



fundacja instytut
CYBERBEZPIECZEŃSTWA

Cyberbezpieczeństwo transportu kolejowego i lotniczego w kontekście działań terrorystycznych

dr Sławomir Żurawski



Fundusz
Sprawiedliwości



Ministerstwo
Sprawiedliwości

Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości



Wprowadzenie

Transport kolejowy i lotniczy stanowi kluczowy element infrastruktury krytycznej każdego państwa. Od jego sprawnego funkcjonowania zależy nie tylko mobilność ludności, lecz także bezpieczeństwo gospodarcze, logistyczne i militarne. W ostatnich latach obserwuje się gwałtowny wzrost liczby cyberataków skierowanych przeciwko sektorowi transportu, które coraz częściej mają charakter hybrydowy i łączą klasyczne techniki sabotażu z działaniami w cyberprzestrzeni.

W kontekście zagrożeń terrorystycznych przestrzeń cyfrowa staje się nowym polem walki, w którym możliwe jest sparaliżowanie całych sieci transportowych bez użycia siły fizycznej. Dane Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) z 2025 r. wskazują, że sektor transportowy był jednym z najczęściej atakowanych w UE, a wśród dominujących metod odnotowano ataki typu ransomware, kradzieże danych, sabotaż systemów sterowania ruchem oraz ataki DDoS mające na celu unieruchomienie infrastruktury informatycznej operatorów¹. Współczesny terroryzm wykorzystuje zatem cyberprzestrzeń jako instrument destabilizacji, co stanowi poważne wyzwanie dla bezpieczeństwa państw i organizacji międzynarodowych.

1 ENISA Threat Landscape 2025, s. 15.

Cyberzagrożenia w transporcie kolejowym - przypadki z Polski i świata

W sierpniu 2023 r. w północno-wschodniej Polsce doszło do poważnego incydentu, który zwrócił uwagę opinii publicznej i ekspertów ds. bezpieczeństwa. Nieznani sprawcy nadali nieuprawnione sygnały radiowe „radio-stop”, które spowodowały zatrzymanie 12 pociągów². Incydent ten był możliwy z wykorzystaniem prostych urządzeń nadawczych działających w paśmie VHF, co obnażyło przestarzałość systemów łączności stosowanych w części polskiej infrastruktury kolejowej. W nagraniach radiowych zarejestrowano m.in. hymn Federacji Rosyjskiej, co nadało sprawie charakter prowokacji informacyjnej. Choć zatrzymanie pociągów nie spowodowało katastrofy, to ujawniło poważne luki w systemie bezpieczeństwa i brak odpowiednich zabezpieczeń przed ingerencją w transmisję sygnałów. W kontekście toczącej się wojny w Ukrainie oraz wzmożonego tranzytu wojskowego i humanitarnego przez Polskę incydent ten miał znaczenie strategiczne. Ukazał, jak niewielkim nakładem środków

można spowodować poważne zakłócenia w kluczowej infrastrukturze logistycznej.

Podobny charakter miał atak przeprowadzony w styczniu 2022 r. na białoruską sieć kolejową przez grupę hakerską Belarussian Cyber-Partisans. Celem cyberataków było zablokowanie systemów zarządzania ruchem kolejowym oraz uniemożliwienie transportu wojsk rosyjskich przez terytorium Białorusi. Sprawcy zaszyfrowali systemy informatyczne przedsiębiorstwa i zażądali zwolnienia więźniów politycznych oraz zaprzestania wspierania rosyjskiej agresji na Ukrainę³. Był to precedensowy przypadek, kiedy cyberatak miał wymiar polityczny, a jego celem było wymuszenie zmian decyzji rządowych. Tego typu działania wpisują się w nową kategorię terroryzmu cyfrowego, w którym środki informatyczne służą osiągnięciu celów ideologicznych.

