Kacper Minda https://orcid.org/0009-0005-6152-5016
Wyższa Szkoła Biznesu i Nauk o Zdrowiu, Instytut Prawa i Kryminologii
e-mail: kacperminda@wp.pl

Sebastian Seliga https://orcid.org/0009-0009-7061-5450
Wyższa Szkoła Biznesu i Nauk o Zdrowiu, Instytut Prawa i Kryminologii
e-mail: seligasebastian@gmail.com

Innowacyjne podejście do zarządzania bezpieczeństwem państwa w walce z terroryzmem

An innovative approach to state security management in the fight against terrorism

https://doi.org/10.25312/ziwgib.904

Streszczenie

Cyfryzacja i sieciowy charakter współczesnego terroryzmu zwiększają znaczenie elastycznego oraz zintegrowanego zarządzania bezpieczeństwem państwa. Celem artykułu jest określenie roli innowacyjnych rozwiązań organizacyjnych i technologicznych w zapobieganiu zagrożeniom terrorystycznym oraz ograniczaniu ich skutków. Opracowanie ma charakter przeglądowo-analityczny i opiera się na jakościowej analizie literatury naukowej, raportów oraz dokumentów instytucjonalnych dotyczących terroryzmu, cyberbezpieczeństwa i zarządzania kryzysowego. Analizie poddano wykorzystanie narzędzi analitycznych, ochronę infrastruktury krytycznej, przeciwdziałanie finansowaniu i propagandzie, koordynację międzyinstytucjonalną, współpracę międzynarodową oraz współdziałanie sektora publicznego i prywatnego. Ustalono, że sama implementacja nowych technologii nie przesądza o skuteczności systemu. Kluczowe są jakość danych, nadzór człowieka, sprawny przepływ informacji, jasny podział kompetencji, interoperacyjność służb oraz przygotowanie wszystkich faz zarządzania kryzysowego. Innowacyjne zarządzanie bezpieczeństwem zwiększa zdolność

państwa do wcześniejszego rozpoznawania zagrożeń i szybszego reagowania, pod warunkiem połączenia technologii z rozwiązaniami organizacyjnymi, społecznymi i prawnymi oraz poszanowaniem praw jednostki.

Słowa kluczowe: terroryzm, zarządzanie bezpieczeństwem, cyberbezpieczeństwo, infrastruktura krytyczna, zarządzanie kryzysowe, nowe technologie, współpraca międzyinstytucjonalna

Abstract

Digitalization and the networked nature of contemporary terrorism increase the importance of flexible and integrated state security management. This article aims to determine the role of organizational and technological innovation in preventing terrorist threats and mitigating their consequences. It adopts a review-based analytical approach and draws on a qualitative analysis of academic literature, institutional reports, and documents concerning terrorism, cybersecurity, and crisis management. The study examines analytical tools, critical infrastructure protection, countering terrorist financing and propaganda, interinstitutional coordination, international cooperation, and public-private partnerships. The findings show that technology alone does not determine the effectiveness of counter-terrorism systems. Data quality, human oversight, efficient information exchange, clear allocation of responsibilities, interoperability, and preparedness across all phases of crisis management are equally important. Innovative security management improves the state's capacity to detect threats earlier and respond more rapidly, provided that technological solutions are integrated with organizational, social, and legal measures and implemented with respect for individual rights.

Keywords: terrorism, security management, cybersecurity, critical infrastructure, crisis management, new technologies, interinstitutional cooperation

Wprowadzenie i podstawa analizy

Współczesny terroryzm rozwija się równolegle z cyfryzacją życia społecznego, globalizacją przepływów finansowych oraz upowszechnieniem technologii komunikacyjnych. Organizacje i pojedynczy sprawcy mogą dzięki nim docierać do odbiorców ponad granicami państw, prowadzić propagandę, rekrutować sympatyków, pozyskiwać informacje, organizować finansowanie i przygotowywać działania bez konieczności tworzenia rozbudowanych struktur hierarchicznych. Państwo nie może zatem opierać systemu bezpieczeństwa wyłącznie na tradycyjnych działaniach policyjnych, wywiadowczych lub wojskowych. Konieczne staje się łączenie rozpoznania zagrożeń, analizy informacji,

cyberbezpieczeństwa, ochrony infrastruktury krytycznej, zarządzania kryzysowego i współpracy wielu podmiotów (Benjamin, 2008: 5).

