The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Cybersecurity and Law

2026 Nr 1(15)

DOI: 10.35467/cal/242480

# Zastosowanie środowiska Cyber Range i koncepcji Digital Twin w procesie kształtowania kompetencji personelu cyberbezpieczeństwa

# The application of Cyber Range environment and the Digital Twin concept in the development of cybersecurity personnel competiences

**Mariusz KRAWCZYK**
Eksperckie Centrum Szkolenia Cyberbezpieczeństwa
ORCID: 0000-0002-9465-7227
E-mail: mkrawczyk@mon.gov.pl)

**Grzegorz PILARSKI**
Akademia Sztuki Wojennej
ORCID: 0000-0001-9728-2611
E-mail: g.pilarski@akademia.mil.pl)

## Streszczenie

W obecnym świecie coraz częściej spotykamy się z różnymi cyberzagrożeniami. Kluczowe znaczenie ma zdolność wczesnego ich identyfikowania co pozwoli na podejmowanie określonych działań prewencyjnych, a także ograniczenie potencjalnych skutków ich wystąpienia. Istotne w tym względzie jest podnoszenie poziomu w procesie kształtowania kompetencji personelu cyberbezpieczeństwa. Jednym z rozwiązań wspomagających ten proces może być zastosowanie środowiska cyberpoligonu (Cyber Range - CR) i koncepcji odwzorowania rzeczywistego obiektu, systemu lub procesu w środowisku cyfrowym (Digital Twin - DT). Celem artykułu jest wyjaśnienie, w jaki sposób środowisko Cyber Range, projektowane z wykorzystaniem logiki Digital Twin może wspierać budowanie i rozwój kompetencji personelu w obszarze cyberbezpieczeństwa.

Artykuł ma charakter koncepcyjno-analityczny, czego efektem jest propozycja metody projektowania, prowadzenia i ewaluacji ćwiczeń rozwijających kompetencje personelu cyberbezpieczeństwa. Zastosowaną metodą badawczą była analiza i krytyczny przegląd literatury przedmiotu, obejmujące publikacje naukowe, raporty instytucjonalne oraz opracowania eksperckie w zakresie środowiska cyberpoligonu (CR) oraz koncepcji odwzorowania rzeczywistego w środowisku cyfrowym (DT). Wartością dodaną były prowadzone badania empiryczne w środowisku cyberpoligonu w Eksperckim Centrum Szkolenia Cyberbezpieczeństwa.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

CR ujęto jako środowisko edukacyjno-ćwiczeniowe, natomiast logikę DT jako sposób selektywnego odwzorowania cyfrowego zależności istotnych w procesie rozwijania zdolności personelu cyberbezpieczeństwa. Autorzy w badaniach skoncentrowali się na kształtowaniu i doskonaleniu kompetencji technicznych, analitycznych oraz decyzyjnych personelu cyberbezpieczeństwa. Szczególne znaczenie przypisano kontrolowanemu realizmowi, scenariuszom, rolom uczestników, artefaktom, telemetryce, kluczowym wskaźnikom efektywności oraz punktowej ocenie wykonania scenariusza.

## *Słowa kluczowe*

*bezpieczeństwo państwa, cyberpoligon, digital twin, cyberbezpieczeństwo, rozwój kompetencji cyfrowych*

## Abstract

In today's world, we are increasingly confronted with various cyber threats. The ability to identify them at an early stage is of crucial importance, as it enables specific preventive measures to be taken and helps to minimise the potential consequences should they occur. In this regard, it is essential to enhance the skills of cybersecurity personnel. One solution to support this process could be the use of a Cyber Range (CR) environment and the concept of replicating a real-world facility, system or process in a digital environment (Digital Twin – DT). The aim of this article is to explain how a Cyber Range environment, designed using Digital Twin logic, can support the development and enhancement of staff competencies in the field of cybersecurity.

This article is conceptual and analytical in nature, resulting in a proposed method for designing, conducting and evaluating exercises aimed at developing the competencies of cybersecurity personnel. The research method employed was an analysis and critical review of the relevant literature, covering academic publications, institutional reports and expert studies on the cyber range (CR) environment and the concept of real-world simulation in a digital environment (DT). An added benefit was the empirical research carried out in the cyber range environment at the Cyber Security Training Center of Excellence.

CR was defined as an educational and training environment, whilst DT logic was defined as a method of selectively mapping the digital relationships relevant to the process of developing the capabilities of cybersecurity personnel. In their research, the authors focused on shaping and improving the technical, analytical and decision-making competencies of cybersecurity personnel. Particular importance was attached to controlled realism, scenarios, participant roles, artefacts, telemetry, key performance indicators and the scoring of scenario execution.

## *Keywords*

*state security, cyber range, digital twin, cybersecurity, development of digital competencies*

## Wprowadzenie

W niniejszym artykule autorzy przyjęli, że pojęcie kompetencji odnosi się do zdolności jednostki do skutecznego wykonywania określonych zadań w konkretnym środowisku pracy. Kompetencje[1] obejmują nie tylko wiedzę teoretyczną, lecz także umiejętności praktyczne, doświadczenie oraz postawy umożliwiające efektywne działanie w sytuacjach operacyjnych. W literaturze

[1] Por. P. Ostolski, The role of digital skills in the changing cybersecurity environment, Cybersecurity and Law 2025, Nr 2 (14), s. 40.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

i praktyce zawodowej funkcjonuje kilka modeli kompetencyjnych umożliwiających definiowanie określonych ról, zadań, niezbędnej wiedzy, umiejętności i kompetencji personelu cyberbezpieczeństwa[2].

Proces kształtowania kompetencji personelu cyberbezpieczeństwa powinien obejmować: kształcenie, szkolenie, realizację ćwiczeń, ocenę osiągniętych rezultatów oraz doskonalenie. Kształcenie odpowiada przede wszystkim za to co „wiemy", szkolenie za to co „umiemy wykonywać", ćwiczenia za to co „umiemy zastosować w warunkach zbliżonych do rzeczywistości", ocena służy temu, aby „sprawdzić na jakim poziomie osiągnięto kompetencje", a doskonalenie za „usuwanie luk kompetencyjnych".

Rozwój kompetencji personelu cyberbezpieczeństwa wymaga czegoś więcej niż przekazania wiedzy teoretycznej. Wykład, prezentacja, test wiedzy lub jednorazowy warsztat mogą budować podstawy rozumienia pojęć, procedur i narzędzi, ale nie wykazują w pełni, czy uczestnik potrafi zastosować tę wiedzę w sytuacji zadaniowej. W praktyce specjalista cyberbezpieczeństwa musi nie tylko znać procedurę, lecz także rozpoznać sygnały incydentu, zinterpretować dane, skorelować alerty, podjąć decyzję, udokumentować działania i wyciągnąć wnioski z ich skutków.