Warto również przytoczyć incydent z Danii z października 2022 r., kiedy to duńska sieć kolejowa została unieruchomiona w wyni-

2 Kolejne incydenty na kolei z sygnałem radio-stop. Stanęło 12 pociągów, CyberDefence24, 29.08.2023, <https://cyberdefence24.pl/cyberbezpieczenstwo/kolejne-incydenty-na-kolei-z-sygnalem-radio-stop-stanelo-12-pociagow> (dostęp: 03.11.2025 r.).

3 T. Balmforth, Belarusian group claims hack on railway system after Russian troop moves, Reuters, 24.01.2022, <https://www.reuters.com/legal/litigation/belarusian-group-claims-hack-railway-system-after-russian-troop-moves-2022-01-24/> (dostęp: 03.11.2025 r.).



ku ataku na oprogramowanie dostarczone przez firmę Supeo – zewnętrznego dostawcę aplikacji dla operatora DSB⁴. Choć sam przewoźnik nie został bezpośrednio zaatakowany, to awaria środowiska testowego dostawcy spowodowała paraliż ruchu pociągów w całym kraju. Pokazuje to, jak duże znaczenie ma zarządzanie ryzykiem w łańcuchu dostaw, w którym słabe ogniwo

może doprowadzić do kryzysu o charakterze narodowym.

Kolejnym przykładem jest atak na kolej irańską z lipca 2021 r., podczas którego hakerzy włamali się do systemów informacyjnych i wyświetlili na tablicach dworcowych fałszywe komunikaty o opóźnieniach pociągów oraz numer infolinii rzekomo pro-

4 Danish train standstill on Saturday caused by cyber attack, Reuters, 3.11.2022, <https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/> (dostęp: 03.11.2025 r.).

wadzącej do biura najwyższego przywódcy Iranu⁵. Celem tej operacji nie była fizyczna destrukcja infrastruktury, lecz kompromitacja instytucji i wywołanie chaosu informacyjnego wśród obywateli.

We wrześniu 2024 r. w Wielkiej Brytanii operator Transport for London został dotknięty cyberincydentem: atak spowodował naruszenie danych klientów (około 5000 osób) i wymusił reset haseł pracowników. Usługi kolejowe i autobusowe pozostały operacyjne, ale wprowadzono ograniczenia w dostępności niektórych funkcji online⁶. To pokazuje, że nawet gdy ruch podstawowy nie został zakłócony, zakłócenia w syste-

mach obsługi mogą mieć wpływ na zaufanie oraz operacje.

Wszystkie te przypadki pokazują, że cyberatak na kolej może mieć różny charakter, od prostego sabotażu radiowego po zaawansowane działania propagandowe i psychologiczne, jednak ich wspólnym mianownikiem jest zdolność do zakłócania funkcjonowania państwa bez użycia tradycyjnych środków przemocy. Współczesne ataki na kolej przybierają wielowątkową postać i wykorzystują zarówno nowoczesne instrumenty cybernetyczne, jak i proste, analogowe środki, które wciąż funkcjonują w infrastrukturze kolejowej.

Cyberzagrożenia w lotnictwie - ataki na systemy naziemne i informacyjne

Transport lotniczy, podobnie jak kolejowy, opiera się na złożonych systemach teleinformatycznych, które zarządzają ruchem, planami lotów i obsługą pasażerów. Już w czerwcu 2015 r. Polska doświadczyła jednego z pierwszych głośnych incydentów tego typu. Cyberatak na systemy operacji naziemnych Polskich Linii Lotniczych LOT spowodował odwołanie 10 rejsów i spara-

lizował obsługę około 1400 pasażerów na warszawskim lotnisku Chopina⁷. Choć nie doszło do naruszenia bezpieczeństwa w powietrzu, to atak pokazał, jak łatwo można sparaliżować działalność lotniczą przez ingerencję w systemy planowania i koordynacji lotów. Ekspertki wskazywali wówczas, że systemy te nie posiadały odpowiednich mechanizmów uwierzytelniania i segmen-

5 Hackers disrupt Iran's rail service with fake delay messages, AP News, 10.07.2021, <https://apnews.com/article/middle-east-technology-iran-a1690f768777b25bc8a8fe6d94bf8669> (dostęp: 03.11.2025 r.).