Innowacyjne zarządzanie bezpieczeństwem oznacza w tym ujęciu nie tylko zakup nowoczesnego sprzętu. Obejmuje również zmiany organizacyjne, rozwój zdolności analitycznych, usprawnienie obiegu informacji, wykorzystywanie symulacji i ćwiczeń, tworzenie partnerstw publiczno-prywatnych oraz zdolność instytucji do uczenia się na podstawie wcześniejszych zdarzeń. Jest to szczególnie ważne wobec zagrożeń asymetrycznych, których sprawcy wybierają słabo chronione elementy systemu i dostosowują metody działania szybciej niż rozbudowane struktury administracyjne (Żebrowski, 2012: 24).

Celem artykułu jest określenie, jakie elementy innowacyjnego zarządzania zwiększają zdolność państwa do przeciwdziałania terroryzmowi oraz jakie ograniczenia towarzyszą stosowaniu nowych technologii. Opracowanie ma charakter przeglądowo-analityczny. Zastosowano jakościową analizę treści literatury naukowej, raportów i dokumentów instytucjonalnych dotyczących terroryzmu, wykorzystania internetu, cyberbezpieczeństwa, ochrony infrastruktury krytycznej oraz zarządzania kryzysowego. Analiza nie stanowi badania empirycznego ani studium konkretnego zamachu. Jej przedmiotem są rozwiązania organizacyjne i technologiczne, które mogą wspierać prewencję, przygotowanie, reagowanie i odbudowę.

Punktem wyjścia jest założenie, że współczesne organizacje terrorystyczne często funkcjonują jako sieci luźno powiązanych komórek i sympatyków. Taki model utrudnia identyfikację ośrodka decyzyjnego, a jednocześnie pozwala sprawcom szybko zmieniać kanały komunikacji i metody działania. Tradycyjne, silnie hierarchiczne systemy bezpieczeństwa mogą reagować z opóźnieniem, jeżeli informacje są rozproszone pomiędzy instytucjami albo przekazywane wyłącznie drogą wielostopniowej procedury. Dlatego przewaga państwa zależy w coraz większym stopniu od zdolności łączenia danych, współdziałania służb i szybkiego podejmowania decyzji (Newman, Clarke, 2008: 12).

Technologie, analiza informacji i przeciwdziałanie finansowaniu terroryzmu

Jednym z podstawowych obszarów innowacji jest rozwój systemów analizy informacji. Służby bezpieczeństwa i organy ścigania korzystają z danych wywiadowczych, informacji finansowych, rejestrów podróży, materiałów z monitoringu oraz danych pochodzących z otwartych źródeł. Połączenie rozproszonych informacji może ujawnić relacje, które pozostają niewidoczne przy analizie pojedynczego zbioru. Umożliwia to tworzenie profili ryzyka, identyfikowanie sieci kontaktów oraz kierowanie zasobów do obszarów wymagających pogłębionej weryfikacji (Santamato, Beumler, 2013: 36).

Znaczenie zyskują algorytmy uczenia maszynowego i narzędzia służące do analizy dużych zbiorów danych. Mogą one wspierać wykrywanie anomalii, porządkowanie materiału i wybór informacji wymagających oceny analityka. Nie powinny jednak być przedstawiane jako systemy samodzielnie „przewidujące" terroryzm. Ich wyniki zależą od jakości danych, przyjętych kryteriów oraz sposobu interpretacji. Błędy, niepełne dane

lub uprzedzenia zapisane w modelu mogą prowadzić do fałszywych wskazań, dlatego niezbędne są kontrola człowieka, możliwość weryfikacji wyniku i jasno określona odpowiedzialność za decyzję.

Podobne korzyści i ryzyka wiążą się z monitoringiem miejskim, analizą metadanych oraz technologiami rozpoznawania twarzy. Rozwiązania te mogą przyspieszać identyfikację osób poszukiwanych, odtwarzanie przebiegu zdarzeń i ochronę obiektów szczególnie zagrożonych. Jednocześnie zwiększają zakres gromadzenia informacji o osobach, które nie są podejrzane o popełnienie przestępstwa. Skuteczne zarządzanie bezpieczeństwem wymaga więc zachowania proporcjonalności, ograniczenia dostępu do danych, określenia czasu ich przechowywania oraz kontroli legalności wykorzystywania narzędzi nadzorczych (Schneier, 2015: 31–34).

