Redakcja naukowa:

Zofia Wilk-Woś
Monika Ostrowska

Bezpieczeństwo i zarządzanie kryzysowe

Zarządzanie bezpieczeństwem lokalnym

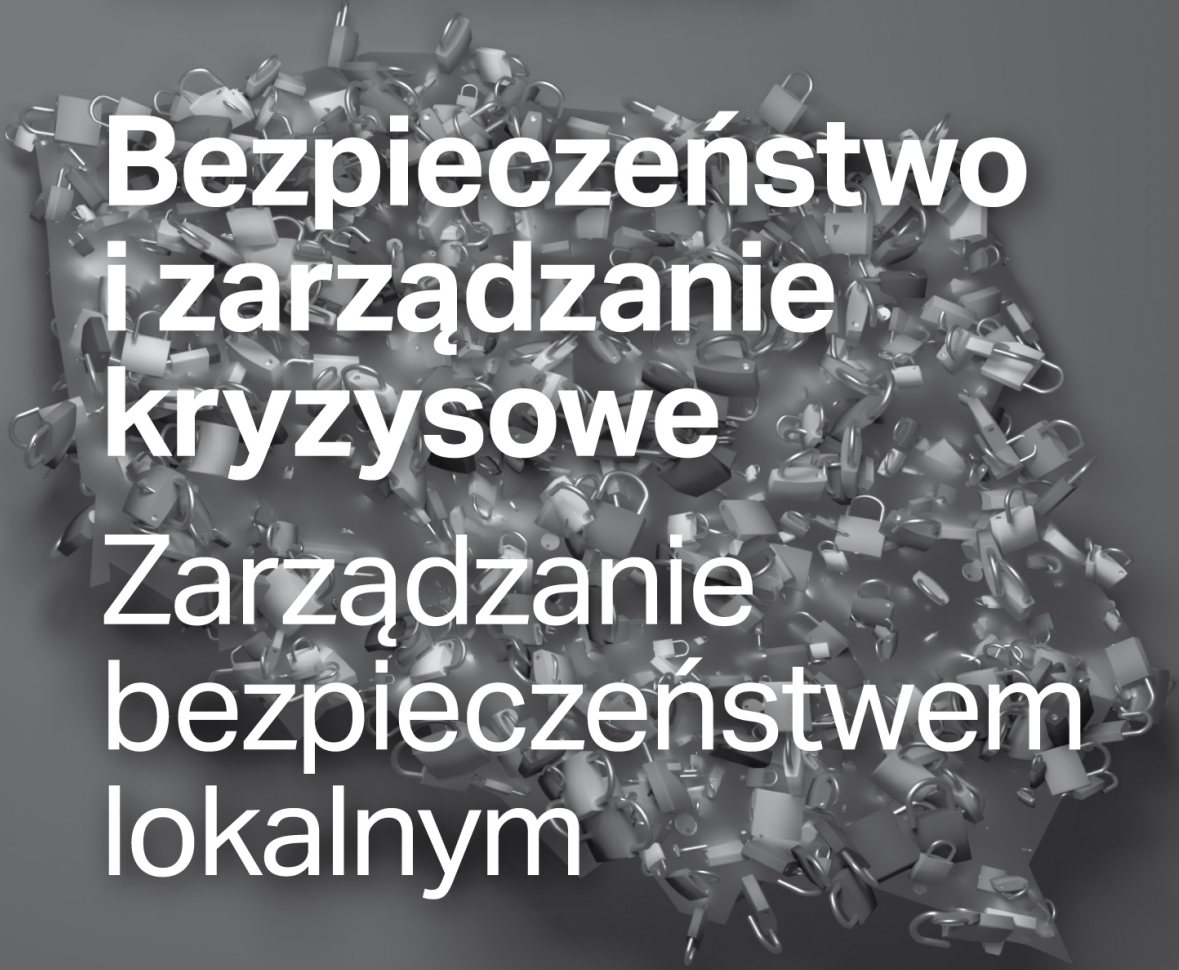
Nr 104 Studia i Monografie
Łódź-Warszawa 2019

Społeczna Akademia Nauk
Łódź

Redakcja naukowa:
Zofia Wilk-Woś
Monika Ostrowska

Bezpieczeństwo i zarządzanie kryzysowe

Zarządzanie bezpieczeństwem lokalnym



Nr 104 Studia i Monografie
Łódź-Warszawa 2019

Społeczna Akademia Nauk
Łódź

Monografia recenzowana
Korekta językowa: Dominika Więzik, Małgorzata Pająk
Skład i łamanie: Małgorzata Pająk
Projekt okładki: Marcin Szadkowski

Studia i Monografie nr 104
2019

ISBN: 978-83-64971-79-2

Wydawnictwo Społecznej Akademii Nauk
Kilińskiego 109
90-011 Łódź
tel. (42) 664 22 39
(42) 676 25 29 w. 339

Spis treści

Zofia Wilk-Woś

Wstęp

Ostatnie wydarzenia w Chinach – wybuch epidemii wirusa COVID-19 – uwidoczniły, że XXI wiek jest i będzie okresem nowych zagrożeń dla ludzkości. Zmiany cywilizacyjne, rozwój techniki i technologii powodują, że ludzie w kilka godzin mogą przemieścić się z jednego końca świata na drugi, a dzięki Internetowi wiadomość potrzebuje kilka sekund, aby dotrzeć do adresata – tego przy sąsiednim biurku i tego za oceanem. Tak jak rozwój dał człowiekowi łatwość podróżowania i komunikowania się, tak samo postawił przed nim szereg wyzwań i niebezpieczeństw. Cyberprzestrzeń stała się pełna zagrożeń, a cyberprzestępstwa dotykają użytkowników Internetu każdego dnia. Jednocześnie społeczeństwa nadal muszą się zmagać ze „starymi" zagrożeniami, jak wyzwania w sferze społecznej czy chociażby niewypały z okresu II wojny światowej. Wyzwania współczesnego świata ujawniają i zmuszają nas do analizy szeregu zjawisk, których poprawne opisanie i zrozumienie pozwoli nam na wypracowanie odpowiednich narzędzi i metod podnoszących poziom bezpieczeństwa. Ta szeroka gama problemów znalazła odzwierciedlenie w prezentowanym Czytelnikowi opracowaniu.

Z prac teoretycznych szczególnie wart uwagi jest rozdział Janusza Ziarko, który zaproponował interesujące podejście metodyczne do sposobu budowania modelu zagrożenia. Autor podkreśla, że dobrze opracowane modele mogą stać się doskonałym narzędziem wspomagającym procesy opisu, wyjaśniania i rozumienia sytuacji zagrażających, a w konsekwencji trafności decyzji operacyjnych, także narzędziem dla działań zapewniających pożądany poziom bezpieczeństwa i porządku publicznego.

Niezwykle istotna jest analiza Bogdana Panka i Mirosława Banasika, w tym sformułowanie wniosków końcowych dla polskiej polityki bezpieczeństwa i obrony. Podkreślili oni między innymi potrzebę dostosowania obecnych dokumentów strategicznych do zmienionej sytuacji w środowisku bezpieczeństwa międzynarodowego i narodowego, zwłaszcza do konfliktu hybrydowego, bo

zdaniem Autorów Polska jest objęta ryzykiem zagrożeń hybrydowych i dlatego nie jest już tak bezpieczna, jak miało to miejsce w ostatnich dziesięcioleciach. Prezentowana w niniejszym tomie diagnoza podkreśla również konieczność odnowy intelektualnej obrony kraju – „najpierw edukować i komunikować ryzyko w wiarygodny sposób".

