.756; enhanced recovery provides the best result among the scenarios considered. The proposed model directly supports quantitative comparison of recovery conditions, identification of recovery-capability deficits, and substantiation of redundancy and recovery arrangements. The model parameters and weighting coefficients are illustrative and require calibration using exercise data, incident records, controlled tests, or simulation before practical application.

Keywords—Capability assessment, cyber defence, cyber forces, dynamic model, information and communication system, recoverability.

I. INTRODUCTION

Cyber impact can cause loss of availability, integrity, or functionality of information and communication system components. To assess the capabilities of Cyber Forces, it is crucial to determine not only the fact of compromise but also the depth of degradation, the speed of containment, and the time required for the system to return to a resilient state. The necessity of ensuring cybersecurity and the resilient functioning of critical information resources is defined by the national regulatory and strategic framework [1], [2]. A static pre- and post-incident assessment does not reflect the recovery trajectory: two assets may reach the same final state but differ in their maximum degradation depth, duration of degradation, and the amount of recovery resources required. For managerial comparison, a model is needed that describes transitions between functional states over time and provides a quantitative indicator of recoverability. Therefore, researching the dynamics of compromise and recovery of information and

communication systems to assess the capabilities of Cyber Forces is highly relevant.

II. LITERATURE REVIEW

NIST Cybersecurity Framework 2.0 and NIST incident-response recommendations treat recovery as an independent cyber-risk management function and associate it with recovery planning, prioritization, and restoration of critical functions [3], [4]. In a military context, these provisions should be combined with assessment of the functional resilience of information and communication systems.

In Ukrainian studies, V. Mashtalir, O. Huk, I. Tolmachov, and S. Faraon considered forecasting the degree of cyber impact on heterogeneous military information systems [5]. V. Horhulenko substantiated mathematical assessment of cyber-warfare effectiveness [6], while O. Huk, O. Permiakov, O. Nesterov, and T. Uvarova investigated approaches to assessing functional resilience of heterogeneous military information systems [7].

A systematic review by D. A. Sepúlveda Estay et al. demonstrates the heterogeneity of existing cyber-resilience assessment approaches and the shortage of universal quantitative procedures [8]. A. Annarelli, F. Nonino, and G. Palombi consider cyber resilience as a managed capability of a system to respond to disruption and restore functioning in its organizational context [9]. A. Kott and I. Linkov emphasize that quantitative cyber-resilience assessment should account for system behaviour over time during degradation and recovery [10]. Dynamic and hierarchical resilience approaches are also developed within the Impact-Wave Analogy [11] and experimental measurement of functionality restoration after cyberattacks [12].

Recent studies further strengthen the quantitative component. S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari summarized cyber-resilience strategies, metrics, and unresolved research issues [13]. H. Cho et al. proposed indicator normalization based on the area under the recovery curve [14], while S. M. Alhidaifi et al. developed a probabilistic model for quantitative resilience assessment of information infrastructure [15]. In the works of J. Järveläinen et al. [16] and R. P. Hilger [17], cyber resilience is treated as a dynamic capability to preserve functions, recover, and adapt. Mathematical representations of the temporal evolution of cyber resilience and dynamic indices were also developed by A. Bahmanova and N. Lace [18], [19]. Earlier, H. Tran et al. proposed a dynamic recovery model after malware propagation, confirming the appropriateness of describing cyber resilience through transitions between states [20].

Despite the development of these approaches, a dynamic model specifically oriented toward assessing the capabilities of the Cyber Forces of the Armed Forces of Ukraine within cyber defence tasks remains insufficiently formalized. Such a model should simultaneously represent the protected operating state, the affected state, and the recovered transitional state of an information and communication system, preserve state normalization, account for the temporal structure of cyber impact, and form an integral indicator from the final state, maximum degradation depth, and recovery duration

III. PROBLEM STATEMENT

The aim of the study is to develop a dynamic model for assessing the recoverability of an information and communication system after cyber impact in support of Cyber Forces capability assessment, to determine the parameters of its functioning, and to form a normalized integral indicator for scenario analysis and decision support. To achieve this aim, the following objectives are set:

- formalize transitions between the protected operating, affected, and recovered transitional states of the information and communication system;
- define a mathematical description of cyber-impact intensity, primary recovery, and controlled return to the protected operating state;
- form a normalized integral recoverability indicator that accounts for the final state, maximum degradation depth, and recovery time;
- conduct numerical and scenario analyses to assess model sensitivity to cyber-impact and recovery parameters.

