

<https://doi.org/10.31891/2307-5732-2026-365-92>

УДК 621.39, 004.75, 004.94

**ПЕТРОСЯН ЛЕВОН**

Державний університет «Київський авіаційний інститут»

<https://orcid.org/0009-0006-0551-9137>

e-mail: [2147491@stud.kai.edu.ua](mailto:2147491@stud.kai.edu.ua)

## **АНАЛІЗ ІНТЕГРАЦІЇ ТЕХНОЛОГІЇ NETWORK DIGITAL TWIN У КОНЦЕПТУАЛЬНУ РАМКУ ОЦІНЮВАННЯ РЕЗИЛЬЄНТНОСТІ ТЕЛЕКОМУНІКАЦІЙНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ ЗА ПРИНЦИПОМ BUILD BACK BETTER**

У роботі проаналізовано інтеграцію технології Network Digital Twin (NDT) у концептуальну рамку оцінювання резильєнтності телекомунікаційної інфраструктури України за принципом Build Back Better (BBB). Гіпотеза полягає у тому, що така рамка здатна подолати розрив між реактивним точковим відновленням та системним підходом до прийняття рішень в умовах конфлікту. На основі синтезу 19 рецензованих та інституційних джерел визначено шість метрик операційної резильєнтності для телекомунікаційних мереж: доступність, зв'язність, відмовостійкість, час відновлення, резервування та енергетична автономність. Архітектуру NDT адаптовано із концепцією Digital Risk Twin (DRT) для умов конфлікту, розроблено замкнений управлінський цикл прийняття рішень. Рамку орієнтовано на специфіку українського телекомунікаційного ринку з урахуванням вимог НКЕК та нормативних документів (ДСТУ ETSI EN 302 217). Працездатність рамки продемонстровано на спрощеному числовому прикладі (гіпотетична мережа із 7 вузлів) та двох якісних сценаріях. Рамка є концептуальною та потребує емпіричної валідації.

**Ключові слова:** цифровий двійник мережі, резильєнтність, телекомунікаційна інфраструктура, відновлення з покращенням, критична інфраструктура.

**PETROSIAN LEVON, GNATIUK VIKTOR**

State University «Kyiv Aviation Institute»

## **ANALYSIS OF NETWORK DIGITAL TWIN TECHNOLOGY INTEGRATION INTO THE CONCEPTUAL FRAMEWORK FOR RESILIENCE ASSESSMENT OF UKRAINE'S TELECOMMUNICATIONS INFRASTRUCTURE BASED ON THE BUILD BACK BETTER PRINCIPLE**

Since February 2022 Ukraine's telecom infrastructure has suffered damages exceeding USD 2.2 billion, with recovery needs estimated at USD 5.86 billion. Current restoration practices remain largely reactive: damaged network elements are replaced on a case-by-case basis without systematic resilience assessment or data-driven prioritisation at the network level. This approach leads to repeated failures in the same segments, inefficient allocation of limited donor funding, and inability to account for cross-sectoral interdependencies, particularly between telecommunications and energy infrastructure. The Build Back Better (BBB) principle, endorsed by international frameworks, calls for using the recovery phase to enhance long-term resilience rather than merely restoring pre-disaster conditions. However, without a quantitative analytical tool, BBB remains a declarative guideline that is difficult to operationalise. This paper analyses the integration of Network Digital Twin (NDT) technology into a conceptual framework for resilience assessment and BBB-driven recovery planning for conflict-affected telecom infrastructure of Ukraine. The hypothesis posits that such a framework can bridge the gap between reactive point-by-point restoration and a systematic approach to decision-making under conflict conditions. Based on a synthesis of 19 peer-reviewed and institutional sources, the study defines six operational resilience metrics adapted for telecom networks: availability, connectivity, fault tolerance, time-to-recover, redundancy, and energy autonomy. The paper adapts an NDT architecture augmented with the Digital Risk Twin (DRT) concept for conditions of incomplete data and ongoing conflict, and specifies a closed-loop decision cycle: data collection, NDT modelling, what-if scenario simulation, resilience-driven prioritisation, BBB intervention, and continuous twin updating. The framework is contextualised for the Ukrainian telecom market, taking into account the regulatory requirements of NCEC and national standards (DSTU ETSI EN 302 217). Two qualitative scenarios illustrate the framework's application to cascading power-telecom failures and backbone link destruction. A simplified numerical example on a hypothetical 7-node network demonstrates the computational viability of the proposed management cycle and the quantitative advantage of BBB interventions over minimal restoration. A comparative analysis of reactive versus proactive (NDT+BBB) recovery approaches is presented. The principal contribution is the novel integration of NDT, resilience metrics, and BBB into a unified decision-support methodology for post-conflict telecom recovery. The framework remains conceptual and requires empirical validation through pilot deployment.

**Keywords:** network digital twin, resilience, telecommunications infrastructure, build back better, critical infrastructure.

Стаття надійшла до редакції / Received 26.02.2026

Прийнята до друку / Accepted 11.04.2026

Опубліковано / Published 28.05.2026



This is an Open Access article distributed under the terms of the [Creative Commons CC-BY 4.0](https://creativecommons.org/licenses/by/4.0/)

© Петросян Левон

### **Постановка проблеми у загальному вигляді**

#### **та її зв'язок із важливими науковими чи практичними завданнями**

Повномасштабне вторгнення Російської Федерації в Україну завдало значних збитків критичній інфраструктурі (СІ) країни. За оцінкою міжнародного союзу електрозв'язку (ІТУ), станом на серпень 2022 року приблизно 20 % телекомунікаційної інфраструктури було пошкоджено або зруйновано, 11 % базових станцій не функціонували, а прямі збитки оцінювалися у 0,71 млрд доларів США [1]. 4-та швидка оцінка збитків і потреб Світового банку (RDNA4) оцінює загальні збитки телекомунікаційного сектору у 2,24 млрд доларів, а потреби у відновленні - у 5,86 млрд доларів на 10-річний горизонт [2]. Оцінки (ІТУ) щодо реабілітації мовленнєвих станцій показують, що реконструкція за принципом Build Back Better (BBB, відновлення з покращенням) може коштувати від мільйонів до сотень мільйонів доларів залежно від концепції [3]. Цифровий профіль країни фіксує

високе проникнення мобільного зв'язку та плани інвестицій операторів (Київстар, Vodafone Україна, lifecell) до 2030 року [4]. Аналіз CSS ETH Zürich підкреслює, що телекомунікації є визначальним сектором CI, а їхня резильєнтність визначає функціонування суспільства в умовах конфлікту [5].