Odmienną problematykę obszaru bezpieczeństwa zaprezentował Janusz Liber. Autor omówił funkcjonowanie i rolę kontrwywiadu biznesowego w ramach bezpieczeństwa korporacyjnego w organizacjach międzynarodowych, wskazując, że głównym zadaniem służb kontrwywiadu jest identyfikowanie informacji o istotnych zagrożeniach dla firmy, jak również ich dystrybucja do odpowiednich komórek organizacyjnych/ osób, celem wsparcia procesu decyzyjnego w korporacji. Podkreślił, że organizując osłonę kontrwywiadowczą przedsiębiorstwa, należy mieć na uwadze nie tylko relacje wewnątrz organizacji, lecz także współdziałanie z organizacjami zewnętrznymi, takimi jak dostawcy i odbiorcy oraz instytucje rządowe.

Dla kreowania bezpieczeństwa społecznego znaczący może być rozdział opracowany przez Jadwigę Mazur. Autorka przedstawiła ogólne wyniki procesu ewaluacji programów profilaktycznych w zakresie przeciwdziałania alkoholizmowi i narkomanii na terenie miasta Łódź, wskazując na pozytywne i negatywne strony tych programów, których głównym celem jest niedopuszczenie do marginalizacji mieszkańców miasta i ich rodzin, dotkniętych problemem wspomnianych uzależnień.

W tomie znalazły się również rozważania Jana Zycha nad rozumieniem procesu zarządzania bezpieczeństwem w środowisku sieciowym. Kwestii cyberbezpieczeństwa dotykają prace Agnieszki Białek i Kamila Martyniaka. Monika Ostrowska i Cezary Podlasiński unaoczniają Czytelnikom, że, w erze zwiększonych inwestycji infrastrukturalnych, problem niewybuchów nadal stanowi niemałe zagrożenie dla bezpieczeństwa ludności. Rozdział Jerzego Guta, Sławomira Mazura i Bogdana Tworowskiego zbiera i porządkuje kwestie związane z rolą Sił Zbrojnych RP w zarządzaniu kryzysowym, natomiast Barbara Standarska próbuje wskazać możliwości zastosowania bezzałogowych statków powietrznych w zadaniach militarnych. W opracowaniu znalazły się jeszcze dwie prace z obszaru bezpieczeństwa transportu – Piotra Niedzielskiego, Michała Antolaka i Magdaleny Zioło, dotycząca Systemu Zarządzania Bezpieczeństwem w transporcie kolejowym oraz Marka Krzywonosa, poświęcona działaniom interesariuszy wewnętrznych i zewnętrznych w poprawie bezpieczeństwa drogowego transportu towarów na terenie UE.

Kończąc, warto dodać, że kolejny tom monografii został przygotowany przez Instytut Bezpieczeństwa Narodowego Społecznej Akademii Nauk przy współpracy z Krakowską Akademią im. Andrzeja Frycza Modrzewskiego oraz Fundacją Instytutu Wywiadu Gospodarczego w Krakowie – i ponownie pokazał, jak istotne dla obszaru bezpieczeństwa i zarządzania kryzysowego są zarówno prace badawcze, jak i praktyka.

Janusz Ziarko
januszziarko@interia.pl
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego,
Wydział Nauk o Bezpieczeństwie

Modelowanie zagrożeń bezpieczeństwa i porządku publicznego – propozycja metodyczna

Wstęp

Nauka coraz częściej i w coraz większym stopniu korzysta z terminów właściwych dla teorii systemów, takich jak złożoność, nieliniowość, chaos, gdyż zdaniem wielu badaczy teoria ta umożliwia dokładniejszy opis poznawanej rzeczywistości, uwzględniający naturę, funkcjonowanie i wzajemne powiązania występujące pomiędzy elementami tej rzeczywistości. Zasadne jest więc pytanie: czy i dlaczego teoria systemów pozwala na dokładniejsze poznanie badanej rzeczywistości (oraz jak w praktyce ją stosować) aniżeli badania prowadzone w paradygmacie analityczno-redukcjonistycznym czy holistycznym. Odpowiedź na nie związana jest z podstawowym dylematem ludzkiego poznania, czyli relacją pomiędzy całością i jej częściami. Uwikłana jest więc w spór między holizmem, optującym za supremacją „całości" nad „częściami", a kartezjańskim redukcjonizmem, według którego „części" dominują nad „całością". System i model, kluczowe pojęcia teorii systemów, łączą w sobie możliwości poznania i opisu zjawisk przynależnych do świata przyrody, jak i do społeczeństwa, umożliwiają odkrywanie funkcjonalnych i strukturalnych zasad charakteryzujących te zjawiska, określanie czynników je warunkujących i ich opisywanie. Podejście systemowe, wykorzystywane w obszarze bezpieczeństwa i porządku publicznego (BiPP),

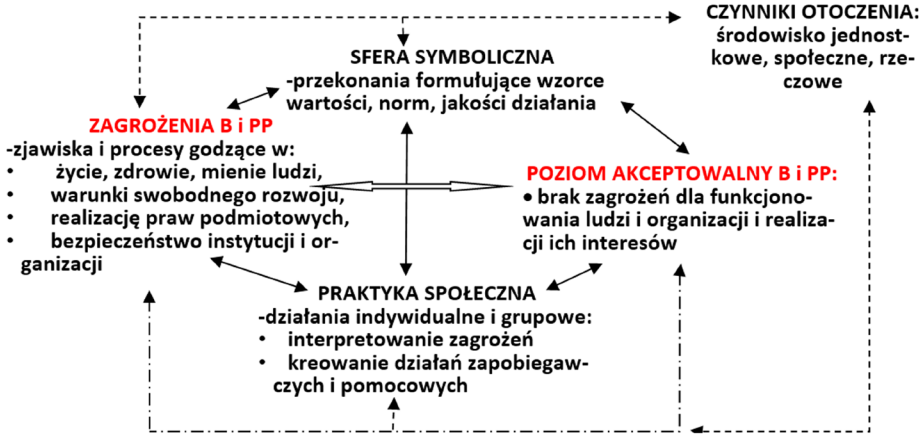
opiera się na założeniu, że BiPP nie powinno być izolowaną społeczną funkcją, ale postrzegane jako bezpośrednio związane ze społecznymi i jednostkowymi wartościami, które łączą wielorakie działania podejmowane dla zapewnienia bezpieczeństwa. Dlatego podejście to zakłada, że BiPP należy traktować z perspektywy złożoności, co wymaga stworzenia i praktycznego wykorzystywania narzędzia badawczego, jakim jest model takiego środowiska i występujących w nim zagrożeń, który uwzględnia kluczowe cechy tego środowiska, dobierane w kontekście badanego zagrożenia oraz umożliwia analizę wpływu różnych środowiskowych/ sytuacyjnych czynników oddziałujących na rozwój zagrożenia i jego skutki oraz chroniących przed nim. Celem prowadzonych tu rozważań jest identyfikacja możliwości implementacji założeń teorii systemów do badania zjawisk BiPP oraz przedstawienie metodycznych rozwiązań wykorzystania modelowania do analizy sytuacji BiPP w kontekście procesów rozwoju zagrożenia i procesów przeciwdziałania mu.