IV. MATERIALS AND METHODS

A. Theoretical Basis of the Dynamic Model

To formalize the degradation and recovery processes, a three-component *S-A-R* model is proposed. The state $S(t)$ characterizes the proportion of information and communication system components operating in the protected operating state; $A(t)$ denotes the proportion of affected components; $R(t)$ denotes the proportion of components that have undergone primary recovery but are still returning to the fully normal operating state. All three variables are normalized and take values within the interval $[0,1]$. Hereinafter, $S(t)$, $A(t)$, and $R(t)$ denote the time trajectories of the corresponding system states, whereas $S(T)$, $A(T)$, and $R(T)$ denote their values at the final simulation time T .

The advantage of this representation is that it allows the degradation process, technical or functional recovery, and the subsequent return of recovered components to a stable operating state to be represented separately. The structure of transitions between the states is shown in Fig. 1.

Normalization condition: $S(t) + A(t) + R(t) = 1$

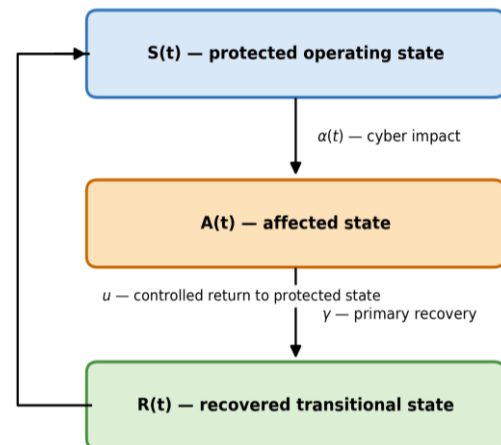


Fig. 1. State-transition scheme of the dynamic model of the information and communication system

The state dynamics are described by the following system of differential equations:

$$\begin{cases} \frac{ds}{dt} = -\alpha(t)S + uR, \\ \frac{dA}{dt} = \alpha(t)S - \gamma A, \\ \frac{dR}{dt} = \gamma A + uR. \end{cases} \quad (1)$$

where $S(t)$ is the proportion of components in the protected operating state; $A(t)$ is the proportion of affected components; $R(t)$ is the proportion of components in the recovered transitional state; $\alpha(t)$ is the cyber-impact intensity; γ is the rate of transition of affected components to the recovered state; and u is the rate of controlled return of recovered components to the protected operating state.

For the normalized model, the following conservation law holds:

$$S(t) + A(t) + R(t) = 1. \quad (2)$$

where $S(t)$, $A(t)$, and $R(t)$ are mutually exclusive normalized proportions of the system components. If the initial condition satisfies $S(0) + A(0) + R(0) = 1$, the sum of the states remains constant because the sum of the right-hand sides of system (1) is equal to zero.

To represent a cyber impact limited in time, it is appropriate to use a piecewise-constant law of intensity variation:

$$\alpha(t) = \begin{cases} \alpha_0, & 0 \leq t \leq t_a, \\ 0, & t > t_a, \end{cases} \quad (3)$$

where α_0 is the intensity of the active cyber impact; t_a is the duration of the active cyber-impact phase. After time t_a , no new degradation occurs within the baseline scenario, and the subsequent dynamics are determined by the parameters γ and u . This assumption is a simplification; however, it makes the model suitable for analysing an individual completed cyber-impact episode. Numerical integration of the system was performed using the fourth–fifth-order Runge–Kutta method with an adaptive step size and local error control over a 24-hour time horizon.