Переважає більшість поточних зусиль із відновлення має реактивний характер: об'єкти ремонтується без системного аналізу мережевої зв'язності та довгострокової вразливості. Принцип BBB, інтегрований у методологію RDNA [2], передбачає підвищення функціональності та стійкості, а не відтворення доконфліктного стану. Однак без інструменту кількісної оцінки резильєнтності BBB залишається декларативним: відсутній механізм обґрунтованого вибору між конкуруючими інтервенціями. Практичний гід Світового банку [14] систематизує заходи підвищення стійкості телекомунікацій (автономне живлення, підземні кабелі, резервування), проте не пропонує інструменту для кількісної пріоритезації на рівні мережі та оцінки каскадних ефектів. Технологія Network Digital Twin (NDT) — віртуальне представлення мережевої інфраструктури, синхронізоване з визначеною частотою [6]. Саме вона, ймовірно, відкриває перспективи для подолання цього розриву, дозволяючи моделювати поведінку мережі та оптимізувати рішення на основі даних.

#### Аналіз досліджень та публікацій

Концепція BBB, закріплена у Сендайській рамковій програмі, передбачає використання фази відновлення як можливості для підвищення стійкості. R. Der Sarkissian та ін. на прикладі відновлення CI після урагану Ірма запропонували формулу BBB CI як функцію трьох компонентів: Build-Back-resilient, Build-Back-sustainable, Build-Back-upgraded [7] і показали, що перехід до підземних мереж одночасно підвищує стійкість та якість послуг. S.-A. Mitoulis та ін. розширили рамку на контекст конфлікту, виділивши три типи резильєнтності: проактивну (resilience by design, RBD), адаптивну (resilience by assessment, RBA) та реактивну постконфліктну (resilience by intervention, RBI), наголошуючи на ролі дистанційних спостережень для пріоритезації [8]. Саме перехід від RBI до RBD, на нашу думку, є центральною ідеєю запропонованої рамки. Це задає логіку всього подальшого аналізу.

Згідно з IOWN Global Forum, NDT - це віртуальне представлення мережевої інфраструктури, що об'єднує гетерогенні дані та аналітичні моделі [6]. IOWN GF виокремлює вісім категорій застосування NDT і серед ключових бізнес-цінностей окремо виділяє резильєнтність: моделювання сценаріїв збоїв та виявлення «чорних лебедів». E. Brucherseifer та ін. запропонували концептуальну рамку Digital Twin (DT) для CI, що підтримує чотири фази циклу резильєнтності - антиципацію, моніторинг, реагування та навчання - завдяки двоспрямованому зв'язку між фізичним об'єктом та віртуальною реплікою [9]. Ця рамка, ймовірно, застосовна до різних типів CI, включаючи телекомунікації.

A. M. Braik та M. Koliou запропонували модель DT для відновлення електромереж із урахуванням взаємозалежностей із дорожньою мережею, поєднуючи фізичні та керовані даними (data-driven) моделі через динамічні баєсівські мережі [10]. S. Ghaffarian увів концепцію Digital Risk Twin (DRT) для управління ризиками катастроф із гібридним збором даних та участю експерта в циклі рішень (human-in-the-loop), що зберігає працездатність при деградації цифрової інфраструктури [11]. H. Liang та ін. застосували глибоке навчання з підкріпленням (Deep Reinforcement Learning, DRL) для оптимізації послідовності відновлення CI з мінімізацією інтегральної метрики Loss of Resilience (LoR) [12].

I. Aviv та U. Ferri показали часткову ефективність кібератак на телеком-інфраструктуру України (AcidRain проти Viasat) завдяки швидкому кіберзахисту та використанню LEO-супутників Starlink як резерву [13]. Практичний гід Світового банку узагальнює заходи стійкості (автономне живлення, підземні кабелі, резервування) [14], I. C. Ferruela акцентує технологічні інновації та міжсекторальну координацію [15], а P. Jiang та ін. описують прогалини у фінансуванні/регулюванні й пропонують чотирифазну модель телеком-резильєнтності [16]. L. Weedage та ін. довели, що національний роумінг підвищує покриття при відмові однієї з мереж [17].

Питання специфічної цінності NDT порівняно з наявними інструментами має вирішальне значення для обґрунтування рамки. NDT, за визначенням [6] та [9], поєднує двоспрямовану синхронізацію між фізичною мережею та моделлю, інтеграцію гетерогенних даних (топологія, телеметрія, середовище) та повномасштабний сценарний аналіз типу «що, якщо» (what-if) на рівні всієї мережі, включно з міжсекторальними залежностями (телеком–енергетика–транспорт) [10]. NMS/OSS (Network Management System / Operations Support Systems) переважно працюють із поточним станом, GIS - зі спрощеною просторовою репрезентацією, а ABM (Agent-Based Modeling) вимагає значної параметризації. Обмеження NDT: високі початкові витрати, вимоги до якості даних і додаткові кіберризики [13].

Наш аналіз засвідчує: NDT переважно досліджується як інструмент оперативного управління мережею, а не оцінки резильєнтності. DT-підходи розроблено для енергетики [10] та транспорту [18], але не телекомунікацій. Але й рамки BBB [7] та conflict-resilience [8] досі не інтегровано з NDT. У відібраній вибірці джерел (2021–2025) не виявлено досліджень, що поєднують NDT як інструмент оцінки резильєнтності телеком-інфраструктури в контексті BBB-відновлення в умовах конфлікту. Мета цієї статті — заповнити цей розрив (хоча й на концептуальному рівні).

#### Формулювання цілей статті

**Метою статті є:** розробка концептуальної рамки інтеграції NDT в оцінку резильєнтності телекомунікаційної інфраструктури України за принципом BBB. Гіпотеза полягає у тому, що така рамка здатна, на рівні якісної аргументації, подолати розрив між реактивним точковим відновленням та системним підходом до прийняття рішень в умовах конфлікту. Внески: C1 - концептуальна рамка інтеграції NDT в оцінку резильєнтності з формалізацією шести метрик; C2 - порівняльний аналіз реактивного та проактивного підходів (Табл. 1); C3 - адаптована архітектура NDT для контексту постконфліктного відновлення (рис. 1), побудована на

основі класифікації сценаріїв застосування NDT IOWN Global Forum (Network Digital Twin Use Case Classification, ver. 2.0) [6]; C4 - замкнений управлінський цикл із визначенням акторів, даних та інструментів для кожного кроку (Табл. 3). Синергетичний ефект інтеграції: NDT без BBB лише моделює мережу «як є»; BBB без NDT залишається декларацією; їхнє поєднання створює можливість кількісно обґрунтованих BBB-інтервенцій із пріоритизацією за метриками резильєнтності.

#### Виклад основного матеріалу

Аналіз реалізовано методом синтезу концептуальної рамки (conceptual framework synthesis), що є різновидом design science research. Процедура включала систематичний відбір 19 джерел за критеріями релевантності (NDT/DT, resilience, BBB, telecom, conflict/disaster), рецензованості та актуальності (2021–2025), а також кодування ключових концептів (метрики, архітектурні рівні, фази циклу, типи інтервенцій) із кожного джерела. На наступних етапах ми виконали синтез метрик резильєнтності з [8], [14], [15], [17], побудову архітектури NDT на основі [6] та [9] з адаптацією до контексту конфлікту, розробку управлінського циклу на основі фазової моделі [9] та пріоритизації [18] і верифікацію через якісні сценарії. Рамка є концептуальною і не претендує на емпіричну валідованість; обмеження цього підходу висвітлюються у розділі із обговореннями.