Ujęcie zjawiska BiPP

Podejście do prowadzonych tu rozważań związane jest w głównej mierze ze sposobem ujęcia BiPP. W klasycznym ujęciu BiPP jest definiowane jako ogół warunków i instytucji chroniących życie, zdrowie i mienie obywateli, czyli jest to stan w państwie tworzony przez normy prawne i społeczne, w którym człowiekowi i ogółowi społeczeństwa nie grozi żadne niebezpieczeństwo, niezależnie od źródeł, z którego miałoby pochodzić, stan umożliwiający normalne funkcjonowanie i rozwój państwa i społeczeństwa [Wiśniewski 2007, s. 14; Sprengel 2008; Misiuk 2008]. Z kolei definicja – odzwierciedlająca, w jaki sposób rozumienie BiPP ewoluowało, od prawie wyłącznego skupienia się na fizycznym środowisku życia ludzi do włączenia czynników psychospołecznych i osobistych praktyk na rzecz BiPP – ujmuje je jako ciągły proces społeczny, w ramach którego instytucje i ludzie współpracują, aby ciągle rozwijać i doskonalić różnorakie mechanizmy i procesy – wspólne i jednostkowe: 1) ukierunkowane na ochronę życia, zdrowia i mienia, 2) dopomagające rozwój jednostkowy i organizacyjny, 3) promujące bezpieczne a eliminujące wrogie zachowania, 4) zapewniające dobre samopoczucie lokalnej społeczności oraz 5) trwałość tych wartości. Ideą tego ujęcia jest włączanie różnych przedmiotów i podmiotów środowiska życia i pracy ludzi i wykorzystywania do promocji BiPP, prewencji i profilaktyki na jego rzecz, nie tylko po to, żeby zapobiegać zagrożeniom, ale także oceniać i poprawiać ogólny stan środowiska i poczucia bezpieczeństwa ludzi (rysunek 1). Działania

dla BiPP wymagają ukierunkowanych przedsięwzięć: 1) prewencyjnych, profilaktycznych i edukacyjnych, uwzględniających i kształtujących wartości i normy kultury BiPP, zarówno organizacyjne, jak i jednostkowe, 2) doskonalących funkcjonowanie instytucji i organizacji w obszarze BiPP, ich praktyki zarządzania i współdziałania, a co najważniejsze, 3) formujących postawy i przekonania ludzi/mieszkańców i pracowników instytucji bezpieczeństwa. Strategie i taktyki BiPP muszą być zaprojektowane tak, żeby pasowały do organizacji lokalnych instytucji, cech ludzi, kultury lokalnej i organizacyjnej, warunków życia i pracy mieszkańców.

Rysunek 1. Ogólny obraz systemu bezpieczeństwa i porządku publicznego



Źródło: opracowanie własne.

Aplikacja podejścia systemowego do badań BiPP

Teza: precyzyjne opisy wyników różnych obserwacji – zdarzeń, procesów, działań instytucji, zachowań i relacji ludzi w sytuacjach zagrażających BiPP – nie są metodą prowadzącą do określenia wymagań dotyczących sposobów działania eliminującego zagrożenie i poprawiającego stan BiPP. Zbieranie ogromu danych nie przybliża nas znacząco do zrozumienia tego, co i dlaczego dzieje się w tej sytuacji, a to znaczy, że nadal nie posiadamy wiedzy, jak działać, by eliminować zagrożenia i podnosić poziom BiPP.

W podejściu systemowym zakłada się, że rzeczywistość BiPP jest bytem niezwykle złożonym o słabo zaznaczonej strukturze, a to powoduje, że jego pełne

poznanie jest bardzo trudne i nie potrafimy go w pełni poznać, by opisać, wyjaśnić i zrozumieć wszystkie elementy i zależności zachodzące między elementami tej rzeczywistości. Ta złożoność rzeczywistości BiPP sprawia, że pozostaje nam jedynie stworzyć i poznać jej postać uproszczoną, zredukowaną, a więc zastąpić badany, złożony fragment rzeczywistości bezpieczeństwa – jego modelem. Czym więc jest podejście systemowe i jak możemy je zastosować w usprawnianiu działań dla BiPP? Podejście systemowe jest zbiorem metod, procedur i narzędzi wywodzących się z teorii systemów, wykorzystywanych w badaniach relacji pomiędzy wyróżnionymi i zdefiniowanymi obiektami sytuacji problemowej, badań prowadzących do opisania, wyjaśnienia oraz zrozumienia problemu i rozwiązania go. W podejściu systemowym postrzegamy system, tutaj wyróżniony element BiPP, jako pewien byt/ rzecz, który też jest systemem i współdziała z mozaiką innych bytów/ rzeczy w swoim węższym i szerszym otoczeniu, a jednocześnie sam składa się z części nawzajem na siebie oddziałujących. Każda część systemu może być samodzielnym systemem i sama może być postrzegana zarówno jako obiekt widziany z zewnątrz, jak i jako zestaw oddziałujących części, a badany system może być częścią wchodzącą w interakcje z jednym lub większą liczbą szerszych systemów. Takie podejście pozwala z jednej strony na całościowe/ systemowe spojrzenie na badaną organizację/ sytuację i występujący w niej problem, łącznie z jej powiązaniami z otoczeniem, z drugiej strony pozwala organizację/ sytuację tę traktować jak system z wejściami i wyjściami, w którym zachodzą określone procesy. Podejście to przejawia się w sposobie poznawczego patrzenia na naturę rzeczywistości, który to sposób silnie związany jest z myśleniem systemowym.

W odniesieniu do BiPP podejście systemowe optuje za traktowaniem wyróżnionego obiektu czy zjawiska BiPP jako jednolitego, celowego systemu, złożonego ze wzajemnie powiązanych części oraz relacji, które się tworzą między nimi, co pozwala spojrzeć na badany problem BiPP jako na całość, stanowiącą zarazem część szerszego otoczenia zewnętrznego. Podejście to zakłada, że wszystkie procesy i działania realizowane w danym społecznym środowisku, ukierunkowane na tworzenie wartości, jaką jest BiPP, powinny być traktowane jako całości – systemy, a nie jako indywidualne części. To wymaga myślenia całościowego/ systemowego, ze względu na konieczne wewnętrzne i zewnętrzne powiązania i zależności. Potrzebne tu są umiejętności: dostrzegania związków i zależności pomiędzy procesami, np.: procesem projektowania przez organy działające na rzecz BiPP działań prewencyjnych i profilaktycznych, ograniczających w danym środowisku występujące zagrożenia, tj. przygotowania planów i programów działania, a możliwościami ludzi i środków angażowanych w te działania, z jednej strony, a z drugiej,

czynnikami (normy i wartości subkultur chuligańskich, pochodzenie społeczne członków grup chuligańskich, ich zorganizowanie, sposoby działania i in.) potęgującymi oddziaływanie zagrożenia. Ważne są tu też umiejętności budowania więzi współpracy, wzajemnych relacji pomiędzy ludźmi, komórkami i jednostkami organizacyjnymi mającymi przygotować i realizować te procesy. Wyróżniony w takim podejściu system społeczny nie ma ostrych, jednoznacznych granic, ponieważ jego wytyczanie jest wynikiem obserwacji, intuicji, zaangażowania i doświadczenia badacza [Morawski 2002, s. 112]. Myślenie i podejście systemowe pozwala:

- zidentyfikować system – który jest tu traktowany jako jednorodny, celowy i otwarty, składający się z wzajemnie powiązanych części tworzących pewną całość wyróżniającą się w otoczeniu – czyli określić jego granice, wyodrębnić i scharakteryzować części/ elementy oraz relacje wiążące części systemu i sam system z otoczeniem, tworząc reprezentację postrzegania systemu, rozumienia swego i innych miejsca w tym systemie;
- zrozumieć funkcjonowanie systemu – którego ukierunkowanie na rozwiązywanie problemów BiPP wymaga wewnętrznej siły i zwartości oraz umiejętności wyszukiwania i wykorzystania zasobów niezbędnych do budowania integralności i rozwoju systemu, do ugruntowywania swojej pozycji w otoczeniu – czyli trafnie opisać i ocenić stan istniejącego systemu, jego części składowe i relacje między nimi i ich właściwościami, zakres i poziom realizowanych procesów i wykonywanych zadań oraz podmiotową rolę człowieka w ich wykonaniu;
- określić/ sformułować problem/y występujący/e w systemie – to skompletować wiedzę o systemie i jego otoczeniu, w różny sposób związaną z jego funkcjonowaniem i przetworzyć ją do postaci wskazującej na potrzebę rozwoju, doskonalenia systemu – co pozwoli zmienić stan początkowy/ istniejący, który jest niezadowalający, na stan zadowalający;
- wskazać rozwiązanie problemu – poprzez kreowanie wizerunku pożądanego stanu systemu i systemowe projektowanie, uwzględniające zarówno obecny stan systemu, ale także jego przyszłe cele, charakterystyczne cechy, wymagane funkcje, które system ma pełnić – czyli przedstawić projekt struktury i funkcjonowania nowego systemu, zmniejszający złożoność, redukujący niepotrzebne role, poprawiający właściwości, usprawniający działania.