B. Formation of the Integral Recoverability Indicator

Rather than using only the proportion $R(T)$, it is appropriate to account for $S(T)$ in the final result, because the successful return of components from $R(t)$ to the protected operating state reduces $R(t)$, while actually indicating an improvement in the

system state. Therefore, for a compact representation of the integral index, the following notation is introduced:

$$S_T = S(T), \quad A_m = A_{\max}, \quad \tau_r = \min\left(1, \frac{t_{\text{rec}}}{t_{\text{rec}}^{\max}}\right).$$

The integral dynamic recoverability index is defined by equation:

$$I_{\text{dun}} = \eta_1 S_T + \eta_2 (1 - A_m) + \eta_3 (1 - \tau_r), \quad (4)$$

where I_{dun} is the integral dynamic recoverability index; S_T is the proportion of components in the protected operating state at the final observation time T ; $A_m = A_{\max}$ is the maximum proportion of affected components over the interval $[0, T]$; τ_r is the normalized recovery-time indicator; τ_{rec} is the time required after the end of the active cyber-impact phase to meet the specified recovery criterion; $\tau_{\text{rec}}^{\max}$ is the maximum allowable recovery time; η_1 , η_2 , and η_3 are weighting coefficients. The normalized recovery-time indicator τ_r equals 0 when the recovery criterion is achieved at the end of the active phase and approaches 1 as the recovery time reaches the maximum allowable value $\tau_{\text{rec}}^{\max}$.

In the numerical calculations, the recovery criterion is defined as achieving $S(t) \geq 0.90$. The indicator $A_{\max}$ characterizes the maximum depth of degradation, whereas τ_{rec} characterizes the time required for the system to return to the specified level of operation.

For the weighting coefficients, the following condition holds:

$$\eta_1 + \eta_2 + \eta_3 = 1, \quad \eta_i \geq 0, \quad (5)$$

where η_1 determines the weight of the final protected operating state, η_2 determines the weight associated with minimizing the maximum degradation depth, and η_3 determines the weight of the recovery-time characteristic. For non-negative weights and normalized components, $I_{\text{dun}} \in [0, 1]$. In the illustrative example, $\eta_1 = 0.40$, $\eta_2 = 0.30$, and $\eta_3 = 0.30$ are used. These weights are illustrative; for practical application, they should be substantiated based on expert assessment and/or empirical calibration.

C. Model Application Algorithm

For practical application of the proposed model, the sequence of computational steps is formalized as an algorithm (Fig. 2). It includes defining the object

of assessment, specifying the input parameters, numerically integrating system (1), determining the dynamic indicators, calculating the integral indicator, and interpreting the results to support decision-making.

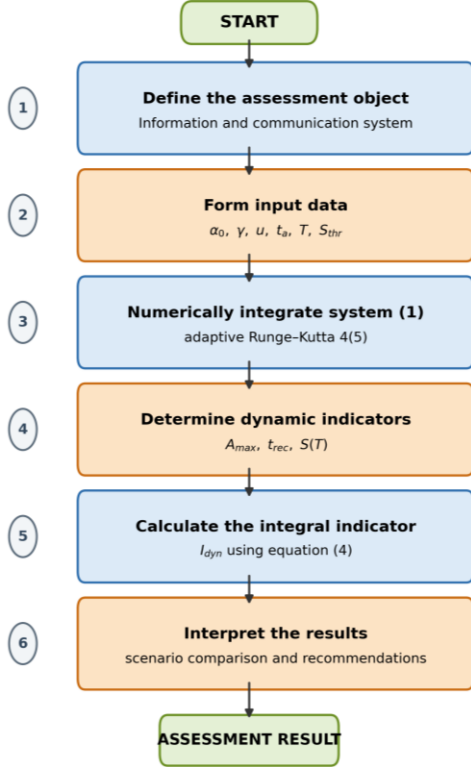


Fig. 2. Algorithm for applying the dynamic recoverability assessment model of an information and communication system

V. RESULTS

A. Numerical Example of the Model Application

Consider an illustrative baseline scenario: $S(0)=1$, $A(0)=0$, $R(0)=0$; the active cyber-impact intensity $\alpha_0=0.20 \text{ h}^{-1}$; the duration of the active phase $t_a=4 \text{ h}$; the rate of transition to the recovered state $\gamma=0.45 \text{ h}^{-1}$; the rate of controlled return to normal operation $u=0.30 \text{ h}^{-1}$. The simulation horizon is $T=24 \text{ h}$, and the maximum allowable recovery time is $t_{\text{rec}}^{\text{max}}=12 \text{ h}$.

Numerical integration of system (1) shows that the maximum proportion of affected components is $A_{\text{max}} \approx 0.244$. After the end of the active phase, the system reaches the level $S(t) \geq 0.90$ in approximately $t_{\text{rec}} \approx 6.80 \text{ h}$, while at the end of the simulation horizon $S(T) \approx 0.998$. According to equation (4), $I_{\text{dyn}} \approx 0.756$.