Z tego powodu coraz większego znaczenia nabierają środowiska ćwiczeniowe, które pozwalają przejść od wiedzy deklaratywnej do kompetencji praktycznej. Cyber Range (CR)[3] tworzy warunki do działania w bezpiecznym i kontrolowanym scenariuszu, natomiast logika Digital Twin (DT)[4] pozwala selektywnie odwzorować te zależności techniczne, organizacyjne i procesowe, które są istotne dla celu dydaktycznego. W takim ujęciu CR/DT[5] nie jest jedynie rozwiązaniem technologicznym, lecz środowiskiem uczenia się przez działanie.

Potrzeba praktycznego rozwijania kompetencji wynika również z charakteru współczesnej cyberprzestrzeni. Nie jest ona wyłącznie środowiskiem technicznym, lecz przestrzenią relacji, oddziaływania i współzależności między podmiotami państwowymi, wojskowymi, gospodarczymi i społecznymi[6]. W takim ujęciu incydent cyberbezpieczeństwa może być elementem szerszych działań hybrydowych, obejmujących presję informacyjną, organizacyjną, polityczną lub społeczną. Dlatego kompetencje personelu nie mogą ograniczać się do znajomości narzędzi. Muszą obejmować zdolność rozumienia sytuacji, interpretowania skutków incydentu,

[2] Do najważniejszych można zaliczyć Europejskie Ramy Kompetencji Cyberbezpieczeństwa (European Cybersecurity Skills Framework – ECSF) oraz ramy kompetencji cyberbezpieczeństwa rozwijane przez NIST (National Initiative for Cybersecurity Education Framework - NIST SP 800-181). Należy jednak nadmienić, że w tym obszarze funkcjonują również inne modele między innymi: European e-Competence Framework (e-CF), Skills Framework for the Information Age (SFIA), oraz Cyber Security Body of Knowledge (CyBOK).

[3] Cyber Range (CR) – środowisko ćwiczeń cyberbezpieczeństwa. Izolowane i kontrolowane środowisko do realizacji ćwiczeń technicznych i decyzyjnych, umożliwiające symulację incydentów, rejestrowanie telemetrii, punktację oraz porównywalny pomiar efektów treningu.

[4] Digital Twin (DT) – cyfrowy bliźniak. Odwzorowanie wybranych elementów infrastruktury, procesów i zależności organizacyjnych, np. topologii logicznej, ról, usług, tożsamości, segmentacji i punktów telemetrycznych, wykorzystywane w środowisku ćwiczeń w celu zwiększenia realizmu scenariuszy bez używania danych produkcyjnych ani ujawniania informacji wrażliwych.

[5] CR/DT – połączony model środowiska ćwiczeń, w którym CR stanowi środowisko wykonania scenariuszy, a DT zapewnia odwzorowanie wybranych zależności technicznych, organizacyjnych i procesowych.

[6] Por. G. Pilarski, M. Nowikowska, P. Galemba, Deepfake technology: definition, characteristics of the phenomenon, and mechanisms of operation, Cybersecurity and Law 2025, Nr 2 (14), s. 16-18.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

współdziałania między rolami oraz podejmowania decyzji w warunkach niepełnej informacji[7].

Celem niniejszego artykułu jest wyjaśnienie, w jaki sposób środowisko Cyber Range z wykorzystaniem koncepcji Digital Twin może wspierać budowanie i rozwój kompetencji personelu w obszarze cyberbezpieczeństwa. W odniesieniu do przedstawionej powyżej sytuacji problemowej, autorzy zdefiniowali problem badawczy w postaci następującego pytania: w jaki sposób środowisko CR, projektowane z wykorzystaniem logiki DT, może wspierać rozwój kompetencji personelu w obszarze cyberbezpieczeństwa?

Z uwagi na nowatorskie podejście do problemu badawczego niniejszy artykuł ma charakter koncepcyjno-analityczny. W procesie badawczym przeprowadzono analizę i krytyczny przegląd literatury przedmiotu, obejmujące publikacje naukowe, raporty instytucjonalne oraz opracowania eksperckie w zakresie środowiska cyberpoligonu oraz koncepcji odwzorowania rzeczywistego w środowisku cyfrowym. Ponadto, wykorzystano wyniki badań jakie przeprowadzono w środowisku cyberpoligonu na bazie Eksperckiego Centrum Szkolenia Cyberbezpieczeństwa.

Autorzy mają świadomość, że dotychczasowe badania w zakresie zastosowania synergicznego połączenia środowiska cyberpoligonu z koncepcją rzeczywistego odwzorowania cyfrowego mają charakter podstawowy i stanowią punkt wyjścia do dalszych prac badawczych mających na celu empiryczną weryfikację zaproponowanego podejścia oraz ocenę jego skuteczności w zakresie kształtowania kompetencji personelu cyberbezpieczeństwa.

## Cyber Range i logika Digital Twin jako narzędzia w budowaniu środowiska rozwoju kompetencji cyfrowych

CR należy rozumieć nie tylko jako platformę technologiczną, lecz przede wszystkim jako środowisko edukacyjno-ćwiczeniowe. Jego podstawową funkcją jest stworzenie warunków, w których uczestnik może zastosować wiedzę w praktyce, pracować z artefaktami, analizować zdarzenia, podejmować decyzje i otrzymywać informację zwrotną. Kompetencja nie jest tu oceniana wyłącznie na podstawie deklaracji lub wyniku testu, lecz ujawnia się w sposobie działania uczestnika wobec problemu.

Szczególne znaczenie mają trzy grupy kompetencji: techniczne, analityczne i decyzyjne. Kompetencje techniczne obejmują między innymi: analizę logów, obsługę narzędzi, konfigurację zabezpieczeń i pracę w środowisku SIEM/SOC[8]. Kompetencje analityczne dotyczą korelacji zdarzeń, interpretacji symptomów i budowy obrazu sytuacji. Kompetencje decyzyjne odnoszą się natomiast do wyboru sposobu działania, priorytetyzacji zadań, eskalacji oraz oceny skutków podjętych decyzji. Wraz z rozwojem wspomnianych powyżej trzech

[7] Zob. szerz. G. Pilarski, Cyberprzestrzeń – relacje w wojnie hybrydowej, Akademia Sztuki Wojennej, Warszawa 2020, s. 69–73; G. Pilarski, Tackling cyberspace threats – the international approach, Security and Defence Quarterly 2016, tom. 12, nr 3, s. 100–101, 111–117; S. Żurawski, Z. Ciekanowski, Wpływ zagrożeń w cyberprzestrzeni na bezpieczeństwo państwa, [w:] Współczesne wyzwania dla bezpieczeństwa państwa, red. D. Brążkiewicz, J. Nowicka, Z. Ciekanowski, L. Elak, Warszawa 2023, s. 10, 24–25.