Резильєнтність (resilience) телекомунікаційної інфраструктури визначається як здатність мережі запобігати інцидентам, протистояти їм, пом'якшувати вплив та відновлюватися, підтримуючи прийнятний рівень обслуговування [15]. У даній роботі термін «резильєнтність» вживається послідовно; «стійкість» застосовується лише у сенсі sustainability. На основі джерел [8], [14], [15], [17] виділено та формалізовано шість метрик:

Доступність (Availability, A):

$$A = \frac{T_{up}}{T_{total}}, \quad (1)$$

де  $T_{up}$  - сумарний час функціонування мережевих елементів,  $T_{total}$  - загальний час спостереження. Джерело даних: телеметрія NMS. Порогове значення:  $A \geq 0,99$  для магістральних вузлів [14], що узгоджується з нормами ДСТУ ETSI EN 302 217 щодо доступності радіорелейних ліній. Це порогове значення наведено як орієнтир і підлягає калібруванню для класів мережевих елементів у межах пілотної валідації.

Зв'язність (Connectivity, C):

$$C = \frac{P_{connected}}{P_{total}}, \quad (2)$$

де  $P_{connected}$  - кількість пар вузлів із наскрізним з'єднанням,  $P_{total}$  - загальна кількість пар. Вимірюється на графі мережі при частковій деградації [17]. Для оцінювання на сервісному рівні (користувачі/трафік) метрику C доцільно доповнювати показниками покриття/обслуговування населення (напр., FDP/FSP) та QoS-метриками з телеметрії [17].

Відмовостійкість (Fault Tolerance, FT): частка вузлів, видалення яких не призводить до втрати зв'язності мережі. Формально:

$$FT = 1 - \frac{|V_{critical}|}{|V|}, \quad (3)$$

де  $V_{critical}$  - множина критичних вузлів (articulation points графа мережі). Обчислюється алгоритмами теорії графів [10], [12]. Метрика характеризує здатність мережі протистояти одиничним відмовам на топологічному рівні; для багатокомпонентних відмов можливі розширення (k-connectivity, потокові підходи (flow-based)).

Час відновлення (Time-to-Recover, TTR): середній час від виявлення відмови до відновлення функціональності:

$$TTR = \frac{\sum(t_{repair_i})}{N_{incidents}}, \quad (4)$$

Джерело: реєстр інцидентів [1].

Надлишковість (Redundancy, R):

$$R = \frac{E-V+1}{E}, \quad (5)$$

для зв'язного графа, де  $E$  - кількість ребер,  $V$  - кількість вузлів. Відображає наявність альтернативних шляхів [17]. Інтерпретація: нормалізована цикломатична надлишковість;  $R = 0$  для деревоподібної мережі без альтернативних шляхів.

Енергетична автономність (Energy Autonomy, EA):

$$EA = \frac{N_{autonomous}}{N_{total}}, \quad (6)$$

де  $N_{autonomous}$  - кількість базових станцій із резервним живленням  $\geq 72$  годин [14] (джерело: дані операторів та відповідні вимоги НКЕК щодо резервного живлення базових станцій).

Працездатність запропонованих метрик продемонстровано на спрощеному числовому прикладі (розділ IV); калібрування порогових значень для реальної мережі є предметом подальших досліджень.

Архітектуру адаптовано з класифікації IOWN GF [6] та рамки DT для CI [9] з урахуванням потреб конфліктного відновлення. Вхідні дані NDT згруповано у шість блоків: топологія мережі [6], телеметрія, реєстр інцидентів [1], [13], енергозабезпечення [10], [14], транспортна доступність [8], [10] та ресурси відновлення [18]. Аналітичний рівень поєднує графові моделі [12], сценарне моделювання та ймовірнісні підходи (зокрема динамічні басейнські мережі [10]) для оцінки каскадних ефектів. Відповідно до [6], NDT включає описовий, предиктивний і прескриптивний рівні. Внесок C3 полягає у адаптації цієї архітектури до контексту оцінки резильєнтності телеком-інфраструктури в умовах конфлікту, а не у створенні нової моделі.

Процедура сценарного аналізу (what-if) аналізу, яка формалізується таким чином. Вхід: граф мережі  $G(V, E)$  з атрибутами вузлів (тип, потужність, стан живлення, EA) та ребер (пропускна здатність, довжина, тип прокладання). Сценарій задається як набір відмов: видалення вузлів/ребер або зниження їхньої ємності (наприклад, відключення живлення в підмножині  $V$ ). Модель: перерахунок метрик  $A, C, FT, R$  для деградованого графа  $G'$  за формулами з розділу III-Б. Вихід: (а) значення метрик до та після сценарію, (б) ранжування вузлів за впливом на зв'язність (центральність за посередництвом (betweenness centrality), зміна  $C$  при видаленні), (в) порівняння варіантів інтервенцій (наприклад, встановлення EA для топ-k вузлів vs. прокладання резервного ребра). Клас інструментів: мережеві симулятори з підтримкою графових операцій (NetworkX, ns-3, спеціалізовані NDT-платформи); мінімальна вимога - можливість імпорту топології та обчислення метрик зв'язності [6], [12].

Результати сценарного аналізу (what-if) перетворюються на BBB-рішення через пріоритизацію на основі резильєнтності (resilience-driven), адаптовану з [18]. У нашій рамці

$$Priority(i) = w_A \cdot \Delta A(i) + w_C \cdot \Delta C(i) + w_{FT} \cdot \Delta FT(i) + w_{EA} \cdot \Delta EA(i), \quad (7)$$

з обмеженнями бюджету, ресурсів і доступності. Ваги визначаються експертами/регулятором; алгоритм формує ранжований список, який коригується експертно (участь експерта в циклі рішень, human-in-the-loop) та логуються для аудиту. Типові BBB-заходи: модернізація обладнання й автономне живлення [14], підземне прокладання ВОЛЗ [7], резервні канали/національний роумінг [17].

Для формалізації процедури визначення вагових коефіцієнтів  $w$  рекомендується застосування методу аналізу ієрархій (Analytic Hierarchy Process, АНП), запропонованого Т. Сааті. АНП передбачає: (1) попарне порівняння метрик резильєнтності ( $C, R, EA$  тощо) за шкалою від 1 (рівна важливість) до 9 (абсолютна перевага одного критерію); (2) побудову квадратної матриці попарних порівнянь розміром  $n \times n$ , де  $n$  — кількість метрик; (3) обчислення вектора пріоритетів (вагових коефіцієнтів) як нормалізованого головного власного вектора матриці; (4) перевірку узгодженості через коефіцієнт узгодженості (Consistency Ratio, CR): матриця вважається узгодженою при  $CR < 0,1$ . Якщо  $CR \geq 0,1$ , експерти повторюють процедуру порівняння для усунення суперечностей. АНП забезпечує прозорість та відтворюваність процедури призначення ваг, що є суттєвим для обґрунтування рішень перед донорами та регулятором. У спрощеному числовому прикладі (розділ IV) використано ілюстративні ваги  $w_C = 0,50$ ,  $w_R = 0,20$ ,  $w_{EA} = 0,30$ , отримані для гіпотетичного сценарію, де зв'язність є домінуючим критерієм.