The dynamics of $S(t)$, $A(t)$, and $R(t)$ for the baseline scenario are shown in Fig. 3.

Figure 3 shows that the proportion of affected components $A(t)$ increases during the active cyber-impact phase and subsequently decreases as a result of recovery. At the same time, $R(t)$ initially accumulates recovered components and then decreases as they return to the protected operating state $S(t)$. This confirms the appropriateness of using $S(T)$, rather than $R(T)$, as the final-state component of the integral index.

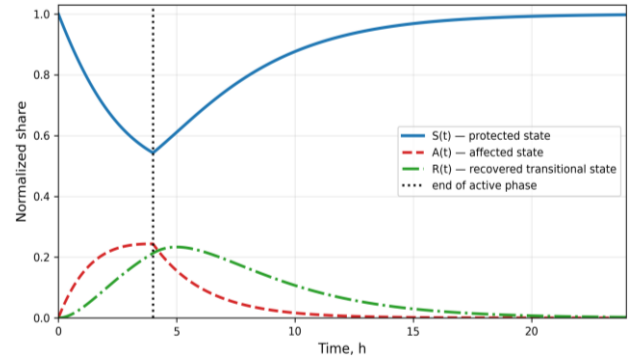


Fig. 3. State dynamics of the information and communication system for the baseline scenario

B. Scenario Analysis

To examine model sensitivity, four scenarios are considered: weak cyber impact, baseline, intensive cyber impact, and enhanced recovery. In all scenarios, the active phase lasts 4 h, while the differences are determined by α_0 , γ , and u . Scenario parameters and results are presented in Table I.

TABLE I COMPARISON OF DYNAMIC-RECOVERABILITY SCENARIOS

Scenario	α_0, h^{-1}	γ, h^{-1}	u, h^{-1}
Weak cyber impact	0.15	0.45	0.30
Baseline	0.20	0.45	0.30
Intensive cyber impact	0.30	0.40	0.25
Enhanced recovery	0.20	0.65	0.50

Simulation Results

Scenario	A_{max}	t_{rec}, h	$S(24)$	I_{dyn}
Weak cyber impact	0.202	6.05	0.998	0.788
Baseline	0.244	6.80	0.998	0.756
Intensive cyber impact	0.328	9.25	0.992	0.667
Enhanced recovery	0.193	3.80	1.000	0.847

The results in Table I demonstrate a nonlinear dependence of recoverability on the model parameters. An increase in cyber-impact intensity simultaneously increases A_{max} and t_{rec} , which leads to a decrease in I_{dyn} . In contrast, increases in γ and u

reduce the maximum proportion of affected components and shorten the time required to return to the specified level $S(t) = 0.90$.

A comparison of the $S(t)$ trajectories for the four scenarios is shown in Fig. 4.

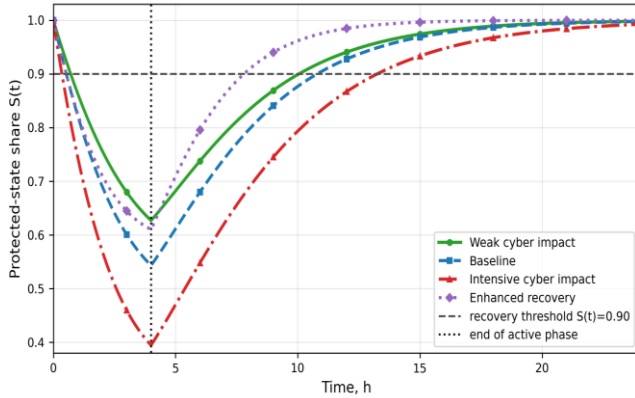


Fig. 4. Comparison of system return to the protected operating state under different scenarios

In Figure 4, the scenarios are distinguished by curve colour: weak cyber impact, the baseline scenario, intensive cyber impact, and enhanced recovery are presented as separate trajectories. The horizontal dashed line corresponds to the recovery criterion $S(t) = 0.90$, while the vertical line marks the end of the active cyber-impact phase at $t = 4$ h. The slowest return to the specified level is observed under intensive cyber impact, whereas the fastest return occurs under the enhanced-recovery scenario.