[8] Security Information and Event Management (SIEM) – zarządzanie informacją i zdarzeniami bezpieczeństwa. System do agregacji, korelacji i analizy logów oraz alertów, wykorzystywany w ćwiczeniach do triage, detekcji, analizy incydentów i oceny działań uczestników. Security Operations Center (SOC) – centrum operacji bezpieczeństwa. Funkcja organizacyjna odpowiedzialna za monitorowanie, wykrywanie, analizę i inicjowanie działań reagowania na incydenty bezpieczeństwa.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

grup kompetencji należy podkreślić, że dodatkowe kompetencje komunikacyjne i zespołowe są nieodłącznym elementem, ponieważ wiele scenariuszy CR wymaga pracy zespołowej i współpracy między rolami.

Takie ujęcie odpowiada szerszemu rozumieniu luki kompetencyjnej w cyberbezpieczeństwie. Braki nie dotyczą wyłącznie umiejętności technicznych, ale obejmują również zdolność do analizy sytuacji, komunikację, rozumienie procedur i umiejętność do podejmowania decyzji pod presją. Uczestnik może znać narzędzia oraz podstawowe techniki i procedury obronne, a mimo to mieć trudność z interpretacją sytuacji, wyborem kolejnych kroków, uzasadnieniem decyzji albo współpracą z innymi rolami w scenariuszu ćwiczeniowym[9].

Luka kompetencyjna powinna być zatem interpretowana szerzej niż jako brak umiejętności technicznych. Współczesne zagrożenia cyberprzestrzeni oddziałują na ciągłość działania usług, ochronę informacji, zdolność administracji do reagowania oraz zaufanie do instytucji publicznych. Oznacza to, że personel cyberbezpieczeństwa musi rozumieć nie tylko techniczny przebieg incydentu, lecz także jego konsekwencje organizacyjne i decyzyjne. W takim ujęciu CR może służyć nie tylko ćwiczeniu obsługi narzędzi, ale również budowaniu zdolności do interpretowania sytuacji, eskalacji, komunikacji i dokumentowania działań[10].

Wartością CR jest zatem kluczowa możliwość przełożenia wiedzy na działanie. Uczestnik nie uczy się jedynie o zdarzeniu, lecz działa wobec zdarzenia. Rozpoznaje dane wejściowe, interpretuje je, podejmuje decyzję, wykonuje czynność i pozostawia ślad możliwy do omówienia. Dzięki temu środowisko ćwiczeniowe staje się pomostem między teorią a praktyką, a nie tylko technologiczną demonstracją możliwości platformy. Z tego powodu rośnie znaczenie ćwiczeń symulacyjnych i środowisk CR, które pozwalają uczestnikom pracować na realistycznych zadaniach, analizować dane i uczyć się na podstawie skutków własnych działań[11].

Wprowadzenie w środowisku cyberpoligonu logiki DT w projektowaniu ćwiczeń zwiększa efekt oddziaływania na uczestnika w procesie kształtowania kompetencji personelu. Koncepcja DT nie powinna być utożsamiana z pełnym kopiowaniem infrastruktury produkcyjnej. W kontekście dydaktycznym ważniejsze jest selektywne odwzorowanie tych zależności, które pozwalają uczestnikowi zrozumieć relację między systemem, danymi, decyzją i skutkiem działania. DT pełni więc funkcję filtra dydaktycznego. Nie przenosi do ćwiczenia całej złożoności rzeczywistego środowiska, lecz wybiera te elementy, które są potrzebne do osiągnięcia celu szkoleniowego.

Takie podejście wzmacnia wartość CR, ponieważ pozwala projektować ćwiczenia jako uporządkowany model zależności między systemami, rolami, artefaktami, decyzjami i wskaźnikami oceny. Dzięki temu uczestnik nie tylko wykonuje zadanie techniczne, ale rozumie, dlaczego określone działanie jest potrzebne, jakie ma konsekwencje i jak wpływa na dalszy przebieg scenariusza.

---

[9] J.R.C. Nurse, J. Milward, O. Alashe, From Security Awareness and Training to Human Risk Management in Cybersecurity, w: HCI for Cybersecurity, Privacy and Trust, Springer, 2025, s. 86–104.

[10] Por. G. Pilarski, Przegląd współczesnych zagrożeń w cyberprzestrzeni, Problemy Techniki Uzbrojenia, 2023, t. 167, nr 5, s. 97–106; H. Wyrębek, Z. Ciekanowski, Administracja publiczna w cyberprzestrzeni, Przegląd Policyjny, 2019, t. 136, nr 4, s. 5–22; S. Żurawski, Z. Ciekanowski, Wpływ zagrożeń w cyberprzestrzeni na bezpieczeństwo państwa, [w:] Współczesne wyzwania dla bezpieczeństwa państwa, red. D. Brążkiewicz, J. Nowicka, Z. Ciekanowski, L. Elak, Warszawa 2023, s. 10, 24–25.

[11] N. Chouliaras, G. Kittes, I. Kantzavelou, L. Maglaras, G. Pantziou, M.A. Ferrag, CRs and Test Beds for Education, Training, and Research, Applied Sciences 2021, 11(4), art. 1809, s. 2–5.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Kontrolowany realizm oznacza świadome ograniczenie odwzorowania do tych elementów, które są potrzebne do osiągnięcia celu ćwiczenia i rozwoju określonych kompetencji. Nie chodzi o pełną replikę środowiska produkcyjnego, lecz o model funkcjonalno-zależnościowy, który pozwala uczestnikom ćwiczyć analizę danych, podejmowanie decyzji i dokumentowanie działań bez ujawniania rzeczywistej topologii, konfiguracji, danych lub procedur ochronnych i obronnych[12],[13].

Tak rozumiany kontrolowany realizm ma szczególne znaczenie w odniesieniu do instytucji publicznych i wojskowych. W ich przypadku nie chodzi o odwzorowanie pełnej topologii, rzeczywistych procedur lub konfiguracji, lecz o uchwycenie tych relacji, które decydują o zdolności do reagowania: przepływu informacji, zależności usług, odpowiedzialności ról, punktów eskalacji oraz skutków decyzji. Pozwala to zachować wartość szkoleniową scenariusza, a jednocześnie ograniczyć ryzyko ujawnienia informacji wrażliwych[14].

Na potrzeby projektowania środowiska CR/DT, kontrolowany realizm może być realizowany na trzech poziomach. Najniższy poziom stanowi model logiczny, opisujący zależności i przepływy bez realizacji działań technicznych. Poziom pośredni to model emulacyjny, w którym możliwe jest wykonywanie wybranych interakcji w kontrolowanym środowisku. Poziom najwyższy ma charakter symulacyjny lub hybrydowy i pozwala badać zachowanie systemu oraz wpływ incydentu na proces, usługę lub łańcuch zależności. Dobór poziomu zależy od celu ćwiczenia, ryzyka ujawnienia informacji[15], dostępności danych i wymaganych kluczowych wskaźników efektywności.