Концепція DRT [11] є доречною для контексту конфлікту, де автоматизований збір даних часто неможливий. У запропонованій архітектурі DRT забезпечує поступову деградацію (graceful degradation): за відсутності актуальної телеметрії частину параметрів заміщують імовірнісними оцінками на основі історичних даних, експертних суджень та дистанційного зондування [11], [19]. Результати сценарного аналізу (what-if) супроводжуються рівнем довіри (confidence) залежно від частки виміряних vs. оцінених даних; рішення з низьким рівнем довіри, за нашими спостереженнями, вимагають додаткової верифікації перед реалізацією. Це принципово важливий запобіжник.

Результати: концептуальна модель проактивного відновлення. Таблиця 1 порівнює реактивний та проактивний (NDT+BBB) підходи. Формулювання подано як очікувані ефекти, оскільки рамка не валідована емпірично. Таблиця також відображає ситуації, де реактивний підхід має переваги.

Таблиця 1

#### Порівняння реактивного та проактивного (NDT+BBB) підходів до відновлення

Критерій	Реактивний підхід	Проактивний (NDT+BBB)
Швидкість точкового ремонту	Висока: не потребує побудови моделі; ремонт починається одразу [14]	Потребує початкових інвестицій у модель; системна відповідь може бути швидшою для складних сценаріїв [9]
Початкові витрати	Низькі: не потребує ІТ-інфраструктури та спеціалістів	Високі: створення та підтримка NDT потребує ресурсів
Довгострокова вартість (ТСО)	Потенційно вища через повторні відмови [7]	Очікується нижча завдяки усуненню системних вразливостей [7], [14]
Ризик повторної відмови	Підвищений: відтворюється попередня вразливість [7]	Очікується зниження завдяки BBB-інтервенціям [7], [8]
Пріоритизація	За доступністю ресурсів та інженерною експертизою	За метриками резильєнтності та сценарним аналізом [12], [18]
ІТ-незалежність	Повна: не залежить від цифрової інфраструктури	Залежить від NDT-платформи; кіберризик [13]
Простота впровадження	Висока: не потребує навчання та нових систем	Низька: потребує підготовки персоналу та інтеграції систем
Аудитовність рішень	Обмежена: рішення ad hoc, важко верифікувати [18]	Потенційно висока: обґрунтування, кероване даними (data-driven), логуються [10], [18]
Довгострокова резильєнтність	Не забезпечується системно [8]	Очікується підвищення через модернізацію та моніторинг [9], [14]

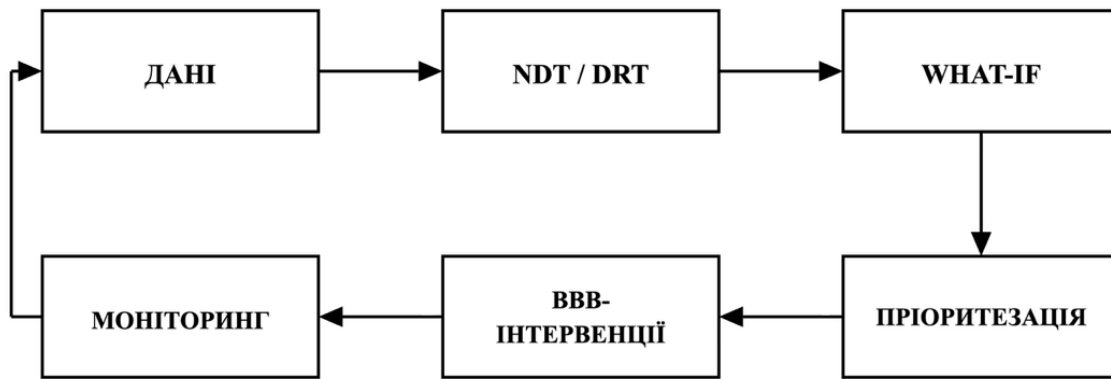


Рис. 1. Концептуальна архітектура інтеграції NDT у цикл прийняття рішень щодо BBB-відновлення

Якісний сценарій 1: Каскадна відмова через відключення енергопостачання. Внаслідок ударів по енергоінфраструктурі регіон втрачає електропостачання; базові станції вимикаються у міру вичерпання резерву. Реактивний підхід передбачає оперативне розгортання генераторів і пріоритетизацію за покриттям та кількістю абонентів [14]. Додана вартість NDT - мережеве ранжування станцій за їхнім внеском у загальну зв'язність (наприклад, через зміну  $C/centrality$ ), виявлення “прихованих” транзитних вузлів та кількісна оцінка приросту  $\Delta C$  при підвищенні енергетичної автономності. BBB-рішення: інвестувати в ЕА насамперед для вузлів із найбільшим мережевим ефектом (за  $\Delta C$ ), що зменшує ризик повторних відмов і TTR у подібних подіях [14], [18].

Якісний сценарій 2: Руйнування магістрального каналу зв'язку. Руйнується магістральна волоконно-оптична лінія зв'язку, що з'єднує регіон із національною мережею. Реактивно трафік перенаправляють альтернативними маршрутами, але вибір часто обмежений кількома варіантами “з досвіду” [14]. NDT дозволяє оперативно перерахувати альтернативні маршрути з урахуванням ємності ребер і навантаження та оцінити вплив на  $\Delta C/\Delta A$  і очікуваний QoS [17]. BBB-рішення: географічно диверсифіковане резервування (зокрема підземний резервний маршрут [7]) і/або супутниковий резерв як додатковий рівень [15], що підвищує  $R$ .

Спрощений числовий приклад. Для демонстрації обчислювальної працездатності запропонованого управлінського циклу розглядається гіпотетична мережа  $G_0$  із 7 вузлів (V1–V7) та 7 ребер. Топологія мережі: V1–V2 (магістраль), V2–V3 (магістраль), V3–V4 (доступ), V2–V5 (доступ), V5–V6 (доступ), V6–V7 (доступ), V3–V6 (перемичка між регіональними сегментами). Вузли V2 та V6 є ключовими хабами з найбільшою кількістю з'єднань; обидва забезпечені автономним живленням ( $\geq 72$  год). Графічне представлення наведено на рис. 2.