VI. DISCUSSION

The proposed model does not attempt to reproduce every process occurring in a real information and communication system. However, it provides an analytically transparent relationship among impact intensity, recovery rate, controlled return to normal operation, and the integral recoverability assessment. Its advantage is the ability to separate three different characteristics: the final functional state, maximum degradation depth, and recovery duration.

The scientific novelty lies in formalizing the dynamic recoverability of an information and communication system as a component of Cyber Forces capability assessment through a combination of the three-state S – A – R model and an integral indicator that simultaneously accounts for the final recovery level, maximum degradation depth, and time required to return to a specified operating level.

Parameters α_0 , γ , and u can be identified from cyber-exercise results, retrospective incident analysis, controlled testing, and simulation. In the presence of

repeated cyber-impact waves, non-stationary parameters, or different component classes, the model should be extended to systems with time-varying coefficients or to multicomponent models.

The parameters and weighting coefficients used in the numerical and scenario analyses are illustrative. Practical application requires identification and calibration using data from a specific information and communication system, cyber exercises, retrospective incident analysis, or controlled testing.

Practical recommendations for model application:

- determine $\alpha(t)$ separately for the active cyber-impact phase and after its completion, without mixing the intensity of new damage with the recovery process;
- estimate γ from the actual time required for localization and primary recovery of components, and u from the rate at which verified components return to the protected operating state;
- set the recovery threshold and $t_{\text{rec}}^{\text{max}}$ according to the criticality of the information and communication system and continuity requirements;
- conduct scenario analysis before and after changes in redundancy, recovery-force composition, or response procedures;
- use I_{dun} together with the absolute values of A_{max} and t_{rec} , because the same integral index may result from different combinations of dynamic characteristics.

VII. CONCLUSIONS AND FUTURE RESEARCH

A dynamic S – A – R model for assessing the recoverability of an information and communication system after cyber impact has been developed. It describes transitions among the protected operating, affected, and recovered states. The model preserves the normalized sum of states and makes it possible to account separately for cyber-impact intensity, recovery rate, and controlled return to normal operation.

The formation of the integral indicator I_{dun} has been refined: its final-state component should be defined through $S(T)$, rather than $R(T)$, because a decrease in $R(t)$ may result from successful return of recovered components to the protected state. The numerical example and scenario analysis show that increasing α_0 worsens A_{max} and t_{rec} , whereas increasing γ and u shortens recovery time and increases the integral assessment.

Future research should focus on identifying model parameters from real data, accounting for

repeated cyber-impact waves, different component criticality levels, time-varying coefficients, and integrating the dynamic module with other components of a comprehensive methodology for assessing Cyber Forces capabilities.

Conflict of interest. The author declares no financial, personal, authorship-related, or other conflict of interest that could have influenced the research or the results presented in this article.

Funding. The study was conducted without financial support.

Use of artificial intelligence tools. OpenAI ChatGPT was used as an auxiliary tool for language editing, translation support, technical formatting, preparation of figures and tables, and bibliographic checking. The scientific concept, mathematical model, calculations, interpretation of results, conclusions, and final approval of the manuscript are the responsibility of the author.