Nowoczesne technologie są wykorzystywane także w szkoleniu służb. Symulacje komputerowe i środowiska wirtualne pozwalają ćwiczyć reakcję na atak w obiekcie transportowym, na imprezie masowej lub w budynku użyteczności publicznej bez narażania uczestników i zakłócania działania rzeczywistej infrastruktury. Wartość takich szkoleń polega przede wszystkim na sprawdzaniu komunikacji, podziału zadań i procesu decyzyjnego. Technologia jest narzędziem, natomiast rzeczywistym celem ćwiczenia pozostaje wykrycie luk organizacyjnych oraz przygotowanie służb do współpracy pod presją czasu (Bielecka, Nowacki, 2017: 33–38).

Odrębny obszar stanowi przeciwdziałanie finansowaniu terroryzmu. Organizacje terrorystyczne korzystają zarówno z tradycyjnych transferów, gotówki i działalności gospodarczej, jak i z nowych usług płatniczych oraz narzędzi utrudniających ustalenie beneficjenta. Analiza transakcji może pomóc w identyfikowaniu nietypowych przepływów, powiązań między podmiotami oraz źródeł finansowania. Nie polega ona jednak wyłącznie na wykrywaniu wysokich kwot. Działalność terrorystyczna bywa finansowana licznymi, pozornie zwyczajnymi operacjami o niewielkiej wartości, co wymaga łączenia informacji finansowych z wiedzą operacyjną i kontekstem zachowania (*FATF Report. Terrorist Financing Risk Assessment Guidance*, 2019: 14).

Skuteczność tego obszaru zależy od współpracy organów państwa z bankami, operatorami płatności i innymi instytucjami obowiązanymi. Podmioty prywatne dysponują danymi transakcyjnymi, natomiast służby posiadają informacje o osobach, miejscach i zdarzeniach istotnych z punktu widzenia bezpieczeństwa. Dopiero odpowiednio uregulowana wymiana informacji pozwala połączyć oba rodzaje wiedzy. Ustalenie to potwierdza szerszą prawidłowość: innowacja technologiczna przynosi efekt wtedy, gdy jest osadzona w sprawnym modelu współpracy i jasnych procedurach postępowania.

Cyberterroryzm, wykorzystanie internetu i ochrona infrastruktury krytycznej

Internet jest wykorzystywany przez podmioty terrorystyczne do propagandy, radykalizacji, rekrutacji, finansowania, szkolenia, planowania i komunikacji. Nie każde takie działanie powinno być jednak automatycznie określane mianem cyberterroryzmu. Publikowanie

treści propagandowych lub kontaktowanie się z sympatykami stanowi wykorzystanie internetu do celów terrorystycznych, natomiast pojęcie cyberterroryzmu powinno być odnoszone przede wszystkim do ataków na systemy informatyczne, których motywacja i skutki odpowiadają istocie terroryzmu. Rozróżnienie to ogranicza pojęciowy chaos i pozwala właściwie dobierać środki reakcji (*The Use of the Internet for Terrorist Purposes*, 2012: 3–12).

Media społecznościowe i komunikatory umożliwiają szybkie rozpowszechnianie przekazów ideologicznych, instrukcji i materiałów gloryfikujących przemoc. Ich zasięg ułatwia kontakt z odbiorcami, którzy wcześniej pozostawaliby poza bezpośrednim wpływem organizacji. Działania przeciwdziałające nie mogą ograniczać się do usuwania treści, ponieważ materiały są łatwo kopiowane i przenoszone między platformami. Potrzebne są równocześnie działania operacyjne, analiza sieci rozpowszechniania, edukacja medialna, przeciwdziałanie radykalizacji i tworzenie wiarygodnych komunikatów alternatywnych. Reakcja wyłącznie techniczna usuwa pojedynczy materiał, lecz nie likwiduje mechanizmu jego oddziaływania (Ferrag, Kantzavelou, Maglaras, 2024: 28).