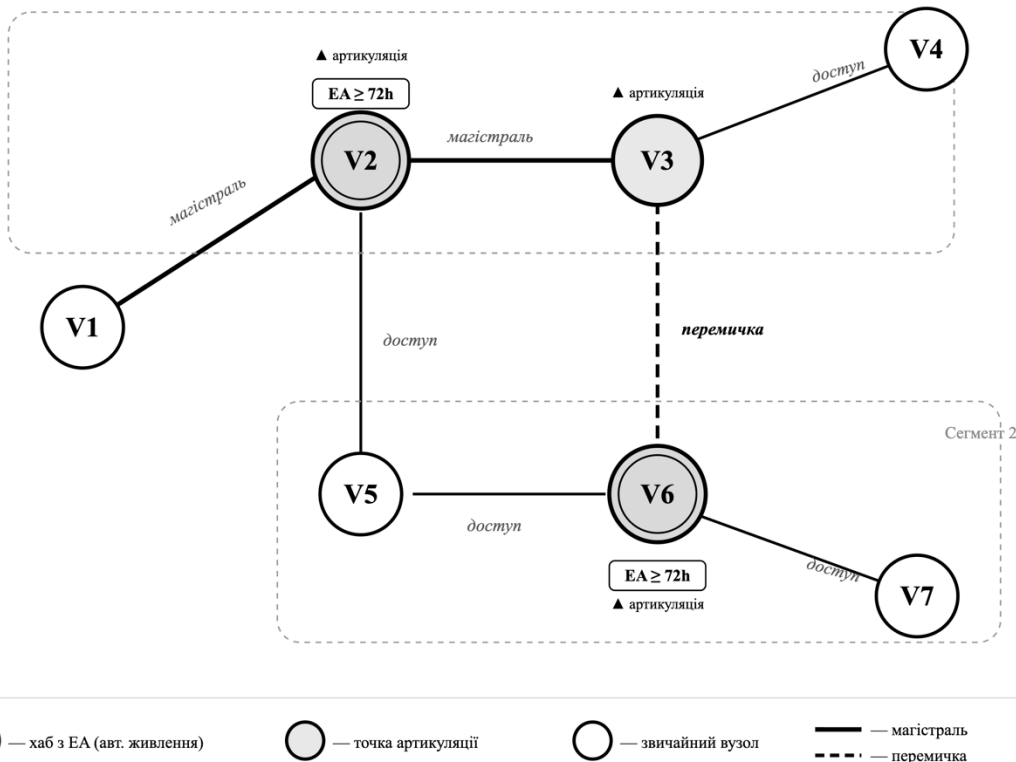


Рис. 2. Граф гіпотетичної телекомунікаційної мережі  $G_0$  (7 вузлів, 7 ребер)

Базові значення метрик для  $G_0$ : зв'язність  $C_0 = P_{connected} / P_{total} = 21/21 = 1,000$  (усі 21 пари вузлів мають наскрізне з'єднання); надлишковість  $R_0 = (E - V + 1) / E = (7 - 7 + 1) / 7 = 1/7 \approx 0,143$  (один незалежний цикл:

V2–V3–V6–V5–V2 через перемичку V3–V6); енергетична автономність  $EA_0 = N_{\text{autonomous}} / N_{\text{total}} = 2/7 \approx 0,286$ . Точки артикуляції (вузли, видалення яких розриває зв'язність): {V2, V3, V6}; відмовостійкість  $FT_0 = 1 - 3/7 \approx 0,571$ .

Сценарій деградації: руйнування вузла V6 (регіональний хаб з автономним живленням). Видаляються вузол V6 та інцидентні ребра V5–V6, V6–V7, V3–V6. Деградований граф  $G'$  містить 6 вузлів та 4 ребра (V1–V2, V2–V3, V3–V4, V2–V5); вузол V7 втрачає усі з'єднання та стає ізольованим. Метрики деградованого стану:  $C' = 10/15 \approx 0,667$  (V7 ізольований; із 15 можливих пар лише 10 залишаються з'єднаними);  $R' = (E - V + k) / E = (4 - 6 + 2) / 4 = 0,000$  (деревоподібна структура без альтернативних шляхів;  $k = 2$  — кількість компонент зв'язності);  $EA' = 1/6 \approx 0,167$  (V6 зруйновано, лише V2 зберігає резервне живлення).

Розглядаються дві альтернативні інтервенції, що ілюструють різницю між мінімальним відновленням та BBB-модернізацією.

Інтервенція А (мінімальне відновлення): прокладання одного нового ребра V4–V7, що відновлює з'єднання ізольованого вузла V7 із основною мережею. Результат:  $C_A = 15/15 = 1,000$  (зв'язність повністю відновлена);  $R_A = (5 - 6 + 1) / 5 = 0,000$  (мережа залишається деревоподібною, без резервних маршрутів);  $EA_A = 1/6 \approx 0,167$  (енергетична автономність не змінена).

Інтервенція В (BBB-модернізація): прокладання двох ребер V4–V7 та V5–V7 (підземна ВОЛЗ із географічною диверсифікацією маршрутів) та встановлення автономного живлення для вузлів V3 і V5. Результат:  $C_B = 15/15 = 1,000$ ;  $R_B = (6 - 6 + 1) / 6 \approx 0,167$  (утворено один незалежний цикл V4–V7–V5–V2–V3–V4, що забезпечує альтернативний маршрут);  $EA_B = 3/6 = 0,500$  (автономне живлення мають V2, V3, V5 — три із шести вузлів).

Таблиця 2

#### Порівняння метрик для вихідного, деградованого стану та двох інтервенцій

Метрика	$G_0$	$G'$ (деград.)	Інтерв. А	Інтерв. В (BBB)
C (зв'язність)	1,000	0,667	1,000	1,000
R (надлишковість)	0,143	0,000	0,000	0,167
EA (енерг. автон.)	0,286	0,167	0,167	0,500

Приріст метрик від інтервенцій відносно деградованого стану ( $\Delta M = M_{\text{intervention}} - M_{\text{degraded}}$ ): для інтервенції А:  $\Delta C = 0,333$ ;  $\Delta R = 0,000$ ;  $\Delta EA = 0,000$ ; для інтервенції В:  $\Delta C = 0,333$ ;  $\Delta R = 0,167$ ;  $\Delta EA = 0,333$ .

За ілюстративними вагами, визначеними за процедурою АНР для гіпотетичного сценарію ( $w_C = 0,50$ ;  $w_R = 0,20$ ;  $w_{EA} = 0,30$ ):

$$Priority(A) = 0,50 \times 0,333 + 0,20 \times 0,000 + 0,30 \times 0,000 = 0,167$$

$$Priority(B) = 0,50 \times 0,333 + 0,20 \times 0,167 + 0,30 \times 0,333 = 0,300$$

Інтервенція В (BBB-модернізація) має пріоритетний бал на 80 % вищий за інтервенцію А (0,300 проти 0,167). Цей результат кількісно демонструє додану вартість BBB-підходу: при однаковому відновленні зв'язності ( $\Delta C = 0,333$  для обох варіантів) BBB-інтервенція додатково підвищує надлишковість ( $\Delta R = 0,167$ ) та енергетичну автономність ( $\Delta EA = 0,333$ ), що суттєво знижує ризик повторних відмов при аналогічних сценаріях деструкції. Навіть при зміні вагових коефіцієнтів (наприклад,  $w_C = 0,60$ ;  $w_R = 0,30$ ;  $w_{EA} = 0,10$ ) інтервенція В зберігає перевагу:  $Priority(A) = 0,200$ ;  $Priority(B) = 0,283$ , що свідчить про робастність результату.