REFERENCES

- [1] Verkhovna Rada of Ukraine (2017) Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the Basic Principles of Cybersecurity in Ukraine], Law of Ukraine No. 2163-VIII, 5 October. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19> (Accessed: 8 September 2026) [in Ukrainian].
- [2] President of Ukraine (2021) Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku ‘Pro Stratehiiu kiberbezpeky Ukrainy’ [On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 ‘On the Cybersecurity Strategy of Ukraine’], Decree No. 447/2021, 26 August. Available at: <https://zakon.rada.gov.ua/laws/show/447/2021> (Accessed: 8 September 2026) [in Ukrainian].
- [3] C. Pascoe, S. Quinn, and K. Scarfone, (2024) The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Papers, CSWP 29. <https://doi.org/10.6028/NIST.CSWP.29>.
- [4] A. Nelson, S. Rekhi, M. Souppaya, and K. Scarfone, (2025) Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST Special Publication 800-61 Rev. 3. <https://doi.org/10.6028/NIST.SP.800-61r3>.
- [5] V. V. Mashtalir, O. M. Huk, I. I. Tolmachov, and S.I. Faraon, “Prohnozuvannia stupeniu kibervplyvu na heterohenni informatsiini systemy viiskovoho pryznachennia z urakhuvanniam yoho evoliutsii,” [Forecasting the degree of cyber impact on heterogeneous military information systems considering its evolution], *Suchasni informatsiini tekhnologii u sferi bezpeky ta oborony*, 48(3), pp. 147–156, 2023. <https://doi.org/10.33099/2311-7249/2023-48-3-147-156> [in Ukrainian].
- [6] V. A. Horhulenکو, “Metodyka otsiniuvannia efektyvnosti vedennia kiberborotby v interesakh zastosuvannia uhrupovan viisk (syl) v operatsiakh,” [Method for assessing the effectiveness of cyber warfare in support of the employment of troop (force) groupings in operations], *Suchasni informatsiini tekhnologii u sferi bezpeky ta oborony*, 55(1), pp. 100–107, 2026. <https://doi.org/10.33099/2311-7249/2026-55-1-100-107> [in Ukrainian].
- [7] O. M. Huk, O. Yu. Permiakov, O. V. Nesterov, and T. A. Uvarova, “Analiz isnuichykh pidkhodiv shchodo otsiniuvannia funktsionalnoi stiikosti heterohennykh informatsiinykh system viiskovoho pryznachennia,” [Analysis of existing approaches to assessing the functional resilience of heterogeneous military information systems], *Suchasni informatsiini tekhnologii u sferi bezpeky ta oborony*, 39(3), pp. 39–44, 2020. <https://doi.org/10.33099/2311-7249/2020-39-3-39-44> [in Ukrainian].
- [8] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, and C. D. Jensen, “A systematic review of cyber-resilience assessment frameworks,” *Computers & Security*, 97, 101996, 2020. <https://doi.org/10.1016/j.cose.2020.101996>.
- [9] A. Annarelli, F. Nonino, and G. Palombi, “Understanding the management of cyber resilient systems,” *Computers & Industrial Engineering*, 149, 106829, 2020. <https://doi.org/10.1016/j.cie.2020.106829>.
- [10] A. Kott, and I. Linkov, “To Improve Cyber Resilience, Measure It,” *Computer*, 54(2), pp. 80–85, 2021. <https://doi.org/10.1109/MC.2020.3038411>.
- [11] J. K. Osborn, and D. A. Sepulveda-Estay, “A Comparative Analysis of the Impact-Wave Analogy Cyber-Resilience Framework,” 2021 *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2021, pp. 333–337. <https://doi.org/10.1109/IEEM50564.2021.9672842>.
- [12] M. J. Weisman, A. Kott, J. E. Ellis, B. J. Murphy, T. W. Parker, S. Smith, and J. Vandekerckhove, “Quantitative Measurement of Cyber Resilience: Modeling and Experimentation,” *ACM Transactions on Cyber-Physical Systems*, 9(1), pp. 1–25, 2025. <https://doi.org/10.1145/3703159>.
- [13] S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, “A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions,” *ACM Computing Surveys*, 56(8), Article 196, pp. 1–48, 2024. <https://doi.org/10.1145/3649218>.
- [14] H. Cho, J.-H. Sung, H.-J. Kang, J. Jang, and D. Shin, “Quantifying Cyber Resilience: A Framework Based on Availability Metrics and AUC-Based