Cyfryzacja zwiększa również podatność infrastruktury krytycznej. Systemy energetyczne, transportowe, telekomunikacyjne, finansowe, wodociągowe i medyczne są ze sobą powiązane, a zakłócenie jednego sektora może wywołać następstwa w kolejnych. Atak na system sterowania, sieć łączności albo usługi dostawcy zewnętrznego nie musi powodować fizycznego zniszczenia, aby poważnie utrudnić funkcjonowanie państwa. Skutkiem może być brak dostępu do usług, paraliż transportu, przerwanie komunikacji, utrata zaufania lub chaos informacyjny (Bąk, 2010: 77–78).

Ochrona infrastruktury nie może ograniczać się do zabezpieczania pojedynczych urządzeń. Wymaga identyfikacji zależności pomiędzy sektorami, oceny podatności dostawców, tworzenia kopii zapasowych, segmentacji sieci, planów ciągłości działania i regularnego testowania procedur. Istotną rolę odgrywają zespoły reagowania na incydenty, które monitorują zagrożenia, wspierają wymianę informacji i koordynują działania naprawcze. W praktyce odporność systemu zależy nie tylko od możliwości powstrzymania ataku, lecz także od zdolności utrzymania podstawowych usług oraz ich szybkiego odtworzenia (Żebrowski, 2012: 364–367, 404–411).

Współczesne cyberzagrożenia mają często charakter hybrydowy. Atak techniczny może być połączony z dezinformacją, presją polityczną, sabotażem lub działaniami prowadzonymi przez podmioty trudne do jednoznacznego przypisania. Z punktu widzenia zarządzania oznacza to konieczność wspólnej analizy incydentów przez specjalistów technicznych, służby bezpieczeństwa, administrację i operatorów infrastruktury. Rozdzielenie tych środowisk może prowadzić do błędnej oceny zdarzenia jako wyłącznie awarii technicznej albo przeciwnie, do nadmiernego przypisywania zwykłemu cyberprzestępstwu charakteru terrorystycznego (Skomra, Wojtasik, 2025: 13–18).

Znaczna część infrastruktury teleinformatycznej należy do przedsiębiorstw prywatnych. Państwo nie posiada więc pełnej kontroli nad zasobami, od których zależy ciągłość podstawowych usług. Partnerstwa publiczno-prywatne powinny obejmować wymianę informacji o zagrożeniach, wspólne standardy, ćwiczenia, procedury zgłaszania incydentów i określenie odpowiedzialności za odtworzenie usług. Sama deklaracja współpracy

jest niewystarczająca. W sytuacji kryzysowej liczą się wcześniej przetestowane kanały komunikacji, osoby uprawnione do podejmowania decyzji oraz zgodność procedur poszczególnych podmiotów (Newman, Clarke, 2008: 56–57).

Zarządzanie kryzysowe i współdziałanie instytucji

Innowacyjne podejście do bezpieczeństwa wymaga odejścia od modelu wyłącznie reaktywnego. Państwo powinno ograniczać prawdopodobieństwo zamachu, przygotowywać zasoby, reagować na zdarzenie i odtwarzać funkcjonowanie instytucji po kryzysie. Zarządzanie kryzysowe obejmuje zatem cztery powiązane fazy: zapobieganie, przygotowanie, reagowanie oraz odbudowę (Bąk, 2010: 83; Wilińska, 2015: 131–132). Pominięcie którejkolwiek z nich osłabia cały system. Skuteczna reakcja nie zrekompensuje braku zabezpieczeń, a rozbudowana prewencja nie zastąpi planów pomocy poszkodowanym i przywracania usług.

Zapobieganie obejmuje analizę ryzyka, rozpoznanie zagrożeń, ochronę obiektów i przeciwdziałanie finansowaniu, rekrutacji oraz radykalizacji. Przygotowanie polega na opracowaniu planów, zapewnieniu zasobów, szkoleniu personelu i prowadzeniu ćwiczeń. Reagowanie wymaga szybkiego dowodzenia, ratowania życia, neutralizacji zagrożenia, zabezpieczenia miejsca zdarzenia i rzetelnej komunikacji. Odbudowa obejmuje naprawę infrastruktury, pomoc społeczną, odtworzenie zdolności instytucji, ocenę strat oraz analizę wniosków. Właśnie ostatni element decyduje o tym, czy system potrafi się uczyć i zmniejszać podatność na kolejne zdarzenia (Makowska, 2016: 112–113).