Modele i modelowanie jako narzędzia analizy systemowej BiPP

Istota modelu

W naukach społecznych przez model rozumie się celowo wyidealizowaną, uproszczoną reprezentację wybranego fragmentu rzeczywistości. Budujemy model, wyodrębniając z tej rzeczywistości (jakiegoś obiektu, zjawiska lub procesu) kluczowe zmienne, czyli elementy, cechy czy zachowania, najistotniejsze regularności i zależności [Sadowski 1978, s. 149], pomijając inne, które mogą być kluczowe dla innego modelu. Zbudowany model wybranego obszaru rzeczywistości uznajemy za prawidłowy tylko wtedy, kiedy istnieje homeomorfizm pomiędzy elementami abstrakcyjnymi (wyidealizowanymi) a elementami rzeczywistymi, co pozwala na odpowiednią interpretację zachowania się elementów abstrakcyjnych w terminach zjawisk czy procesów rzeczywistych. W praktyce badany fragment rzeczywistości bezpieczeństwa charakteryzowany jest przez bardzo dużą liczbę zmiennych, z których tylko niewielka ich część jest kluczowa. Budując model, koncentrujemy się na znalezieniu tych kluczowych zmiennych. Ważne jest pytanie: które elementy/ zmienne są kluczowe, czyli które zmienne istotnie wpływają na zmienną zależną – BiPP. Właściwie dobrane elementy modelu sprawiają, że możliwe jest rozpoznanie oraz jasny i zrozumiały opis i wyjaśnienie problemów występujących w zagrażającej sytuacji. Umożliwia sformułowanie celów i zadań oraz przedstawienie przewidywanego zachowania podmiotów sytuacyjnych w kontekście zmian związanych z rozwiązywanym problemem. Wówczas model staje się dobrym narzędziem analizy, bo otwiera poznawcze perspektywy, a to pomaga w wieloperspektywicznym ujmowaniu BiPP i przedstawieniu tej rzeczywistości w wielu uproszczonych formach, a także pozwala na symulowanie zachowania określonych obiektów modelowanej zagrażającej BiPP sytuacji. Stanowi specyficzne repozytorium wiedzy o tej sytuacji, o jej strukturze, elementach i o procesach w niej zachodzących oraz o występujących w niej problemach.

Pojęcie modelowania

A.K. Koźmiński twierdzi [1979, s. 39], że podstawową „(…) metodą analizy systemowej jest modelowanie, czyli budowa abstrakcyjnych konstrukcji odzwierciedlających w uproszczony sposób rzeczywistość". Taka wyabstrahowana konstrukcja to model, będący uproszczonym odwzorowaniem systemu istniejącego w rzeczywistości, który jest zbyt złożony, żeby można go było badać bezpośrednio. Stąd modele „(…) nigdy nie dorównują stopniem złożoności systemom rzeczywistym, które mają odwzorowywać, odzwierciedlają, bowiem jedynie określone, interesujące ich twórców

i użytkowników aspekty funkcjonowania systemów istniejących" [Koźmiński 1979, s. 23]. Podstawowe cele, dla jakich buduje się modele, modeluje się poznawaną rzeczywistość, możemy podzielić na dwie zasadnicze grupy [Balcerak, Kwaśnicki 2019]:

- opisanie elementów i odkrycie ważnych zależności, prawidłowości i wzorców, prowadzące do zrozumienia i wyjaśnienia zaobserwowanego zjawiska czy procesu (zmienne wejściowe),
- przewidywanie wartości zmiennych wyjściowych, obrazujących rozwój badanego zjawiska czy procesu, co pozwala na zaprojektowanie systemu tak, by jego działanie spełniało oczekiwania użytkowników.

Proces modelowania, czyli „(…) upraszczania i redukcji towarzyszy każdej czynności wydzielania systemu z otoczenia. (…) w każdym przypadku powinien przebiegać ze świadomością dokonywanych uproszczeń. W badaniach systemów redukcja musi dotyczyć zarówno ilości rozważanych elementów jak i ich cech" [Gomółka 2000, s. 34]. W praktyce modelowania odwzorowuje się jedynie najważniejsze części i zależności badanego systemu, a proces redukcji złożoności, taki upraszczający zabieg, powinien być przeprowadzony w taki sposób, aby zachowanie modelu odpowiadało w przybliżeniu zachowaniu się upraszczanego systemu, co umożliwia rozpoznanie, zarówno stanu, jak i sposobu jego funkcjonowania. Takie uproszczenie umożliwia zastąpienie badania rzeczywistych systemów: przedmiotów, zdarzeń i procesów BiPP badaniem zachowania modelu i na tej podstawie formułowania wniosków, które zachowują swą ważność także w odniesieniu do badanego systemu – fragmentu rzeczywistości BiPP [Jankowski 1997, s. 8 i nast.]. Znaczącym więc pożytkiem z modelowania jest możliwość eksperymentowania z modelem, a nie z realną rzeczywistością. Eksperymenty prowadzone z użyciem modelu pozwalają na ocenę skutków decyzji i wynikających z nich działań szybciej, taniej i bez szkody [Kuszewski, Szapiro, Szufel 2015, s. 7]. Mamy przy tym świadomość, że poznajemy dany fragment rzeczywistości BiPP jedynie z określonego punktu widzenia, przyjętego w założeniach poznawczych. Jesteśmy więc w stanie dostrzec, zaobserwować tylko, określony celem poznania bądź zakresem posiadanej wiedzy czy poznawczym zmotywowaniem, ustalony podzbiór, czyli wybrane elementy badanego układu. Elementy te i zachodzące między nimi relacje ustalane są w sposób arbitralny przez obserwatora w procesie obserwacji systemu. Tak więc pomiędzy modelem a oryginałem zachodzą określone zależności, pozwalające na sformułowanie wniosków dotyczących oryginału na podstawie obserwacji modelu. Wówczas model odgrywa rolę poznawczego pośrednika pomiędzy poznającym badaczem a system oryginałem [Flakiewicz 2002, s. 15].

Model zagrożeń dla BiPP występujących w środowisku społecznym, wykorzystywany do eksperymentowania – symulowania ich rozwoju, oddziaływania,

możliwości ich eliminowania, powinien być skonstruowany w sposób pozwalający odpowiedzieć m.in. na następujące pytania badawcze:

(1) Jakie zmiany w środowisku społecznym prowadzą do istotnych zmian w strukturze i intensywności zagrożeń BiPP? Jak możemy poznawać zagrożenia wpływające na ogólny poziom BiPP w środowisku?

(2) Jak możemy określić, jakie rodzaje interwencji poprawiłyby BiPP? Jakie są różnice w efektach wprowadzenia doraźnych instrumentów interwencyjnych wpływających na intensywność zagrożeń i ich skutki?