Najważniejsze pytanie w zakresie przyjęcia określonego stopnia realizmu nie brzmi: „jak wiernie odwzorować rzeczywistość?", lecz: „jaki poziom odwzorowania jest potrzebny, aby uczestnik mógł rozwinąć określoną kompetencję?". Dla ćwiczenia analitycznego wystarczy czasem zestaw realistycznych logów, alertów i zależności usługowych. Dla ćwiczenia decyzyjnego ważniejszy może być model ról, kanałów komunikacji i konsekwencji wyborów. Dla ćwiczenia technicznego potrzebne będą natomiast elementy emulowane, które pozwolą wykonać konkretne działania.

Wartość CR/DT polega więc nie na maksymalnym skopiowaniu rzeczywistości, lecz na dobraniu takiego poziomu realizmu, który najlepiej wspiera rozwój kompetencji uczestnika[16]. Tak rozumiany DT działa jak filtr dydaktyczny. Nie przenosi do ćwiczenia całej rzeczywistości, ale wybiera te elementy, które są potrzebne do wywołania właściwego problemu poznawczego i praktycznego. Dzięki temu uczestnik nie jest przeciążany zbędnymi szczegółami, a instruktor może skupić ocenę na tych zachowaniach, które rzeczywiście świadczą o rozwoju kompetencji.

---

[12] S. Suhail, R. Jurdak, R. Hussain, Security Attacks and Solutions for DTs, arXiv:2202.12501, 2022, s. 1–2.

[13] B. Airehenbuwa, T. Hasan, S. Sarkar, U. Guin, Advancing Security with DTs: A Comprehensive Survey, arXiv:2505.17310, 2025, s. 1–3, 15–17.

[14] M. Nowikowska, Informacja – jako przedmiot ochrony prawnej – granice jawności [w:] J. Taczkowska-Olszewska, M. Nowikowska, Prawo do informacji publicznej. Informacje niejawne. Ochrona danych osobowych, Warszawa 2019, s. 97-98.

[15] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, t.j. Dz.U. 2025 poz. 1209, art. 1 i 4.

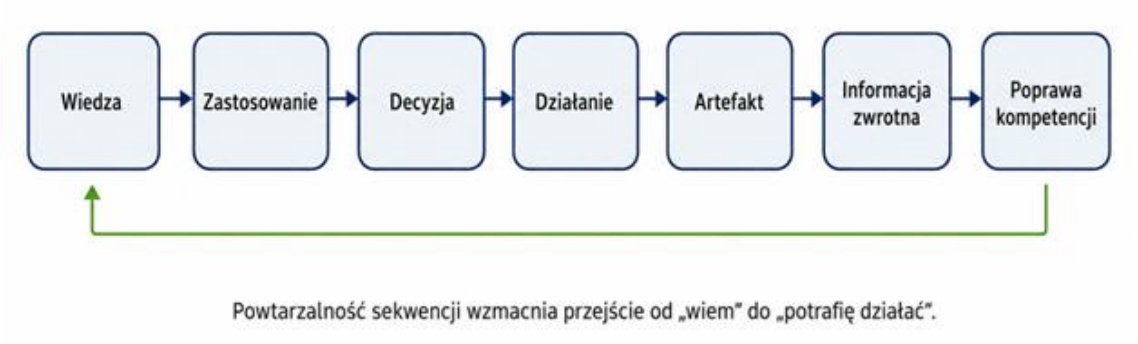
[16] Y. Jiang, W. Wang, J. Ding, X. Lu, Y. Jing, Leveraging DT Technology for Enhanced Cybersecurity in Cyber-Physical Production Systems, Future Internet, 2024, nr 16(4), art. 134, s. 1–5, 8–10, 16–17.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

## Od wiedzy deklaratywnej do kompetencji praktycznej

Rozwój kompetencji nie polega wyłącznie na przyswojeniu wiedzy, ale na zdolności jej zastosowania w określonym kontekście. Wiedza deklaratywna oznacza, że uczestnik potrafi wyjaśnić pojęcie, wskazać procedurę albo rozpoznać definicję. Kompetencja praktyczna oznacza natomiast, że potrafi zastosować tę wiedzę w działaniu (Rysunek 1).

**Rys. 1**. *Model przejścia od wiedzy deklaratywnej do kompetencji praktycznej*




**Źródło:** *opracowanie własne*.

W środowisku CR uczestnik może otrzymać alert, zestaw logów, zgłoszenie, wynik skanowania lub próbkę artefaktu. Następnie powinien ocenić znaczenie informacji, ustalić priorytet, dobrać sposób działania i pozostawić ślad w postaci: notatki, zgłoszenia incydentu (tzw. ticket), raportu, chronologii zdarzeń (tzw. timeline) albo decyzji. Taki ślad umożliwia omówienie sposobu działania i wskazanie elementów wymagających poprawy.

Przewaga CR nad szkoleniem tradycyjnym wynika nie tylko z wykorzystania środowiska technicznego, lecz z możliwości przejścia od wiedzy deklaratywnej do działania. Uczestnik ćwiczenia nie tylko zna procedurę, ale musi ją zastosować w warunkach zadaniowych, przy niepełnej informacji i w relacji z innymi rolami.

Jednym z najważniejszych walorów CR jest możliwość praktycznego nabywania i doskonalenia umiejętności personelu w sytuacji, która nie jest idealnie uporządkowana. Uczestnik nie otrzymuje gotowej odpowiedzi ani listy kroków, lecz zestaw sygnałów, z których część może być niejednoznaczna. Taki model zbliża proces dydaktyczny do realnego sposobu pracy specjalisty cyberbezpieczeństwa, ale nadal pozostaje bezpieczny i kontrolowany. W rozwoju kompetencji technicznych ważna jest poprawność wykonania czynności.

W rozwoju kompetencji analitycznych istotne jest rozumienie, dlaczego dana czynność jest potrzebna. W rozwoju kompetencji decyzyjnych kluczowe staje się uzasadnienie wyboru. Dlatego w środowisku CR/DT uczestnik powinien nie tylko „kliknąć właściwą opcję", ale również pozostawić ślad rozumowania: notatkę, raport, uzasadnienie decyzji albo wpis w systemie zgłoszeniowym.

Mechanizm przejścia od wiedzy deklaratywnej do kompetencji praktycznej polega na tym, że znajomość procedur, pojęć i narzędzi zostaje sprawdzona w sytuacji zadaniowej. W kontekście dydaktycznym kompetencja ujawnia się nie w deklaracji, lecz w sytuacji zadaniowej, czyli wtedy, gdy uczestnik potrafi zastosować wiedzę, zinterpretować dane, uzasadnić decyzję i pozostawić artefakt możliwy do omówienia. Dlatego cyberpoligon może być traktowany jako środowisko walidowania i rozwijania kompetencji, a nie wyłącznie jako narzędzie prezentacji zagrożeń.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Jednym z istotnych elementów budowy środowiska CR/DT są scenariusze ćwiczeniowe. Scenariusz ćwiczenia nie powinien być jedynie opisem ataku lub incydentu. Powinien być narzędziem dydaktycznym, które określa cel ćwiczenia, role uczestników, oczekiwane działania, zdarzenia kontrolne, wymagane artefakty, kryteria oceny i sposób udzielenia informacji zwrotnej.