Zagrożenie terrorystyczne angażuje jednocześnie policję, służby specjalne, administrację rządową i samorządową, straż pożarną, ratownictwo medyczne, wojsko oraz operatorów infrastruktury. Każda instytucja ma inne kompetencje, procedury i systemy łączności. Brak wspólnego obrazu sytuacji może prowadzić do dublowania działań, opóźnień albo pominięcia istotnej informacji. Dlatego jednym z głównych kryteriów nowoczesności systemu jest interoperacyjność, rozumiana jako zdolność różnych podmiotów do współpracy mimo odmienności organizacyjnych.

Interoperacyjność wymaga jasnego podziału odpowiedzialności. Przed wystąpieniem kryzysu należy ustalić, kto prowadzi analizę zagrożenia, kto podejmuje decyzje strategiczne, kto dowodzi na miejscu zdarzenia, kto odpowiada za komunikację publiczną, a kto utrzymuje ciągłość kluczowych usług. W wielopoziomowym systemie administracji ważne jest również połączenie decyzji centralnych z działaniami wojewódzkimi, powiatowymi i gminnymi. Nawet prawidłowo opracowana strategia pozostanie dokumentem bez znaczenia, jeżeli nie zostanie przełożona na wykonalne zadania i znane wcześniej procedury (Żebrowski, 2012: 203, 210–212).

Szczególne znaczenie mają regularne ćwiczenia międzyinstytucjonalne. Pozwalają one zweryfikować realny czas przekazywania informacji, działanie systemów łączności, dostępność zasobów i zgodność procedur. Ćwiczenie powinno kończyć się analizą błędów, przypisaniem działań naprawczych oraz kontrolą ich wykonania. Bez takiego mechanizmu szkolenie może stać się wydarzeniem formalnym, które nie zwiększa odporności państwa.

Innowacyjność organizacyjna polega zatem na tworzeniu pętli uczenia się: planowaniu, testowaniu, ocenie i aktualizacji rozwiązań.

Współpraca międzynarodowa jest konieczna ze względu na transgraniczny charakter komunikacji, finansowania i przemieszczania się sprawców. Obejmuje wymianę informacji wywiadowczych, pomoc prawną, wspólne szkolenia, ochronę granic i koordynację działań operacyjnych. W podejściu NATO wskazuje się na wzajemne powiązanie świadomości zagrożeń, zdolności do działania oraz zaangażowania partnerów. Model ten podkreśla, że posiadanie sprzętu i wyspecjalizowanych jednostek nie wystarcza bez aktualnej wiedzy o zagrożeniu i zdolności współpracy (Santamato, Beumler, 2013: 18–20).

W systemie krajowym równie istotna jest współpraca ze strukturami lokalnymi. Samorządy, lokalna policja, zarządcy transportu, szkoły, placówki medyczne i organizacje społeczne znają specyfikę przestrzeni oraz grup narażonych na radykalizację. Mogą wcześniej dostrzegać zmiany zachowania, konflikty i podatności konkretnych miejsc. Nie oznacza to przenoszenia zadań służb specjalnych na społeczność, lecz budowanie kanałów zgłaszania zagrożeń i wzajemnego zaufania. Państwo działające wyłącznie na poziomie centralnym może dysponować zaawansowanymi narzędziami, a jednocześnie nie posiadać wiedzy o lokalnym kontekście (Newman, Clarke, 2008: 5–6).

Wymiar społeczny, komunikacja i skutki terroryzmu

Terroryzm jest nakierowany nie tylko na bezpośrednie ofiary. Jego celem jest wywołanie lęku, presji politycznej i poczucia, że państwo nie potrafi zapewnić bezpieczeństwa. Dlatego zarządzanie zagrożeniem musi obejmować komunikację społeczną. Po zdarzeniu obywatele potrzebują szybkich, jasnych i wiarygodnych informacji o skali zagrożenia, zalecanym zachowaniu i dostępnej pomocy. Brak komunikatu albo sprzeczne wypowiedzi instytucji tworzą przestrzeń dla plotek, dezinformacji i paniki.