(3) Jak możemy ustalić gotowość społeczeństwa i jego instytucji do wdrożenia interwencji w zakresie BiPP?

(4) W jaki sposób możemy określić najlepszą drogę do wdrożenia interwencji w zakresie BiPP? Jakie są skutki wprowadzania interwencji na różne sposoby?

(5) Jaką korzyść odnosi człowiek, a jaką społeczeństwo z wdrożenia określonych działań w obszarze BiPP?

(6) Jak zróżnicowanie indywidualnych cech podmiotów (jednostek organizacyjnych działających w obszarze BiPP oraz jednostek i grup społecznych w lokalnych środowiskach) wpływa na organizacje działań jednostkowych i wielopodmiotowych na rzecz BiPP?

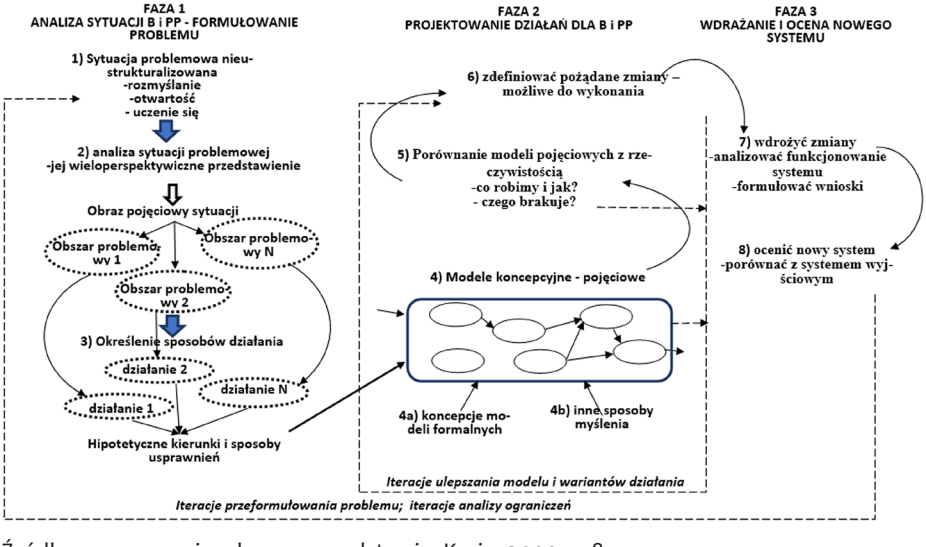
Przedstawione pytania, nie pretendując do miana wyczerpującego zestawu pytań, mają pozwolić zauważyć złożoność procesów związanych z rozwojem i oddziaływaniem zagrożeń dla BiPP oraz ich eliminowaniem przez organizacje działające w tym obszarze, jak i przez ludzi (pojedyncze osoby czy grupy).

Miejsce modelu i modelowania w podejściu systemowym do badania zjawisk BiPP

Na podejście systemowe składają się fazy, etapy i czynności (rysunek 2). W fazie pierwszej koncentrujemy uwagę na analizach różnych sytuacji wpływających na stan i dynamikę BiPP. Budujemy o nich wiedzę, pozwalającą na identyfikację zachodzących zjawisk generujących zagrożenia, jak i tych chroniących ludzi, organizacje i środowisko. Realizując etapy fazy pierwszej, poszukujemy odpowiedzi na następujące pytania: jakie są założenia i cele systemu BiPP? Jakie są realizowane procesy w systemie oraz jakie zasoby zaangażowane są w ich realizację? Jaka jest struktura systemu i jakie są jego elementy i relacje pomiędzy nimi? Jaka jest struktura tych elementów, postrzeganych indywidualnie lub jako całość? Z jakich zasileń korzysta system, jakie są efekty ich przetwarzania oraz ograniczenia utrudniające ich przetwarzanie? Jak i w jakie wchodzą interakcje w systemie i środowisku? Jakie są granice systemu? Jakie są cele realizowanych procesów i ich przebiegi? Czy w efekcie tej fazy badacz systemu może stwierdzić, jakie są rozbieżności między „co jest"

a tym, „co jest wymagane"? Pomaga to w określeniu występujących w systemie problemów bezpieczeństwa oraz ich środowiskowego kontekstu, a także w formułowaniu hipotez, przekładających potrzeby bezpieczeństwa na cele i sposoby ich realizacji. W efekcie umożliwia to badaczowi szybsze i dokładniejsze przedstawienie sytuacji problemowej, jej różnych aspektów np. zlokalizowanie zachowań, procesów funkcjonalnych i procesów dysfunkcjonalnych, dewiacyjnych dla systemu. Wówczas, łączy on w logiczną całość wszystkie informacje i różne perspektywy, tworząc bogaty obraz analizowanej sytuacji, który pokazuje jej elementy, ich znaczenia, związki i relacje pomiędzy nimi, szanse, zagrożenia, mocne i słabe strony. Taki rozbudowany obraz sytuacji stanowi bogate źródło informacji o niej, pozwalające dostrzegać jej złożoność, nadawać znaczenia jej elementom i wiążącym je relacjom. Następnie, dla wybranych problemów, pozwala na wskazanie na adekwatne do określonych problemów kierunki działania i wyrażanie tych myśli – propozycji sposobów działania i ich hipotetycznych efektów w kategoriach systemowych. Określenie tych propozycji stanowi podstawę do modelowania koncepcyjnego, a w rzeczywistości jest zwartą wersją naszego zrozumienia sytuacji. Pozwala to badaczowi ujawnić i sformułować ważne dla sytuacji tematy i zagadnienia, które stanowią problem/y, a które należy poddać analizom w dalszej pracy analitycznej i projektowej.

Rysunek 2. Fazy, etapy i kroki podejścia systemowego



Źródło: opracowanie własne na podstawie: Karim 2009, s. 8.

Kluczowe znaczenie ma realizacja fazy drugiej – projektowanie działań istotnych dla prawidłowego funkcjonowania systemu BiPP to badanie możliwych sposobów osiągnięcia celu. Istotne jest tu pytanie dotyczące cech, jakie musi posiadać modelowe narzędzie analityczne do badania zagrożeń BiPP, ich oddziaływania, potencjalnych skutków i sposobów eliminowania. Rozważania wskazują na konieczność uwzględnienia w modelu [Kuszewski, Szapiro, Szufel 2015, s.10-11]:

1. istotnych cech czynników sprawczych zagrożenia (podmiotowych i przedmiotowych) w różnorakich uwarunkowaniach i etapach jego aktywizowania się i oddziaływania;

2. kluczowych cech czynników opisujących pokrzywdzonych oddziaływaniem zagrożenia w różnorakich uwarunkowaniach i etapach jego aktywizowania się i oddziaływania;

3. heterogeniczności i hierarchii w procesie podejmowania decyzji o sposobach zapobiegania rozprzestrzeniania i potęgowania zagrożeń,

4. różnych form oddziaływania przez jednostki i instytucje na sytuacje BiPP,

5. decyzji dotyczących każdego podmiotu, którego zachowanie podlega modelowaniu,

6. zależności społecznych, kulturowych, technicznych, rodzinnych i innych charakteryzujących modelowane sytuacje, zarówno na poziomie mikro, mezo, jak i na poziomie makro.