Scenariusz ćwiczenia powinien być projektowany w logicznym ciągu od określenia celu szkoleniowego, poprzez zdefiniowanie pożądanych efektów, kompetencji i określonych ról uczestników, aż do określenia kryteriów oceny oraz odpowiadających im wskaźników efektywności. Oznacza to, że najpierw określa się, jaką kompetencję uczestnika należy rozwinąć lub zweryfikować, następnie dobiera się role i poziom realizmu, a dopiero później definiuje zdarzenia kontrolne, wymagane artefakty i kryteria oceny[17].

Wymagane role w ćwiczeniu porządkują proces doskonalenia i nabywania umiejętności, przykładowo:

- analityk SOC może odpowiadać za analizę alertów i korelację zdarzeń;
- specjalista IR[18] obejmuje odpowiedzialność za ocenę sytuacji i wybór działań;
- specjalista DFIR[19] przejmuje zakres zadań związanych z zabezpieczeniem oraz analizą artefaktów;
- administrator systemu pełni rolę nadzorczą przy wykonywaniu zmian technicznych;
- zespół red team[20] odpowiada za dostarczenie kontrolowanych technik przeciwnika;
- zespół blue team[21] ćwiczy detekcję i reakcję;
- zespół purple team[22] odpowiednio przekształca doświadczenia z ćwiczenia w poprawę reguł i scenariuszy.

Wprowadzenie komponentu ofensywno-defensywnego nie oznacza jednoznacznie nadania ćwiczeniom charakteru ofensywnego. Jego zasadniczą funkcją jest kontrolowane odtworzenie technik, taktyk i procedur przeciwnika (TTP)[23] w celu doskonalenia detekcji, wstępnej oceny i priorytetyzacji alertów bezpieczeństwa (tzw. triage), reakcji, odporności konfiguracji oraz procedur obronnych (tzw. defensive playbook). Powyższe przykładowe podejście pozwala traktować red team jako źródło realistycznych bodźców szkoleniowych, blue team

---

[17] E. Ear, J.L.C. Remy, S. Xu, Towards Automated CR Design: Characterizing and Matching Demands to Supplies, arXiv:2307.04416, 2023, s. 1–8.

[18] Incident Response (IR) – reagowanie na incydenty. Zestaw procesów i działań obejmujących identyfikację, analizę, ograniczanie skutków, usunięcie przyczyn, odtworzenie działania oraz wyciąganie wniosków z doświadczeń.

[19] Digital Forensics and Incident Response (DFIR) – informatyka śledcza i reagowanie na incydenty. Obszar obejmujący zabezpieczanie, analizę i interpretację artefaktów cyfrowych oraz odtwarzanie przebiegu incydentu na potrzeby reakcji, raportowania i wnioskowania po zdarzeniu.

[20] Red Team – zespół atakujący lub symulujący przeciwnika. Uczestnicy, instruktorzy albo automaty przeciwnika realizujący zaplanowane działania ofensywne w scenariuszu, służące weryfikacji detekcji, reakcji i odporności organizacji.

[21] Blue Team – zespół obronny. Uczestnicy realizujący zadania wykrywania, analizy, reagowania i odtwarzania działania, wykorzystujący narzędzia monitorowania, procedury operacyjne i mechanizmy obronne.

[22] Purple Team – model współpracy ofensywa–defensywa. Forma ćwiczeń, w której Red Team i Blue Team współpracują, aby zwiększyć skuteczność detekcji, zrozumienie TTP przeciwnika oraz usprawnić procedury reagowania.

[23] Tactics, Techniques and Procedures (TTP) – taktyki, techniki i procedury przeciwnika. Opis sposobów działania adwersarza, wykorzystywany do projektowania scenariuszy, mapowania detekcji i oceny reakcji.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

jako zespół reagowania, a purple team jako mechanizm transferu wiedzy między rozpoznaniem sposobu działania przeciwnika a poprawą zdolności obronnych organizacji[24].

Ćwiczenie bazujące na środowisku CR/DT powinno pozostawiać możliwy do analizy ślad dowodowy. Powinien on obejmować między innymi: logi systemowe i zdarzeniowe, zapisy decyzji w komponencie TTX[25], zgłoszenia, punktową ocenę wyniku działania (tzw. scoring), raporty techniczne, wskaźniki kompromitacji (ang. indicators of compromise – IoC)[26], komunikaty sytuacyjne, chronologię przebiegu incydentu oraz wnioski poćwiczeniowe[27].

Artefakty są traktowane przede wszystkim jako pomocnicze narzędzia procesu dydaktycznego, zarówno w tworzeniu scenariusza jak i weryfikacji i ocenie działania uczestnika ćwiczenia. Pozwalają ustalić, które informacje zostały zauważone, które pominięte, gdzie wystąpiły opóźnienia, jakie decyzje podjęto i jak zostały uzasadnione.

Dobrze zaprojektowany scenariusz pełni funkcję mapy uczenia się. Powinien jasno wskazywać, czego uczestnik ma się nauczyć, jakie decyzje ma podjąć, jakie działania wykonać i jakie ślady pozostawić. Jeżeli scenariusz jest jedynie atrakcyjną sekwencją zdarzeń technicznych, może być ciekawy, ale nie musi rozwijać kompetencji. Jeżeli natomiast jest powiązany z rolami, artefaktami i kryteriami oceny, staje się narzędziem dydaktycznym. W tabeli 1 przedstawione zostały relację między formą ćwiczenia, funkcją dydaktyczną i rozwijaną kompetencją.

***Tabela 1.*** *Typ ćwiczenia a rozwijane kompetencje*

| Typ ćwiczenia | Główna funkcja | Rozwijane kompetencje | Powiązane role ECSF |
|---|---|---|---|
| TTX | ćwiczenie decyzyjne i organizacyjne | eskalacja, komunikacja kryzysowa, priorytetyzacja usług, decyzje pod presją | CISO, Cybersecurity Risk Manager, Cyber Legal, Policy & Compliance Officer |
| Hands-on SOC/IR | ćwiczenie techniczne w środowisku range | detekcja, triage, analiza alertów, powstrzymanie i ograniczenie skutków (containment), odtworzenie systemów (recovery) | Cyber Incident Responder, Cybersecurity Implementer |
| DFIR | rekonstrukcja i analiza dowodowa | zabezpieczenie artefaktów, timeline, analiza malware, raportowanie | Digital Forensics Investigator, Cyber Threat Intelligence Specialist |
| Red team - blue team | symulacja działań przeciwnika i obrony | rozpoznanie TTP, detekcja, reakcja, odporność konfiguracji | Penetration Tester, Cyber Incident Responder, |

[24] G. Pilarski, T. Zawadzki, Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, Wiedza Obronna, 2025, tom. 292, nr 3, s. 129–148; G. Pilarski, K. Mikusek, Cyber threats to OT systems in the energy industry, Wiedza Obronna, 2023, tom. 283, nr 2, s. 1–19.