Komunikacja kryzysowa powinna być przygotowywana przed zdarzeniem. Należy ustalić podmiot odpowiedzialny za przekaz, kanały publikacji, procedurę potwierdzania informacji oraz sposób prostowania fałszywych wiadomości. Szczególne znaczenie mają media społecznościowe, ponieważ umożliwiają szybkie dotarcie do obywateli, ale jednocześnie przyspieszają rozpowszechnianie niesprawdzonych treści. Wiarygodność komunikacji zależy od jej regularności, spójności i zgodności z rzeczywistymi działaniami służb.

Do społecznych skutków terroryzmu należą długotrwały lęk, trauma, spadek zaufania do instytucji oraz wzrost uprzedzeń wobec grup utożsamianych ze sprawcami. Reakcja państwa skoncentrowana wyłącznie na represji może pogłębiać podziały i wzmacniać narrację organizacji ekstremistycznych. Programy przeciwdziałania radykalizacji powinny zatem łączyć działania służb z edukacją, pomocą psychologiczną, pracą lokalną i wzmacnianiem odporności społecznej. Ich celem nie jest zastępowanie odpowiedzialności karnej, lecz ograniczanie warunków sprzyjających rekrutacji.

Terroryzm wywołuje również skutki gospodarcze. Państwo ponosi koszty ochrony obiektów, zabezpieczenia wydarzeń, rozwoju monitoringu, szkolenia służb i odbudowy infrastruktury. Przedsiębiorstwa mogą doświadczać przestojów, spadku ruchu klientów,

utraty danych lub wzrostu kosztów ubezpieczenia. Największe straty nie zawsze wynikają z samego zamachu, lecz z długotrwałego zakłócenia transportu, usług publicznych i zaufania do bezpieczeństwa danego miejsca. Z tego względu analiza kosztów powinna obejmować zarówno bezpośrednie szkody, jak i następstwa organizacyjne oraz społeczne.

Ograniczanie skutków wymaga budowania odporności społecznej. Oznacza ona zdolność obywateli i instytucji do zachowania podstawowych funkcji, korzystania z wiarygodnych źródeł informacji i powrotu do normalnego działania. Nie polega na bagatelizowaniu zagrożenia, lecz na przygotowaniu procedur i zasobów, które zmniejszają podatność na wywoływanie paniki. W tym sensie edukacja, komunikacja i pomoc poszkodowanym są równie ważnymi elementami zarządzania bezpieczeństwem, jak technologie wykrywania zagrożeń.

Wnioski końcowe

Przeprowadzona analiza wskazuje, że innowacyjne zarządzanie bezpieczeństwem państwa ma charakter systemowy. Jego skuteczność nie wynika z zastosowania pojedynczej technologii, lecz z połączenia zdolności analitycznych, ochrony infrastruktury krytycznej, zarządzania kryzysowego, współpracy międzynarodowej, partnerstw publiczno-prywatnych oraz działań społecznych. Nowoczesne narzędzia zwiększają szybkość przetwarzania informacji i umożliwiają dostrzeganie relacji w rozproszonych danych, ale nie zastępują oceny człowieka, prawidłowego dowodzenia ani odpowiedzialności instytucjonalnej.

Najważniejszym ustaleniem jest to, że główne bariery skuteczności mają często charakter organizacyjny, a nie techniczny. Należą do nich niepełny przepływ informacji, niejasny podział kompetencji, brak interoperacyjności, niesprawdzone procedury oraz niewystarczająca współpraca z operatorami prywatnymi. Zakup kolejnych systemów bez usunięcia tych ograniczeń może zwiększać ilość danych i złożoność systemu, nie poprawiając realnie bezpieczeństwa.

Drugie ustalenie dotyczy konieczności objęcia działaniami całego cyklu zarządzania kryzysowego. Państwo powinno równocześnie zapobiegać, przygotowywać się, reagować i odbudowywać zdolności po zdarzeniu. Ochrona przed terroryzmem nie kończy się wraz z neutralizacją sprawców. Obejmuje odtworzenie usług, pomoc poszkodowanym, komunikację społeczną i analizę doświadczeń, które powinny prowadzić do aktualizacji procedur.