6 F. Ruiz, Attacks against the transportation sector: 10 recent critical security breaches, Fluid Attacks, 6.02.2025, <https://fluidattacks.com/pt/blog/attacks-against-transportation-sector> (dostęp: 03.11.2025 r.).

7 Hackers ground 1,400 passengers at Warsaw in attack on airline's computers, The Guardian, 21.06.2015, <https://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot> (dostęp: 03.11.2025 r.).



tacji sieci, co umożliwiło dostęp z zewnątrz. Dla polskiego sektora lotniczego był to ważny sygnał ostrzegawczy, który przyspieszył procesy modernizacyjne w zakresie cyberbezpieczeństwa.

Równie istotne okazały się wydarzenia z października 2022 r. w Stanach Zjednoczonych, kiedy to grupa prorosyjskich hakerów Killnet przeprowadziła serię ataków DDoS na portale internetowe największych lotnisk, w tym w Atlancie, Los Angeles, Chicago i Nowym Jorku⁸. Mimo że same operacje lotnicze nie zostały sparaliżowane, ataki doprowadziły do chwilowej niedostępności stron internetowych, na których pasażerowie sprawdzali informacje o lotach i rezer-

wacjach. Miało to wymiar propagandowy i psychologiczny. Celem było wywołanie dezorganizacji oraz paniki wśród użytkowników usług lotniczych.

Tego typu działania pokazują, że współczesny terroryzm nie zawsze dąży do fizycznego zniszczenia infrastruktury, lecz coraz częściej wykorzystuje cyberprzestrzeń do tworzenia poczucia zagrożenia i niepewności społecznej. W branży lotniczej raporty z 2024 r. wskazują, że 55% organizacji lotniczych miało do czynienia z atakiem ransomware w ciągu poprzednich 12 miesięcy; wzrosła także liczba incydentów związanych z dronami (średnio 21 zagrożeń dronowych na respondenta⁹).

8 G. Wallace i in., Russian-speaking hackers knock multiple US airport websites offline. No impact on operations reported, CNN, 10.10.2022, <https://edition.cnn.com/2022/10/10/us/airport-websites-russia-hackers> (dostęp: 03.11.2025 r.).

9 US Cybersecurity in Aviation: 2024, Bridewell, <https://www.bridewell.com/us/insights/white-papers/detail/cybersecurity-in-aviation-2024> (dostęp: 03.11.2025 r.).

W odpowiedzi na rosnące zagrożenia Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA) opracowała nowe regulacje dotyczące bezpieczeństwa informacyjnego, znane jako Part-IS (Information Security), które nakładają na przewoźników i porty lotnicze obowiązek wdrożenia systemów zarządzania ryzykiem w obszarze IT i OT¹⁰. Równolegle dyrektywa NIS2 wprowadza obowiązek raportowania incydentów oraz rozszerza zakres odpowiedzialności menedżerów za bezpieczeństwo cyfrowe w sektorze transportowym. Przykłady

z Polski i USA dowodzą, że cyberbezpieczeństwo lotnictwa nie może ograniczać się wyłącznie do zabezpieczenia samolotów, lecz musi obejmować całe zaplecze informacyjne, w tym systemy naziemne, aplikacje pasażerskie oraz kanały komunikacji publicznej. Współczesne ataki pokazują bowiem, że najłatwiej uderzyć w obszary, które nie są bezpośrednio objęte procedurami bezpieczeństwa lotniczego, ale mają kluczowe znaczenie dla funkcjonowania całego systemu.