Зауважимо: наведений приклад є ілюстративним і демонструє обчислювальну працездатність запропонованого управлінського циклу. Для реальної мережі з сотнями вузлів обчислення метрик потребує спеціалізованого програмного забезпечення (NetworkX, ns-3 або NDT-платформа [6]), а вагові коефіцієнти — формальної процедури АНР із залученням профільних експертів та представників регулятора.

Таблиця 3

#### Деталізація управлінського циклу NDT+BBB: актори, дані, інструменти

Крок	Актор	Вхідні дані	Метод/інструмент	Вихід	Періодичність
1. Збір даних	Оператор, RS-провайдер	Телеметрія NMS, Sentinel-1 SAR [19], звіти [1]	Автоматична агрегація + DRT для пропусків [11]	Актуалізований датасет NDT	Безперервно / орієнтовно 6-12 днів (RS, залежно від доступності даних)
2. Побудова NDT	NDT-платформа (оператор)	Датасет кроку 1, топологія	Графове моделювання, баєсівські мережі [10]	Описовий + предиктивний двійник	При оновленні даних
3. What-if	Аналітик / регулятор	NDT-модель, набір сценаріїв	Симуляція відмов, перерахунок A, C, FT, R, EA	Матриця «сценарій → $\Delta$ метрики»	За запитом / щомісяця
4. Пріоритезація	Регулятор + експерти	Матриця кроку 3, бюджет, ресурси	Priority(i) = $\sum w \cdot \Delta M(i)$ [18]; участь експерта в циклі рішень (human-in-the-loop)	Ранжований план інтервенцій	При зміні сценарію / бюджету

Продовження таблиці 3

5. BBB-інтервенція	Оператор, підрядник	План кроку 4, специфікації [14]	Модернізація, резервування, заглиблення [7]	Виконані BBB-заходи	За планом
6. Моніторинг	Оператор, донор (аудит)	Телеметрія, RS, звіти	Порівняння метрик до/після [9]	Оновлений NDT; звіт для донорів	Безперервно

Governance. Фінальне рішення щодо пріоритетів затверджується оператором за погодженням регулятора (НКЕК (NCEC)). Усі рішення логуються з обґрунтуванням (метрики, сценарій, бюджет) для забезпечення прозорості перед донорами та аудитором. Експертна корекція алгоритмічних рекомендацій є обов'язковим етапом (участь експерта в циклі рішень, human-in-the-loop), що мінімізує ризик хибної пріоритизації.

Переваги. На наш погляд, запропонована рамка потенційно забезпечує інвестиційну ефективність через зменшення повторних витрат та оптимізацію ресурсів [14], [18], а також прозорість для донорів через обґрунтування пріоритетів, кероване даними (data-driven), що відповідає принципам аудиторності BBB-фінансування [7] і є критичним з огляду на масштаб фінансування (5,86 млрд доларів [2]). І не менш важливим є зниження часу простою (downtime) через превентивне виявлення вразливостей [9] та системність прийняття рішень з урахуванням міжсекторальних залежностей [5], [15]. Порівняно з практичним гідом WB [14], який систематизує заходи стійкості, але не пропонує інструменту кількісного обґрунтування, NDT-рамка додає можливість мережевої пріоритизації та оцінки каскадних ефектів.

Обмеження. Дефіцит даних у зоні бойових дій ускладнює збір телеметрії та коректне калібрування моделі [8]. DRT (розділ III-Д) частково компенсує пропуски, але при великій частці оцінених даних зростає ризик хибної пріоритизації. Мінімізація: аналіз чутливості (sensitivity analysis), ретроспективна перевірка на відомих інцидентах та обов'язковий контроль з участю експерта (human-in-the-loop) (крок 4, Табл. 3). Додаткові обмеження: висока вартість створення/підтримки NDT та кіберризиків (NDT як цифрова модель CI може бути ціллю атак) [13]. Рамка є концептуальною і потребує емпіричної валідації; для точкових ремонтів із достатньою інженерною експертизою NDT може бути економічно невиправданим.

Критерії фальсифікації. Рамка визнається неефективною, якщо вартість створення та підтримки NDT перевищує 15–20% від бюджету відновлення сегмента або точність моделі (відповідність прогнозованих та фактичних метрик) нижче 70%. Також вважаємо за доцільне враховувати затримку оновлення моделі понад цикл прийняття рішень (>1 тижня) та незабезпеченість кіберзахисту NDT-платформи. Ці критерії підлягають перевірці у пілотному дослідженні.

Валідація предиктивної точності NDT. Для кількісної оцінки предиктивної здатності цифрового двійника у межах пілотного дослідження ми рекомендуємо порівнювати прогнозовані NDT значення метрик (A, C, FT, TTR) з фактичними даними телеметрії. Доцільним видається використання класичних метрик точності: RMSE (Root Mean Square Error) для оцінки середньоквадратичного відхилення, MAE (Mean Absolute Error) для середньої абсолютної похибки та MAPE (Mean Absolute Percentage Error) для нормалізованого порівняння між метриками з різними одиницями виміру. Зокрема, критерій фальсифікації «точність моделі нижче 70 %» формалізується як MAPE > 30 % для будь-якої з ключових метрик протягом періоду спостереження: якщо середня відносна похибка прогнозу NDT перевищує 30 %, модель потребує перекалібрування або визнається непридатною для даного сегмента. Регулярне обчислення RMSE та MAE дозволить ідентифікувати конкретні сегменти мережі або метрики, де модель потребує додаткового калібрування, та відстежувати динаміку точності NDT у часі.

Вимоги до емпіричної валідації. Пілотна валідація потребує сегмента мережі (50–100 базових станцій) у регіоні з контрольованою складністю та доступу до топології й телеметрії у співпраці з оператором із можливим підкріпленням дистанційним зондуванням [19]. За нашими оцінками, необхідним є порівняння базового сценарію (baseline, реактивний підхід) vs. NDT-підтримані рішення за метриками A, C, TTR, період спостереження  $\geq 6$  місяців та партнерство операторів, НКЕК/регулятора, ІТУ і наукових установ. Перспективним напрямком є інтеграція DRL [12] як ядра оптимізації послідовності відновлення на кроці 4 (мінімізація LoR).

### Висновки з даного дослідження

#### і перспективи подальших розвідок у даному напрямі

Запропоновано концептуальну рамку інтеграції NDT в оцінку резильєнтності телекомунікаційної інфраструктури України за принципом BBB. На основі синтезу 19 джерел виявлено розрив: у відібраній вибірці джерел (2021–2025) не виявлено досліджень, що поєднують NDT, оцінку резильєнтності та BBB для телеком-інфраструктури в умовах конфлікту. Гіпотеза про подолання розриву між реактивним точковим відновленням та системним підходом підтверджується на рівні якісної аргументації: порівняльний аналіз (Табл. 1) демонструє очікувані переваги та обмеження обох підходів, а сценарії ілюструють специфічну додану вартість NDT - кількісну оцінку мережевих ефектів, яка недосяжна при точковому реактивному відновленні.