Trzecim ustaleniem jest potrzeba zachowania równowagi między bezpieczeństwem a prawami jednostki. Rozbudowane systemy monitoringu i analizy danych mogą wspierać działania antyterrorystyczne, ale wymagają proporcjonalności, kontroli legalności, zabezpieczenia danych i możliwości weryfikacji decyzji. Brak tych mechanizmów może osłabić zaufanie społeczne, które stanowi ważne źródło informacji i warunek współpracy obywateli z instytucjami.

Innowacyjne zarządzanie bezpieczeństwem zwiększa zdolność państwa do wcześniejszego rozpoznawania zagrożeń, szybszego reagowania i ograniczania skutków terroryzmu. Warunkiem jest jednak traktowanie technologii jako elementu spójnego systemu, a nie jako celu samego w sobie. Najbardziej odporny model łączy nowoczesne narzędzia

z kompetentnym personelem, jasnymi procedurami, współpracą wielu sektorów i regularnym uczeniem się na podstawie ćwiczeń oraz rzeczywistych zdarzeń.

Bibliografia

Bąk T. (2010), *Zarządzanie kryzysowe w przypadku zamachu terrorystycznego*, „Zeszyty Naukowe Wyższej Szkoły Oficerskich Wojsk Lądowych", nr 3(157), s. 76–96.

Benjamin D. (2008), *Strategic Counterterrorism*, Washington: The Brookings Institution.

Bielecka J., Nowacki G. (2017), *Służby specjalne w zwalczaniu zagrożeń terrorystycznych w Polsce i na świecie*, „Autobusy. Technika, Eksploatacja, Systemy Transportowe", nr 9, s. 33–38.

FATF Report. Terrorist Financing Risk Assessment Guidance (2019), Paris: FATF.

Ferrag M.A., Kantzavelou I., Maglaras L. (2024), *Hybrid Threats, Cyberterrorism and Cyberwarfare*, Boca Raton: CRC Press.

Makowska J. (2016), *Rola zarządzania kryzysowego w systemie zarządzania bezpieczeństwem narodowym*, „De Securitate", nr 1(2), s. 111–113.

Newman G.R., Clarke R.V. (2008), *Policing Terrorism: An Executive's Guide*, Washington: Office of Community Oriented Policing Services.

Santamato S., Beumler M.-T. (2013), *The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessments, and Actions*, Washington: National Defense University Press.

Schneier B. (2015), *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York: W.W. Norton & Company.

Skomra W., Wojtasik K. (2025), *Infrastruktura krytyczna jako cel działań hybrydowych. Studia przypadków ataków na obiekty i systemy IK*, „Terroryzm! Studia, Analizy, Prewencja", wydanie specjalne, s. 13–34, https://doi.org/10.4467/27204383TER.25.001.21504

The Use of the Internet for Terrorist Purposes (2012), New York: United Nations.

Wilińska M. (2015), *Zarządzanie kryzysowe w systemie bezpieczeństwa państwa*, „Obronność. Zeszyty Naukowe", nr 3(15), s. 127–136.

Żebrowski A. (2012), *Zarządzanie kryzysowe elementem bezpieczeństwa Rzeczypospolitej Polskiej*, Kraków: Wydawnictwo Naukowe Uniwersytetu Pedagogicznego.

O autorach

Kacper Minda – student pierwszego roku studiów magisterskich na kierunku kryminologia, wiążący swoją przyszłość zawodową ze służbą w Policji; obecnie funkcjonariusz Policji oraz członek Koła Naukowego „Jurysta".

Sebastian Seliga – student pierwszego roku studiów magisterskich na kierunku kryminologia, zainteresowany procesem karnym oraz nowymi formami przestępczości; członek Koła Naukowego „Jurysta".

About the Authors

Kacper Minda – a first-year master's student in criminology who plans to pursue a career in the police. He currently works as a junior debt collection advisor and is a member of the Research Club "Jurysta".

Sebastian Seliga – a first-year master's student in criminology interested in criminal procedure and emerging forms of crime. He is a member of the Research Club "Jurysta".

Ten utwór jest dostępny na licencji Creative Commons Uznanie autorstwa-Na tych samych warunkach 4.0 Międzynarodowe.

Open Access