Podejściem, które pozwala na uwzględnienie powyższych założeń, jest metoda modelowania systemu na poziomie mikro, w której traktuje się system jako zbiór niezależnych elementów. Cechy i zachowanie tych elementów nie mogą być rozpatrywane jako prosta suma czynników składowych, gdyż całość posiada cechy inne i niewystępujące w żadnym elemencie składowym. Te cechy są następstwem współdziałania, współzależności i różnorodności poszczególnych elementów składowych systemu. Modele takie pozwalają więc uwzględniać zróżnicowanie indywiduów, interakcje między nimi i obserwować pojawiające się efekty sieciowe. W modelu takim pojedyncze elementy są autonomiczne, ale powiązane z otoczeniem. Twórca modelu ustala jego elementy składowe, określa ich charakterystyki. Praca z modelem polega na prowadzeniu eksperymentów i badaniu dynamiki systemu według określonych wcześniej reguł. To umożliwia elastyczny i sekwencyjny przegląd różnych zestawów elementów modelu i ich powiązań wewnętrznych i z otoczeniem. W efekcie daje wyobrażenie o m.in. stanie i przebiegu danego procesu, jego efektach, a eksperymentowanie z użyciem różnych zestawów elementów umożliwia optymalizację procesu, zarówno w wymiarze indywidualnym, jak i zagregowanym, co służy rozwojowi i doskonaleniu określonych działań [Kuszewski, Szapiro, Szufel 2015, ss. 13–15].

Faza trzecia to wdrażanie i ocena nowego systemu, mająca na celu poprawę sytuacji BiPP. Po porównaniu wariantów działania i ocenie pozytywnych i negatywnych skutków każdego z wariantów, dysponujemy planem składającym się z konkretnych i możliwych do wykonania działań. W planie należy też uwzględnić metody oraz wskaźniki postępów. Niemniej jednak nie jest to koniec procesu, gdyż poprawienie sytuacji (w przeciwieństwie do rozwiązania problemu) jest procesem stopniowym i powtarzalnym. Przechodzenie przez cykle podejścia systemowego zwiększa wiedzę badacza i interesariuszy o zagrażającej sytuacji, a także o roli różnych czynników związanych z sytuacją, co powiązane jest z procesem uczenia się, który odbywa się podczas iteracji. W tym etapie ocenić należy, czy związek pomiędzy sytuacją a uczeniem się jest na tyle efektywny, że pozwala na rozwiązanie sytuacji.

Identyfikacja zagrożeń – budowanie modelu zagrożenia dla BiPP

Identyfikacja i zrozumienie dynamiki zagrożeń związanych z sytuacją stanowi punkt wyjścia analiz i decyzji o sposobach działania dla poprawy bezpieczeństwa i porządku publicznego. Istotne jest poznanie cech czynników sprawczych zagrożenia (podmiotowych i przedmiotowych) i ich znaczenia dla jego oddziaływania w różnorakich uwarunkowaniach i etapach jego aktywizowania się. Wymaga to między innymi:

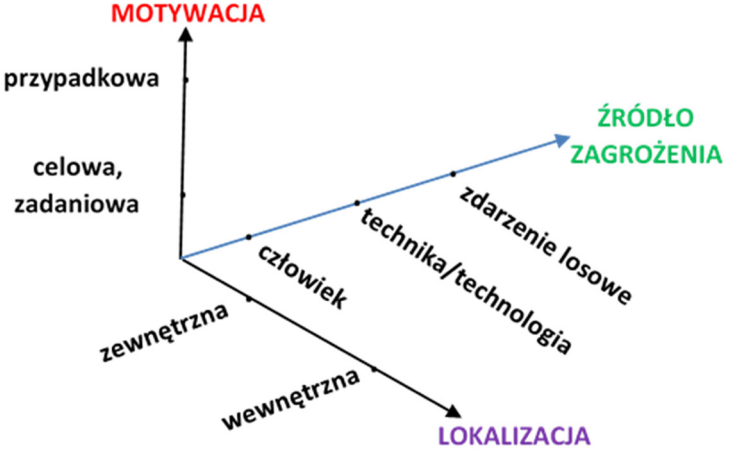
1. precyzyjnego zdefiniowania czynników wpływających na BiPP,
2. określania różnorakich relacji i zależności występujących pomiędzy nimi,
3. wdrożenia jednoznacznej terminologii opisującej te czynniki,
4. stałego budowania wiedzy o wielorakiej złożoności problemów i czynników wpływających na BiPP.

Dlatego istotne jest, po pierwsze, żeby przed opracowaniem np.: modeli/planów działań profilaktycznych dla BiPP czy programów szkolenia młodzieży, w tym procedur i instrukcji bezpiecznego zachowania się w sytuacjach zagrażających, właściwie zdefiniować czynniki warunkujące BiPP, a to jest wykonalne dopiero po wnikliwej ich obserwacji i analizie w rzeczywistych warunkach, gwarantujących zrozumienie ich istoty, występujących powiązań i oddziaływania. Po drugie, określenie kontekstu [PN-EN ISO 9000: 2015, punkt 2.2.3], czyli czynników w zewnętrznym i wewnętrznym otoczeniu sytuacji zagrażającej, które są ważne dla dynamiki tej sytuacji oraz realizacji celów i osiągania zamierzonych efektów BiPP. Zaproponować można tutaj metodykę opisu zagrożenia, wykorzystującą podział przestrzeni zagrożenia na podprzestrzenie zgodnie z modelem trzech wymiarów ortogonalnych oznaczonych pojęciami: źródło zagrożenia (przyczyny

zajścia niebezpiecznego zdarzenia), motywacja (aktywizująca zdarzenie niebezpieczne), lokalizacja (miejsca zajścia niebezpiecznego zdarzenia) (rysunek 3).

Dla przykładu przedstawiono identyfikację – modelowe przedstawienie zagrożeń wywołujących zdarzenia niebezpieczne w osobowym transporcie miejskim, stanowiące podstawę podjęcia działań mających na celu zmniejszenie liczby takich zdarzeń oraz minimalizację ich skutków. Problemem do rozwiązania będzie poznanie/ określenie czynników występujących w środkach komunikacji miejskiej i w społecznym otoczeniu, wywołujących agresję pasażerów i na tej podstawie wskazanie różnorakich sposobów ograniczających to zjawisko.

Rysunek 3. Wizualizacja wymiarów zagrożenia

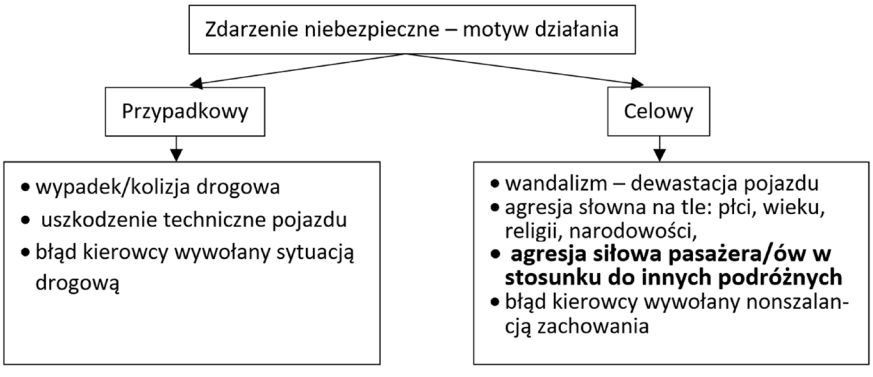


Źródło: opracowanie własne, na podst.: Ruf i in. online, dostęp: 25.03.2019.