Практичний внесок - замкнений управлінський цикл (Табл. 3) із визначенням акторів, даних та інструментів на кожному кроці, що може слугувати основою для систем підтримки рішень. Синергетичний ефект інтеграції NDT+BBB ми вбачаємо у переході від декларативного BBB до кількісно обґрунтованих інтервенцій з пріоритизацією за метриками резильєнтності. NDT забезпечує дані для моделювання, BBB визначає напрямок

модернізації, а їхнє поєднання створює можливість порівняння варіантів інтервенцій за впливом на мережеву зв'язність.

Ключові обмеження: концептуальний характер (потребує емпіричної валідації), залежність від якості даних, вартість впровадження. Пріоритетні напрямки майбутніх досліджень, як нам видається: пілотна валідація на сегменті мережі з калібруванням метрик, інтеграція міжсекторальних ДТ (телекомунікації + енергетика + транспорт) та застосування DRL-методів [12] як обчислювального ядра пріоритезації. І кожен із цих напрямків може суттєво змінити практичну цінність рамки.

### Література

1. Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine. – Geneva : ITU Office for Europe, 2022. – 71 p – Режим доступу: [https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructur%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22\\_FINAL.pdf](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructur%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf).
2. Ukraine Fourth Rapid Damage and Needs Assessment (RDNA4). – Washington, DC : World Bank, 2025 – Режим доступу: <https://openknowledge.worldbank.org/entities/publication/0f04dfe0-41ea-410f-bdd9-4d2bc9d40569>.
3. Primary Assessment of Rehabilitation Costs for Five Broadcasting Stations in Ukraine. – Geneva : ITU, 2024. – 19 p – Режим доступу: <https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Projects/2022/Council%20Resolution%20on%20Ukraine%20-%20Coordination%20and%20Implementation/Council-Resolution-on-Ukraine---Coordination-and-Implementation.aspx>.
4. Ukraine Digital Development Country Profile. Ver. 3.0. – Geneva : ITU, 2025. – 85 p – Режим доступу: [https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final\\_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf).
5. Aebi S. Critical infrastructure resilience in Ukraine: Energy, transportation, and communication / S. Aebi, A. Hauri, J. Kamberaj. – Zürich : Center for Security Studies (CSS), ETH Zürich, 2024. – 42 p. – DOI: <https://doi.org/10.3929/ethz-b-000662463>.
6. Network Digital Twin Use Case Classification. Ver. 2.0. – IOWN Global Forum, Inc., 2024. – 84 p – Режим доступу: [https://iowngf.org/wp-content/uploads/2025/02/IOWN-GF-RD-NDT\\_Use\\_Case-2.0.pdf](https://iowngf.org/wp-content/uploads/2025/02/IOWN-GF-RD-NDT_Use_Case-2.0.pdf).
7. Der Sarkissian R. Evaluating the implementation of the “Build-Back-Better” concept for critical infrastructure systems: Lessons from Saint-Martin’s island following Hurricane Irma / R. Der Sarkissian, A. Dabaj, Y. Diab, M. Vuillet // Sustainability. – 2021. – Vol. 13, no. 6. – Art. no. 3133. – DOI: <https://doi.org/10.3390/su13063133>.
8. Mitoulis S.-A. Conflict-resilience framework for critical infrastructure peacebuilding / S.-A. Mitoulis, S. Argyroudis, M. Panteli, C. Fuggini, S. Valkaniotis, W. Hynes, I. Linkov // Sustainable Cities and Society. – 2023. – Vol. 91. – Art. no. 104405. – DOI: <https://doi.org/10.1016/j.scs.2023.104405>.
9. Brucherseifer E. Digital Twin conceptual framework for improving critical infrastructure resilience / E. Brucherseifer, H. Winter, A. Mentges, M. Mühlhäuser, M. Hellmann // Automatisierungstechnik. – 2021. – Vol. 69, no. 12. – P. 1062–1080. – DOI: <https://doi.org/10.1515/auto-2021-0104>.
10. Braik A. M. A digital twin framework for efficient electric power restoration and resilient recovery in the aftermath of hurricanes considering the interdependencies with road network and essential facilities / A. M. Braik, M. Koliou // Resilient Cities and Structures. – 2024. – Vol. 3, no. 3. – P. 79–91. – DOI: <https://doi.org/10.1016/j.rcns.2024.07.004>.
11. Ghaffarian S. Rethinking digital twin: Introducing digital risk twin for disaster risk management / S. Ghaffarian // npj Natural Hazards. – 2025. – Vol. 2. – Art. no. 79. – DOI: <https://doi.org/10.1038/s44304-025-00135-x>.
12. Liang H. Resilience-based post disaster recovery optimization for infrastructure system via deep reinforcement learning / H. Liang, B. Moya, F. Chinesta, E. Chatzi // arXiv. – 2024. – arXiv:2410.18577. – DOI: <https://doi.org/10.48550/arXiv.2410.18577>.
13. Aviv I. Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem / I. Aviv, U. Ferri // International Journal of Critical Infrastructure Protection. – 2023. – Vol. 43. – Art. no. 100637. – DOI: <https://doi.org/10.1016/j.ijcip.2023.100637>.
14. Ayers S. Resilient Telecommunications Infrastructure: A Practitioner’s Guide / S. Ayers, T. Birk. – Washington, DC : World Bank, 2024. – 44 p – Режим доступу: <https://documents1.worldbank.org/curated/en/099121724111526960/pdf/P1785971617dfc0361b79b10ed943988d67.pdf>
15. Ferreruela I. C. Enhancing the resilience of communication networks / I. C. Ferreruela // OECD Digital Economy Papers, no. 374. – Paris : OECD Publishing, 2025. – 36 p. – DOI: <https://doi.org/10.1787/d6920477-en>.
16. Jiang P. Crisis-ready telecom: Global approaches to emergency management in telecommunications / P. Jiang, J. Rowsell, S. Schmidt // Telecommunications Policy. – 2025. – Vol. 49, no. 4. – Art. no. 102914. – DOI: <https://doi.org/10.1016/j.telpol.2025.102914>.
17. Weedage L. On the resilience of cellular networks: How can national roaming help? / L. Weedage, S. R. C. Magalhães, C. Stegehuis, S. Bayhan // IEEE Transactions on Network and Service Management. – 2024. – Vol. 21, no. 2. – P. 1702–1714. – DOI: <https://doi.org/10.1109/TNSM.2024.3352168>.

18. Koptiika N. Sustainability and resilience-driven prioritisation for restoring critical infrastructure after major disasters and conflict / N. Koptiika, R. Di Bari, S. Argyroudis, J. Ninic, S.-A. Mitoulis // *Transportation Research Part D: Transport and Environment*. – 2025. – Art. no. 104592. – DOI: <https://doi.org/10.1016/j.trd.2025.104592>.