[25] Tabletop Exercise (TTX) – ćwiczenie sztabowe lub decyzyjne. Ćwiczenie prowadzone w formule symulacji proceduralnej i decyzyjnej, ukierunkowane na komunikację, koordynację, eskalację i procesy organizacyjne, bez konieczności pełnego odtworzenia technicznego ataku.

[26] Indicators of Compromise (IoC) – wskaźniki kompromitacji to obserwowalne dane lub ślady wskazujące na możliwość wystąpienia incydentu bezpieczeństwa lub nieuprawnionego naruszenia systemu informatycznego.

[27] ENISA, The ENISA Cybersecurity Exercise Methodology, 2026, s. 5, 20-21, 27-32, 45-49, 62-63.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

| | | | |
|---|---|---|---|
| | | | Cybersecurity Architect |
| Purple team | transfer wiedzy między ofensywą i obroną | walidacja detekcji, poprawa reguł, usprawnianie planów (playbooków) | Penetration Tester, CTI Specialist, Cyber Incident Responder |
| OT/ICS CR/DT | ćwiczenie wpływu incydentu na proces | stabilizacja procesu, izolacja stref, recovery, bezpieczeństwo operacyjne | Cybersecurity Architect, Cybersecurity Implementer, Risk Manager |

***Źródło:*** *opracowanie własne.*

W powyższej tabeli przedstawiono syntetyczne zestawienie zależności między typami ćwiczeń a kompetencjami rozwijanymi w środowisku CR/DT. Ćwiczenie typu TTX wzmacnia kompetencje decyzyjne, typu hands-on SOC/IR[28] rozwija kompetencje techniczne i analityczne, typu DFIR uczy pracy na artefaktach, a zespół purple team wspiera rozumienie relacji między działaniem ofensywnym i defensywnym w procesie uczenia się.

Szczególne znaczenie mają trzy pierwsze obszary: TTX jako przestrzeń decyzji, hands-on SOC/IR jako przestrzeń działania technicznego oraz DFIR jako przestrzeń analizy i dokumentowania. Ich połączenie ogranicza ryzyko jednostronnego, wyłącznie technicznego rozumienia cyberbezpieczeństwa i pozwala rozwijać kompetencje w sposób bardziej zbliżony do realnych zadań personelu.

Warto przy tym zachować język bliski uczestnikowi szkolenia. Dobrze zaprojektowany scenariusz powinien odpowiadać na pytanie: „co mam zrobić, co widzę, dlaczego to jest ważne i jak poznam, że zrobiłem to dobrze?”. Takie ujęcie wzmacnia przejrzystość ćwiczenia i ułatwia późniejszą analizę poćwiczeniową.

W tym zakresie pomocne stają się określone mierzalne wskaźniki takie jak kluczowe wskaźniki efektywności (ang. Key Performance Indicators - KPI)[29] i system oceny punktowej (tzw. scoring)[30]. Jednakże wskaźniki te powinny być traktowane jako narzędzia wspierające rozwój kompetencji, a nie wyłącznie jako mechanizmy kontroli lub klasyfikacji uczestników. Pomiar ma sens wtedy, gdy prowadzi do informacji zwrotnej, porządkuje obserwacje instruktora i pomaga uczestnikowi zrozumieć własny sposób działania.

W środowisku CR/DT kluczowe wskaźniki efektywności powinny być projektowane razem ze scenariuszem, a nie dopisywane po zakończeniu ćwiczenia. Każde KPI powinno mieć definicję, źródło danych, regułę liczenia, próg interpretacyjny oraz powiązanie z rolą lub kompetencją. Dopiero wtedy wynik ćwiczenia może być porównywany między iteracjami i wykorzystywany do planowania dalszych działań szkoleniowych[31].

[28] Hands-on SOC/IR oznacza praktyczne, oparte na bezpośrednim wykonywaniu zadań szkolenie lub ćwiczenia z zakresu SOC i reagowania na incydenty.

[29] Key Performance Indicators (KPI) – kluczowe wskaźniki efektywności. Zestaw wskaźników ilościowych i jakościowych stosowanych do oceny skuteczności treningu, sprawności działań operacyjnych i postępu kompetencyjnego uczestników ćwiczeń.

[30] Scoring – punktowa ocena wykonania scenariusza. Mechanizm przyznawania punktów za osiągnięcie określonych celów, wykonanie zadań, poprawność reakcji, kompletność artefaktów i zgodność z procedurami.

[31] ENISA, The ENISA Cybersecurity Exercise Methodology, version 1.0, 2026, s. 51-55; K. Wetzel, S. Grayson, K. Santos, NICE Framework Competency Areas: Assessing Learners and Audiences Against Workforce Competencies, NIST IR 8355, 2023, s. 3, 7; ENISA, European Cybersecurity Skills Framework User Manual, 2022, s. 12, 24-25.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Wskaźniki można uporządkować w trzech grupach. Pierwszą stanowią wskaźniki wiedzy, obejmujące wynik testu, poprawność rozpoznania pojęć i znajomość procedur. Drugą stanowią wskaźniki działania: czas reakcji, poprawność triage, trafność analizy, kompletność raportu i jakość wykonanych czynności. Trzecią stanowią wskaźniki współpracy: jakość komunikacji, kompletność przekazania informacji oraz współdziałanie między rolami.

Scoring jest tu rozumiany jako syntetyczna operacjonalizacja scenariusza, czyli sposób zamiany zdarzeń kontrolnych, warunków zaliczenia i jakości artefaktów na wynik punktowy. Nie zastępuje on KPI ani oceny instruktorskiej, lecz porządkuje wykonanie scenariusza i ułatwia porównanie kolejnych iteracji ćwiczenia.

Skuteczna ewaluacja wymaga powiązania celów scenariusza z mierzalnymi zdarzeniami kontrolnymi. Macierz scenariusza powinna wskazywać, jakie działania są oczekiwane, które role są odpowiedzialne za ich wykonanie, jakie artefakty mają powstać, jakie KPI zostaną zmierzone i w jaki sposób wynik zostanie przełożony na scoring[32].