- Normalization,” *Electronics*, 14(12), 2465. <https://doi.org/10.3390/electronics14122465>.
- [15] S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, “Cyber resilience quantification: A probabilistic estimation model for IT infrastructure,” *Reliability Engineering & System Safety*, 265, 111473, 2026. <https://doi.org/10.1016/j.res.2025.111473>.
- [16] J. Järveläinen, D. Dang, M. Mekkanen, and T. Vartiainen, “Towards a framework for improving cyber security resilience of critical infrastructure against cyber threats: a dynamic capabilities approach,” *Journal of Decision Systems*, 34(1), Article 2479546, 2025. <https://doi.org/10.1080/12460125.2025.2479546>.
- [17] R. P. Hilger, “From cybersecurity to cyber resilience: a systemic and scalable approach for improving resilience and adaptive capacity,” *Journal of Cybersecurity*, 12(1), tyag011, 2026. <https://doi.org/10.1093/cybsec/tyag011>.
- [18] A. Bahmanova, and N. Lace, “Modelling Cyber Resilience in SMEs as a Socio-Technical System: A Systemic Approach to Adaptive Digital Risk Management,” *Systems*, 14(2), Article 151, 2026. <https://doi.org/10.3390/systems14020151>.
- [19] A. Bahmanova, and N. Lace, “Predictive Cyber Risk Analytics and Computational Risk Metrics for SME Cyber Resilience Using Time-Series Modelling,” *Mathematics*, 14(16), Article 2963, 2026. <https://doi.org/10.3390/math14162963>.
- [20] H. Tran, E. Campos-Nanez, P. Fomin, and J. Wasek, “Cyber resilience recovery model to combat zero-day malware attacks,” *Computers & Security*, 61, pp. 19–31, 2016. <https://doi.org/10.1016/j.cose.2016.05.001>.

Received: July 19, 2026

Accepted: August 12, 2026

Published: September 18, 2026

Dokil Valentyn. ORCID 0000-0002-6321-0940. Colonel. Adjunct.

Department of Cyber Warfare, Institute of Information and Communication Technologies and Cyber Defence, National Defence University of Ukraine, Kyiv, Ukraine.

Research area: Cyber Forces capability assessment, cyber defence, cyber resilience of information and communication systems.

Publications: 7.

E-mail: v.dokil.kkb@gmail.com

В. М. Докіль. Динамічна модель оцінювання відновлюваності інформаційно-комунікаційної системи в інтересах оцінювання спроможностей Кіберсил Збройних Сил України

У статті розглянуто динамічне оцінювання відновлюваності інформаційно-комунікаційної системи після кібервпливу в інтересах оцінювання спроможностей Кіберсил Збройних Сил України. Метою дослідження є розроблення динамічної моделі, яка відображає ураження, первинне відновлення та кероване повернення компонентів до штатного захищеного стану, а також формування нормованого показника для сценарного порівняння. Методика дослідження ґрунтується на тристанній S–A–R-системі диференціальних рівнянь, законі збереження суми нормованих станів, кусково-сталому описі інтенсивності кібервпливу, чисельному інтегруванні методом Рунге–Кутти з адаптивним кроком і сценарному аналізі. У моделі розрізняються компоненти у штатному захищеному стані, уражені компоненти та компоненти, які пройшли первинне відновлення, але ще повертаються до повного штатного режиму. Інтегральний показник відновлюваності поєднує кінцевий рівень штатного стану, максимальну глибину ураження та нормований час відновлення. Для перевірки поведінки моделі використано числовий приклад і чотири демонстраційні сценарії: слабкий кібервплив, базовий режим, інтенсивний кібервплив та посилене відновлення. Результати показують, що зростання інтенсивності кібервпливу збільшує максимальну частку уражених компонентів і подовжує відновлення, тоді як підвищення інтенсивностей первинного відновлення та керованого повернення зменшує глибину деградації і скорочує час досягнення заданого рівня функціонування. У базовому сценарії максимальна частка уражених компонентів становить приблизно 0,244, час відновлення – близько 6,80 год, а інтегральний показник – близько 0,756; найкращий результат серед розглянутих сценаріїв забезпечує посилене відновлення. Запропонована модель дає змогу кількісно порівнювати сценарії, виявляти дефіцит відновлювальної спроможності та обґрунтовувати резервування й організацію відновлення. Параметри моделі та вагові коефіцієнти мають демонстраційний характер і для практичного застосування потребують калібрування за даними кібернавчань, журналів інцидентів, контрольованих випробувань або імітаційного моделювання.

Ключові слова: відновлюваність, динамічна модель, інформаційно-комунікаційна система, кібероборона, кіберсили, оцінювання спроможностей.

Докіль Валентин Миколайович. ORCID 0000-0002-6321-0940. Полковник. Ад’юнкт.

Кафедра кіберборотьби, Інститут інформаційно-комунікаційних технологій та кібероборони, Національний університет оборони України, Київ, Україна.

Напрямок наукової діяльності: оцінювання можливостей кіберсил, кіберзахист, кіберстійкість інформаційно-комунікаційних систем.

Кількість публікацій: 7.

E-mail: v.dokil.kkb@gmail.com