Zakończenie

Analiza przypadków z Polski, Białorusi, Danii, Iranu oraz Stanów Zjednoczonych pokazuje, że cyberprzestrzeń stała się nowym polem działań terrorystycznych wymierzonych w transport kolejowy i lotniczy. Choć większość z tych incydentów nie doprowadziła do katastrof, to ich skutki społeczne, ekonomiczne i wizerunkowe były znaczące. Wspólnym mianownikiem tych przykładów jest łatwość przeprowadzenia ataku przy niewielkich nakładach finansowych i technicznych. Paraliż infrastruktury transportowej nawet na kilka godzin może prowadzić do poważnych strat gospodarczych, a w sytuacji konfliktu zbrojnego – do zaburzenia łańcuchów dostaw i mobilności wojskowej. Przypadek „radio-stop” w Polsce pokazał, że nawet przestarzałe technologie mogą

stać się celem sabotażu, atak na PLL LOT udowodnił natomiast, że wrażliwym punktem lotnictwa są systemy naziemne. W kontekście tych doświadczeń konieczne jest konsekwentne wdrażanie unijnych regulacji NIS2 i EASA Part-IS, rozwijanie współpracy międzynarodowej w zakresie wymiany informacji o zagrożeniach oraz prowadzenie regularnych ćwiczeń z udziałem operatorów transportu, służb i administracji publicznej. Cyberbezpieczeństwo transportu nie jest już kwestią techniczną, lecz strategicznym elementem bezpieczeństwa narodowego, którego zaniedbanie może prowadzić do destabilizacji całych państw.

10 EASA, Information Security (Part-IS), 2025, <https://www.easa.europa.eu> (dostęp: 03.11.2025 r.).

Źródła

- Balmforth T., Belarusian group claims hack on railway system after Russian troop moves, Reuters, 24.01.2022, <https://www.reuters.com/legal/litigation/belarusian-group-claims-hack-railway-system-after-russian-troop-moves-2022-01-24/> (dostęp: 03.11.2025 r.).
- Danish train standstill on Saturday caused by cyber-attack, Reuters, 3.11.2022, <https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/> (dostęp: 03.11.2025 r.).
- ENISA Threat Landscape 2025.
- EASA, Information Security (Part-IS), 2025, <https://www.easa.europa.eu> (dostęp: 03.11.2025 r.).
- Hackers disrupt Iran's rail service with fake delay messages, AP News, 10.07.2021, <https://apnews.com/article/middle-east-technology-iran-a1690f768777b25bc8a8fe6d94bf8669> (dostęp: 03.11.2025 r.).
- Hackers ground 1,400 passengers at Warsaw in attack on airline's computers, The Guardian, 21.06.2015, <https://www.theguardian.com/business/2015/jun/21/hackers-1400-passengers-warsaw-lot> (dostęp: 03.11.2025 r.).
- Kolejne incydenty na kolei z sygnałem radio-stop. Stanęło 12 pociągów, CyberDefence24, 29.08.2023, <https://cyberdefence24.pl/cyberbezpieczenstwo/kolejne-incydenty-na-kolei-z-sygnalem-radio-stop-stanelo-12-pociagow> (dostęp: 03.11.2025 r.).
- Ruiz F., Attacks against the transportation sector: 10 recent critical security breaches, Fluid Attacks, 6.02.2025, <https://fluidattacks.com/pt/blog/attacks-against-transportation-sector> (dostęp: 03.11.2025 r.).
- US Cybersecurity in Aviation: 2024, Bridewell, <https://www.bridewell.com/us/insights/white-papers/detail/cybersecurity-in-aviation-2024> (dostęp: 03.11.2025 r.).
- Wallace G., Lyngaas S., Muntean P., Watson M., Russian-speaking hackers knock multiple US airport websites offline. No impact on operations reported, CNN, 10.10.2022, <https://edition.cnn.com/2022/10/10/us/airport-websites-russia-hackers> (dostęp: 03.11.2025 r.).



Fundusz
Sprawiedliwości



Ministerstwo
Sprawiedliwości

Sfinansowano ze środków Funduszu Sprawiedliwości, którego dysponentem jest Minister Sprawiedliwości

www.instytutcyber.pl



fundacja instytut
CYBERBEZPIECZEŃSTWA