Pomiar w środowisku cyberpoligonu nie powinien być odbierany przez uczestnika jedynie jako mechanizm oceny. Jego podstawowa wartość polega na tym, że pomaga zobaczyć własny sposób działania. Uczestnik może dowiedzieć się, gdzie stracił czas, które sygnały pominął, który raport był niekompletny, a która decyzja była poprawna, ale zbyt późna. Taka informacja jest bardziej rozwojowa niż sama liczba punktów.

Najbardziej użyteczny model informacji zwrotnej powinien łączyć trzy wymiary: czas, jakość i proces. Wymiar czasu pokazuje tempo rozpoznania, klasyfikacji i wykonania zadania. Wymiar jakości dotyczy poprawności analizy, trafności decyzji, kompletności dokumentowania i jakości raportowania. Wymiar procesu pozwala sprawdzić, czy uczestnik działał logicznie, konsekwentnie i zgodnie z wymaganiami scenariusza[33].

Model czasu, jakości i procesu można traktować jako praktyczny model informacji zwrotnej. Czas pokazuje tempo uczenia się i działania, jakość pokazuje poprawność rozumowania, a proces pokazuje spójność kolejnych kroków. Dopiero te trzy perspektywy razem pozwalają powiedzieć, czy uczestnik rzeczywiście rozwija kompetencje.

Z perspektywy języka bliskiego uczestnikowi ważne jest, aby informacja zwrotna była zrozumiała i możliwa do przełożenia na następne działanie. Komunikat „uzyskałeś 70 punktów” ma ograniczoną wartość. Komunikat „dobrze rozpoznałeś alert, ale pominąłeś korelację z logami uwierzytelnienia i dlatego eskalacja była opóźniona” buduje realną ścieżkę poprawy działania.

Jednym z kluczowych elementów wpływających na budowanie i rozwój kompetencji jest analiza poćwiczeniowa czyli analiza/raport poćwiczeniowy (ang. After Action Review/Report - AAR)[34]. Jest to ustrukturyzowane omówienie przebiegu ćwiczenia, obejmujące ocenę realizacji celów, identyfikację mocnych i słabych stron, analizę decyzji uczestników, ocenę artefaktów oraz sformułowanie działań korygujących. Jej podstawową funkcją jest

[32] ENISA, The ENISA Cybersecurity Exercise Methodology, version 1.0, 2026, s. 31, 40, 61.
[33] A. Nelson, J. McCarthy, R.R. Petersen, K. Scarfone, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile, NIST SP 800-61 Rev. 3, National Institute of Standards and Technology, 2025, s. 19, s. 27-28, s. 34.
[34] After Action Review/Report (AAR) – analiza/raport poćwiczeniowy. Ustrukturyzowane omówienie przebiegu ćwiczenia, obejmujące ocenę realizacji celów, identyfikację mocnych i słabych stron, analizę decyzji uczestników, ocenę artefaktów oraz sformułowanie działań korygujących.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

przekształcenie doświadczenia w świadome uczenie się, identyfikację luk kompetencyjnych i planowanie dalszego rozwoju uczestnika. Pełni funkcję mechanizmu doskonalenia umiejętności uczestnika i zespołu ćwiczeniowego. Jej celem jest nie tylko wskazanie błędów, lecz także określenie, które elementy wiedzy, analizy, decyzji lub dokumentowania wymagają wzmocnienia przed kolejną iteracją[35],[36].

W wymiarze dydaktycznym analiza poćwiczeniowa powinna odpowiadać na pytania: „co uczestnik miał zrobić?", „co rzeczywiście zrobił?", „dlaczego podjął określone decyzje?", „jakie działania wykonał poprawnie?", „gdzie pojawiły się błędy lub luki kompetencyjne?" i „jakie działania rozwojowe powinien podjąć przed kolejnym ćwiczeniem?". Podejście iteracyjne wzmacniają modele oparte na cyklu życia ćwiczenia cyberbezpieczeństwa (tzw. cyber exercise lifecycle), w których scenariusz, role, dane wejściowe, metryki i ewaluacja są traktowane jako powiązane elementy procesu. Zastosowanie takiego modelu pozwala zmniejszać przypadkowość ćwiczeń, poprawiać ich dopasowanie do celu oraz zwiększać możliwość porównywania wyników między iteracjami[37].

Analiza poćwiczeniowa powinna być prowadzona językiem rozwoju, a nie wyłącznie językiem błędu. Jej celem nie jest wskazanie, kto „zawinił", ale zrozumienie, jakie elementy kompetencji wymagają wzmocnienia. W tym sensie AAR stanowi ustrukturyzowany proces analizy przebiegu ćwiczenia, w którym uczestnik dowiaduje się o tym: co zobaczył, czego nie zauważył, jak rozumował i co może zrobić inaczej w kolejnym ćwiczeniu. Praktyczna wartość AAR rośnie wtedy, gdy wnioski są jednoznaczne, mierzalne i możliwe do wdrożenia. Zamiast ogólnego stwierdzenia „poprawić analizę alertów", lepiej wskazać: „w kolejnej iteracji uczestnik powinien ćwiczyć korelację alertów EDR z logami AD"[38]. W przedstawionej postaci wniosek staje się zadaniem rozwojowym.

W praktyce model wieloźródłowy powinien prowadzić do omówienia, w którym każdy wniosek jest powiązany z dowodem: logiem, decyzją, wynikiem KPI, obserwacją instruktora, wypowiedzią uczestnika lub artefaktem poćwiczeniowym. Dzięki temu AAR nie jest ogólnym podsumowaniem szkolenia, lecz konkretną informacją zwrotną wspierającą dalszy rozwój kompetencji.

## Podsumowanie

Na podstawie przeprowadzonych badań można stwierdzić, że środowisko Cyber Range z powiązaną logiką Digital Twin może skutecznie wspierać rozwój kompetencji personelu cyberbezpieczeństwa. Skuteczność proponowanego rozwiązania opiera się na założeniu, że środowisko CR/DT nie jest traktowane jako samodzielne rozwiązanie technologiczne, lecz jako element metodycznie zaprojektowanego procesu przygotowania personelu do realizacji zadań w cyberprzestrzeni.

Znaczenie środowiska cyberpoligonu polega na tym, że umożliwia uczestnikowi działanie w scenariuszu, podejmowanie decyzji, pracę na artefaktach i otrzymywanie informacji zwrotnej. Natomiast użyteczność DT w proponowanym rozwiązaniu wynika z możliwości selektywnego odwzorowania zależności

[35] ENISA, Cyber Europe 2024 After Action Report, 2024, s. 6–8, 20, 24–26, 28, 32–35.
[36] ENISA, Best Practices for Cyber Crisis Management, 2024, s. 18–23, 39–40, 44–45.
[37] T. Pfaller, F. Skopik, P. Smith, M. Leitner, Towards Customized Cyber Exercises using a Process-based Cyber Exercise Lifecycle Model, 2024, s. 2, 4-8, 10-12.
[38] EDR z logami AD oznacza połączenie danych z EDR (Endpoint Detection and Response) zlogami Active Directory (AD).