Tok myślowej analizy przedstawiono kolejno na rysunkach (tekstem pogrubionym przedstawiono omawiane zagrożenie):

- **na rysunku 4 –** klasyfikacja zdarzeń niebezpiecznych ze względu na motywację aktywizującą zdarzenie [Woropay, Boja 2010, ss. 51–60];

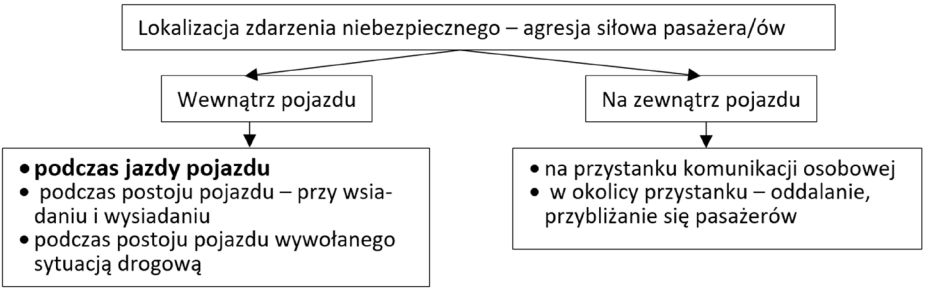
Rysunek 4. Zdarzenia niebezpieczne ze względu na motywację aktywizującą zdarzenie



Źródło: opracowanie własne.

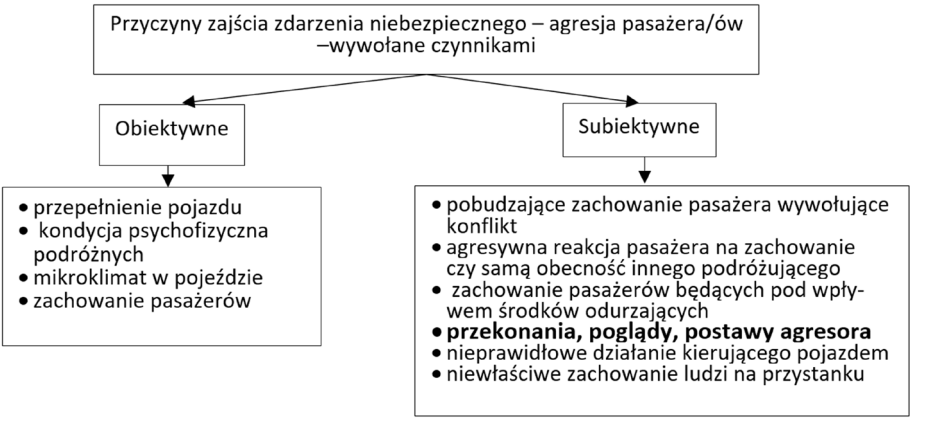
- **na rysunku 5** – klasyfikacja czynników wywołujących zdarzenie niebezpieczne: agresja siłowa pasażera/ów, w aspekcie miejsce zajścia zdarzeń niebezpiecznych;
- **na rysunku 6** – prawdopodobne przyczyny zajścia zdarzenia niebezpiecznego, rozpatrywane w perspektywie czynników obiektywnych i subiektywnych;
- **na rysunku 7** – dwuwymiarowa macierz relacji i zależności wiążących wybrane czynniki sytuacyjne i czynniki otoczenia sprzyjające użyciu agresji siłowej przez pasażera w środkach komunikacji miejskiej w stosunku do innego podróżującego. Celem tworzenia takich macierzy jest przedstawienie powiązań i zależności między znaczącymi dla rozwoju zagrożenia/ agresji czynnikami sytuacyjnymi i otoczenia, prowadzące do wyodrębnienia, zrozumienia i komunikowania tych relacji. Relacje te ukazywane są w parach czynników rozmieszczonych w rzędach i kolumnach macierzy. Znaczenie powiązań pomiędzy czynnikami sytuacyjnymi, a także między czynnikami sytuacyjnymi i otoczenia, może być określane w postaci reguły subiektywnej, co ułatwia pozyskiwanie wiedzy, wyjaśniającej powstawanie i rozwijanie się zagrożenia związanego z taką sytuacją. Taka macierz jest operacyjnie bardziej przydatna, gdy stosujemy ją także do określenia siły i dynamiki tych związków.

Rysunek 5. Czynniki wywołujące zdarzenie niebezpieczne: agresja siłowa pasażera/ów, w aspekcie miejsce zajścia zdarzenia



Źródło: opracowanie własne.

Rysunek 6. Prawdopodobne przyczyny zajścia zdarzenia niebezpiecznego rozpatrywane w perspektywie czynników obiektywnych i subiektywnych



Źródło: opracowanie własne.

Rysunek 7. Macierz przykładowych relacji pomiędzy czynnikami wywołującymi zachowania agresywne

	Czynniki sytuacyjne	Lekceważenie podmiotowości ludzi przez agresora	Anonimowość agresora – ograniczona odpowiedzialność	Zaspokojenie potrzeby agresora manifestowania poglądów	Brak reakcji pasażerów na przejawy agresji – lęk przed atakiem	Czynniki otoczenia	Przyzwolenie polityczno-społeczne na zachowania agresywne	Minimalne prawdopodobieństwo poniesienia odczuwalnej kary	Brak szybkiej reakcji organów porządkowych na agresję
Czynniki sytuacyjne	X	Relacje: czynniki sytuacyjne – czynniki sytuacyjne					Relacje: czynniki sytuacyjne – czynniki otoczenia		
Lekceważenie podmiotowości ludzi przez agresora		X						Brak wewnętrznych zahamowań	
Anonimowość agresora – ograniczona odpowiedzialność			X						
Zaspokojenie potrzeby agresora manifestowania, siły, postaw, poglądów				X	Nieskrępowane agresywne zachowania				
Brak reakcji pasażerów na przejawy agresji – lęk przed atakiem					X				
Czynniki otoczenia		Relacje: czynniki otoczenia – czynniki sytuacyjne				X	Relacje: czynniki otoczenia – czynniki otoczenia		

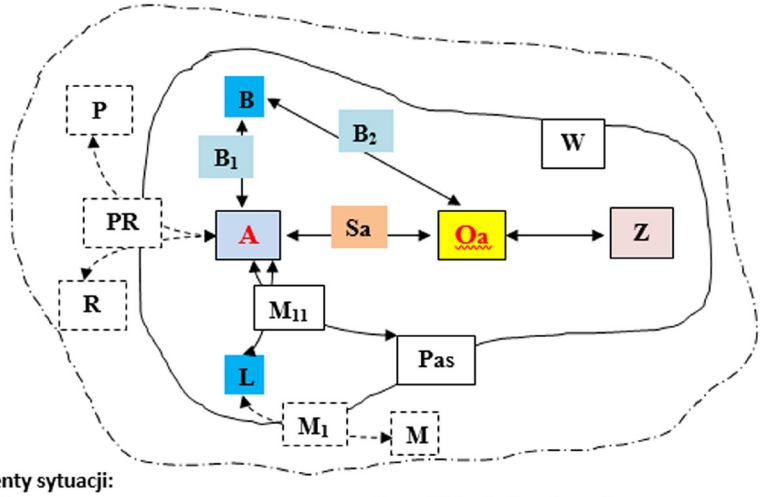
	Czynniki sytuacyjne	Lekceważenie podmiotowości ludzi przez agresora	Anonimowość agresora – ograniczona odpowiedzialność	Zaspokojenie potrzeby agresora manifestowania poglądów	Brak reakcji pasażerów na przejawy agresji – lęk przed atakiem	Czynniki otoczenia	Przyzwolenie polityczno-społeczne na zachowania agresywne	Minimalne prawdopodobieństwo poniesienia odczuwalnej kary	Brak szybkiej reakcji organów porządkowych na agresję
Czynniki sytuacyjne	X	Relacje: czynniki sytuacyjne – czynniki sytuacyjne					Relacje: czynniki sytuacyjne – czynniki otoczenia		
Przyzwolenie polityczno-społeczne na zachowania agresywne					Uwolnienie od poczucia winy, skrupułów		X		Skłanianie do agresji
Minimalne prawdopodobieństwo poniesienia odczuwalnej kary			Swoboda zachowań agresywnych					X	
Brak szybkiej reakcji organów porządkowych na agresję									X

Źródło: opracowanie własne.