19. Koptiika N. Rapid post-disaster infrastructure damage characterisation using remote sensing and deep learning technologies: A tiered approach / N. Koptiika, A. Karavias, P. Krassakis, Z. Ye, J. Ninic, N. Shakhovska, S. Argyroudis, S. Mitoulis // *Automation in Construction*. – 2025. – Vol. 170. – Art. no. 105955. – DOI: <https://doi.org/10.1016/j.autcon.2024.105955>.

## References

1. Interim assessment on damages to telecommunication infrastructure and resilience of the ICT ecosystem in Ukraine. – Geneva : ITU Office for Europe, 2022. – 71 p – Available at: [https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22\\_FINAL.pdf](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Interim%20assessment%20on%20damages%20to%20telecommunication%20infrastructure%20and%20resilience%20of%20the%20ICT%20ecosystem%20in%20Ukraine%20-2022-12-22_FINAL.pdf).
2. Ukraine Fourth Rapid Damage and Needs Assessment (RDNA4). – Washington, DC : World Bank, 2025 – Available at: <https://openknowledge.worldbank.org/entities/publication/0f04dfe0-41ea-410f-bdd9-4d2bc9d40569>.
3. Primary Assessment of Rehabilitation Costs for Five Broadcasting Stations in Ukraine. – Geneva : ITU, 2024. – 19 p – Available at: <https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Pages/Projects/2022/Council%20Resolution%20on%20Ukraine%20-%20Coordination%20and%20Implementation/Council-Resolution-on-Ukraine---Coordination-and-Implementation.aspx>.
4. Ukraine Digital Development Country Profile. Ver. 3.0. – Geneva : ITU, 2025. – 85 p – Available at: [https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final\\_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf](https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf).
5. Aebi S. Critical infrastructure resilience in Ukraine: Energy, transportation, and communication / S. Aebi, A. Hauri, J. Kamberaj. – Zürich : Center for Security Studies (CSS), ETH Zürich, 2024. – 42 p. – DOI: <https://doi.org/10.3929/ethz-b-000662463>.
6. Network Digital Twin Use Case Classification. Ver. 2.0. – IOWN Global Forum, Inc., 2024. – 84 p – Available at: [https://iowngf.org/wp-content/uploads/2025/02/IOWN-GF-RD-NDT\\_Use\\_Case-2.0.pdf](https://iowngf.org/wp-content/uploads/2025/02/IOWN-GF-RD-NDT_Use_Case-2.0.pdf).
7. Der Sarkissian R. Evaluating the implementation of the “Build-Back-Better” concept for critical infrastructure systems: Lessons from Saint-Martin’s island following Hurricane Irma / R. Der Sarkissian, A. Dabaj, Y. Diab, M. Vuillet // *Sustainability*. – 2021. – Vol. 13, no. 6. – Art. no. 3133. – DOI: <https://doi.org/10.3390/su13063133>.
8. Mitoulis S.-A. Conflict-resilience framework for critical infrastructure peacebuilding / S.-A. Mitoulis, S. Argyroudis, M. Panteli, C. Fuggini, S. Valkaniotis, W. Hynes, I. Linkov // *Sustainable Cities and Society*. – 2023. – Vol. 91. – Art. no. 104405. – DOI: <https://doi.org/10.1016/j.scs.2023.104405>.
9. Brucherseifer E. Digital Twin conceptual framework for improving critical infrastructure resilience / E. Brucherseifer, H. Winter, A. Mentges, M. Mühlhäuser, M. Hellmann // *Automatisierungstechnik*. – 2021. – Vol. 69, no. 12. – P. 1062–1080. – DOI: <https://doi.org/10.1515/auto-2021-0104>.
10. Braik A. M. A digital twin framework for efficient electric power restoration and resilient recovery in the aftermath of hurricanes considering the interdependencies with road network and essential facilities / A. M. Braik, M. Koliou // *Resilient Cities and Structures*. – 2024. – Vol. 3, no. 3. – P. 79–91. – DOI: <https://doi.org/10.1016/j.rcns.2024.07.004>.
11. Ghaffarian S. Rethinking digital twin: Introducing digital risk twin for disaster risk management / S. Ghaffarian // *npj Natural Hazards*. – 2025. – Vol. 2. – Art. no. 79. – DOI: <https://doi.org/10.1038/s44304-025-00135-x>.
12. Liang H. Resilience-based post disaster recovery optimization for infrastructure system via deep reinforcement learning / H. Liang, B. Moya, F. Chinesta, E. Chatzi // *arXiv*. – 2024. – arXiv:2410.18577. – DOI: <https://doi.org/10.48550/arXiv.2410.18577>.
13. Aviv I. Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem / I. Aviv, U. Ferri // *International Journal of Critical Infrastructure Protection*. – 2023. – Vol. 43. – Art. no. 100637. – DOI: <https://doi.org/10.1016/j.ijcip.2023.100637>.
14. Ayers S. Resilient Telecommunications Infrastructure: A Practitioner’s Guide / S. Ayers, T. Birk. – Washington, DC : World Bank, 2024. – 44 p – Available at: <https://documents1.worldbank.org/curated/en/099121724111526960/pdf/P1785971617dfc0361b79b10ed943988d67.pdf>.
15. Ferreruela I. C. Enhancing the resilience of communication networks / I. C. Ferreruela // *OECD Digital Economy Papers*, no. 374. – Paris : OECD Publishing, 2025. – 36 p. – DOI: <https://doi.org/10.1787/d6920477-en>.
16. Jiang P. Crisis-ready telecom: Global approaches to emergency management in telecommunications / P. Jiang, J. Rowsell, S. Schmidt // *Telecommunications Policy*. – 2025. – Vol. 49, no. 4. – Art. no. 102914. – DOI: <https://doi.org/10.1016/j.telpol.2025.102914>.
17. Weedage L. On the resilience of cellular networks: How can national roaming help? / L. Weedage, S. R. C. Magalhães, C. Stegehuis, S. Bayhan // *IEEE Transactions on Network and Service Management*. – 2024. – Vol. 21, no. 2. – P. 1702–1714. – DOI: <https://doi.org/10.1109/TNSM.2024.3352168>.
18. Koptiika N. Sustainability and resilience-driven prioritisation for restoring critical infrastructure after major disasters and conflict / N. Koptiika, R. Di Bari, S. Argyroudis, J. Ninic, S.-A. Mitoulis // *Transportation Research Part D: Transport and Environment*. – 2025. – Art. no. 104592. – DOI: <https://doi.org/10.1016/j.trd.2025.104592>.
19. Koptiika N. Rapid post-disaster infrastructure damage characterisation using remote sensing and deep learning technologies: A tiered approach / N. Koptiika, A. Karavias, P. Krassakis, Z. Ye, J. Ninic, N. Shakhovska, S. Argyroudis, S. Mitoulis // *Automation in Construction*. – 2025. – Vol. 170. – Art. no. 105955. – DOI: <https://doi.org/10.1016/j.autcon.2024.105955>.