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

technicznych, organizacyjnych i procesowych istotnych dla celu prowadzenia ćwiczenia. W tym aspekcie kluczowe znaczenie ma kontrolowany realizm. Ćwiczenie powinno być wystarczająco wiarygodne, aby angażować uczestnika i wymuszać działanie, ale jednocześnie na tyle bezpieczne, aby nie ujawniać rzeczywistych danych, konfiguracji, procedur ani zależności organizacyjnych. Istotą nie jest zatem maksymalne skopiowanie rzeczywistości, lecz o dobranie takiego poziomu odwzorowania, który najlepiej wspiera rozwój określonych kompetencji.

Skuteczność środowiska CR/DT zależy przede wszystkim od jakości scenariusza, jasności ról, właściwego doboru artefaktów oraz sposobu wykorzystania mierzalnych wskaźników efektywności, systemu oceny punktowej oraz analizy poćwiczeniowej. Pomiar nie powinien sprowadzać się tylko do punktacji. Jego podstawową funkcją powinna być informacja zwrotna, która pozwala uczestnikowi zidentyfikować: co zrobił poprawnie, jakie sygnały pominął, które decyzje były trafne lub opóźnione oraz co powinien poprawić w kolejnej iteracji.

Ograniczeniem modelu jest ryzyko nadmiernej koncentracji na aspektach technicznych ćwiczeń. Jeżeli scenariusz koncentruje się wyłącznie na obsłudze narzędzi, może pomijać kompetencje analityczne, decyzyjne, komunikacyjne oraz organizacyjne. Podobnie nadmierny realizm może zwiększać ryzyko ujawnienia informacji wrażliwych, a uproszczona punktowa ocena może spłaszczać ocenę kompetencji. Dlatego rozwój kompetencji wymaga periodyczności, informacji zwrotnej i stałego doskonalenia scenariuszy.

W szerszej perspektywie środowisko CR/DT może być traktowane jako narzędzie wzmacniania cyberodporności organizacji. Współczesne incydenty cyberbezpieczeństwa nie kończą się na warstwie technicznej, lecz wpływają na ciągłość usług, jakość decyzji, komunikację, zaufanie do instytucji i zdolność odtwarzania działania. Dlatego rozwój kompetencji personelu powinien być powiązany z ćwiczeniem procedur, komunikacji, eskalacji, dokumentowania decyzji oraz analizy poćwiczeniowej.

Kluczowym wnioskiem z przeprowadzonych badań jest spostrzeżenie, że technologia nie zastąpi metodyki[39]. Nawet zaawansowane środowisko cyberpoligonu będzie miało ograniczoną wartość, jeżeli scenariusze są przypadkowe, role niejasne, a informacja zwrotna sprowadza się tylko do liczby uzyskanych punktów. Z kolei dobrze zaprojektowane środowisko, nawet prostsze technologicznie, może skutecznie budować i doskonalić kompetencje, jeżeli prowadzi uczestnika od wiedzy, przez decyzję i działanie, do refleksji oraz poprawy sposobu działania.

## Bibliografia

Airehenbuwa B., Hasan T., Sarkar S., Guin U., Advancing Security with Digital Twins: A Comprehensive Survey, arXiv:2505.17310, 2025.

Ciekanowski Z., Wyrębek H., Współczesne technologie informatyczne – szanse i zagrożenia, De Securitate et Defensione. O Bezpieczeństwie i Obronności, 2017, nr 1(3).

[39] Por. M. G. Pilarski, The Concept of Recommender System Supporting Command and Control System in Hierarchical Organization, 2014 European Network Intelligence Conference, Wroclaw, Poland 2014, s. 140, doi: 10.1109/ENIC.2014.9.

The article is licensed under a Creative Commons Attribution-ShareAlike 4.0 Unported (CC BY-SA)

Chouliaras N., Kittes G., Kantzavelou I., Maglaras L., Pantziou G., Ferrag M.A., Cyber Ranges and TestBeds for Education, Training, and Research, Applied Sciences, 2021, vol. 11, nr 4.

Ear E., Remy J.L.C., Xu S., Towards Automated Cyber Range Design: Characterizing and Matching Demands to Supplies, arXiv:2307.04416, 2023.

Jiang Y., Wang W., Ding J., Lu X., Jing Y., Leveraging Digital Twin Technology for Enhanced Cybersecurity in Cyber-Physical Production Systems, Future Internet, 2024, vol. 16, nr 4.

Nowikowska M., Informacja – jako przedmiot ochrony prawnej – granice jawności [w:] J. Taczkowska-Olszewska, M. Nowikowska, Prawo do informacji publicznej. Informacje niejawne. Ochrona danych osobowych, Warszawa 2019.

Nurse J.R.C., Milward J., Alashe O., From Security Awareness and Training to Human Risk Management in Cybersecurity, w: HCI for Cybersecurity, Privacy and Trust, Springer 2025.

Ostolski P., The role of digital skills in the changing cybersecurity environment, Cybersecurity and Law, 2025, Nr 2 (14).

Pfaller T., Skopik F., Smith P., Leitner M., Towards Customized Cyber Exercises Using a Process-based Cyber Exercise Lifecycle Model 2024.

Pilarski G., Cyberprzestrzeń – relacje w wojnie hybrydowej, Warszawa 2020.

Pilarski G., Nowikowska M., Galemba P., Deepfake technology: definition, characteristics of the phenomenon, and mechanisms of operation, Cybersecurity and Law, 2025, Nr 2(14).

Pilarski G., Tackling cyberspace threats – the international approach, Security and Defence Quarterly, 2016, t. 12, nr 3.

Pilarski G., Przegląd współczesnych zagrożeń w cyberprzestrzeni, Problemy Techniki Uzbrojenia 2023, t. 167, nr 5.

Pilarski G., Mikusek K., Cyber threats to OT systems in the energy industry, Wiedza Obronna 2023, t. 283, nr 2.

Pilarski G., The Concept of Recommender System Supporting Command and Control System in Hierarchical Organization, 2014 European Network Intelligence Conference, Wroclaw, Poland, 2014, doi: 10.1109/ENIC.2014.9.

Pilarski G., Zawadzki T., Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, Wiedza Obronna 2025, t. 292, nr 3.

Suhail S., Jurdak R., Hussain R., Security Attacks and Solutions for Digital Twins, arXiv:2202.12501, 2022.

Wyrębek H., Ciekanowski Z., Administracja publiczna w cyberprzestrzeni, Przegląd Policyjny 2019, t. 136, nr 4.

Żurawski S., Ciekanowski Z., Wpływ zagrożeń w cyberprzestrzeni na bezpieczeństwo państwa, [w:] Współczesne wyzwania dla bezpieczeństwa państwa, red. D. Brążkiewicz, J. Nowicka, Z. Ciekanowski, L. Elak, Warszawa 2023.