• **na rysunku 8** – model zdarzenia niebezpiecznego, przedstawiający zależności strukturalne wybranych elementów sytuacji zagrażającej i jej otoczenia. Modelując zagrożenie, badacz, z wielu możliwych rzeczy, zjawisk, zdarzeń czy cech opisujących sytuację zagrażającą, ulokowaną w danej społecznej rzeczywistości, świadomie wybiera tylko te elementy, które pozwalają uporządkować i opisać tę sytuację, a w konsekwencji wyjaśnić, jaka kombinacja tych elementów i w jaki sposób determinują to zagrożenie, dając jego skoordynowany obraz. Zakłada się, że czynniki powstania sytuacji niebezpiecznej traktować należy jako zdarzenia czy fakty niezależne, które mogą oddziaływać pojedynczo lub łącznie. Przyczyna sprawcza agresji (główna) – użycie siły (S) przez agresora (A)

w stosunku do ofiary agresji (Oa) uaktywnia się na skutek równoczesnego oddziaływania kombinacji różnych czynników sytuacyjnych i z otoczenia sytuacji, które wywołują motywację do działania u agresora (rysunek 8).

Rysunek 8. Model zagrożenia agresją siłową i jego uwarunkowania



Elementy sytuacji:
Oa – ofiara agresji
W – wnętrze środka komunikacji
A – agresor, anonimowość agresora
Sa – siła agresji
Pas – pasażerowie
Z – zagrożenie, skutki użycia siły

Czynniki i relacje sytuacyjne:
B – brak reakcji pasażerów na przejawy agresji
B_1 – relacja sprzyjająca agresorowi
B_2 – relacja zwiększająca zagrożenie Oa
L – lekceważenie podmiotowości ludzi przez agresora
M_{11} – motywacja użycia siły przez agresora

Czynniki i relacje sytuacyjne i otocznie:
M – minimalne prawdopodobieństwo poniesienia odczuwalnej kary
M_1 – pobudzenie motywacji użycia siły przez agresora
P – przyzwolenie polityczno-społeczne na zachowania agresywne
R – brak szybkiej reakcji organów porządkowych na agresję
PR – zachęta do agresji odczuwana przez agresora

Źródło: opracowanie własne.

Zakończenie

Zaproponowane podejście metodyczne, ilustrujące sposób budowania modelu zagrożenia, może być pomocne w przezwyciężaniu trudności związanych z niepewnością i złożonością rzeczywistych sytuacji zagrażających. Dobrze opracowane

modele, a temu służy przedstawiona propozycja metodyczna, mogą stać się doskonałym narzędziem wspomagającym procesy opisu, wyjaśniania i rozumienia sytuacji zagrażających, a w konsekwencji trafności decyzji operacyjnych. Modele takie i eksperymentowanie na nich, czyli wykorzystywanie możliwości wirtualnego badania i przekształcania rzeczywistości bezpieczeństwa, pozwalają na wypracowanie modelu funkcjonalnego ze znanymi parametrami, który wskazuje na konieczne działania zapewniające pożądany poziom bezpieczeństwa i porządku publicznego.

Bibliografia

Balcerak A., Kwaśnicki W., *Modelowanie symulacyjne systemów społeczno-gospodarczych: różnorodność podejść i problemów* [online], https://www.researchgate.net/publication/265823604, dostęp: 23.03.2019.

Flakiewicz W. (2002), *Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje,* Wydawnictwo C. H. Beck, Warszawa.

Gomółka Z. (2000), *Cybernetyka w zarządzaniu. Modelowanie cybernetyczne. Sterowanie systemami*, Agencja Wydawnicza Placet, Warszawa.

Jankowski B. (1997), *Modelowanie rozwoju krajowego systemu energetycznego z uwzględnieniem wymagań stabilizacji redukcji emisji dwutlenku węgla w Polsce,* IPPT PAN, Warszawa.

Karim S. (2009), *Applying Systems Approach to Educational – Organizational Change - Improvment of an Interdisciplinary Program: Master Program in Sustainable Development*, Institutionen för Geovetenskaper, Uppsala University.

Koźmiński A.K. (1979), *Analiza systemowa organizacji*, PWN, Warszawa.

Kuszewski T., Szapiro T., Szufel P. (2015), *Modelowanie wieloagentowe w badania decyzji edukacyjnych,* Instytut Badań Edukacyjnych, Warszawa.

Misiuk A. (2008), *Administracja porządku i bezpieczeństwa publicznego*, Warszawa.

Morawski J.M. (2002), *Dominanty ujęć systemowych* [w:] *Wybrane problemy metodologii badań na potrzeby sportu*, M.J. Morawski (red.), Warszawa.

Ruf L., Thorn A., Christen T., Gruber B., Portmann R., *Threat Modeling in Security Architecture – The Nature of Threats* [online], https://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf, dostęp: 25.03.2019.

Sadowski W. (1978), *Podstawy ogólnej teorii systemów. Analiza logiczno-metodologiczna*, Warszawa.

Sprengel B. (2008), *Służby mundurowe ochrony bezpieczeństwa wewnętrznego*, Toruń.

Wiśniewski B. (red.) (2007), *Zarządzanie bezpieczeństwem państwa w kontekście zadań administracji publicznej*, Wyższa Szkoła Administracji, Bielsko-Biała.

Woropay M., Bojar P. (2010), *Identyfikacja zdarzeń niepożądanych w systemie transportu miejskiego*, „Problemy Eksploatacji", nr 1.

Bogdan Panek
bpanek@spoleczna.pl
Społeczna Akademia Nauk

Mirosław Banasik
miroslaw.banasik@interia.pl
Uniwersytet Jana Kochanowskiego

Przyszłość Europy i konsekwencje dla polskiej polityki bezpieczeństwa i obrony

Wstęp

Generalny trend, z jakim mamy do czynienia w ostatnich latach, ukazuje bardzo negatywny rozwój środowiska bezpieczeństwa w Europie i w Polsce. Obecnie istnieje wiele geopolitycznych kryzysów (Bliski i Środkowy Wschód, Korea Północna i Ukraina), mamy do czynienia z niepewnym rozwojem światowej gospodarki i nasilonymi konfliktami zbrojnymi na peryferiach Europy. Unia Europejska obecnie znajduje się na drodze pewnego ożywienia, starając się przezwyciężyć fazę stagnacji, wynikłą z wewnętrznych sporów i błędów jej państw członkowskich. W tym samym czasie Stany Zjednoczone Ameryki Północnej pod przywództwem Donalda Trumpa stopniowo wycofują się z odpowiedzialności za globalne bezpieczeństwo, będąc wcześniej jego głównym czynnikiem stabilizacji i coraz częściej skłaniają się w kierunku przyjęcia „dzikiej karty". Wynikająca z tego „próżnia władzy" wypełniana jest przez Chiny, Rosję oraz potęgi regionalne (Iran, Arabia

Saudyjska), co w konsekwencji powoduje dodatkową dynamikę konfliktu. Ponadto, wiele wyzwań związanych z bezpieczeństwem pozostaje a nawet wzrasta w związku z masowymi migracjami, międzynarodowym terroryzmem, wojnami hybrydowymi, cyberatakami, zagrożeniami dla egzystencji, a także niestabilnością w europejskim sąsiedztwie (Bałkany Zachodnie, Turcja, Bliski i Środkowy Wschód).

Celem niniejszego rozdziału było zidentyfikowanie i diagnoza kluczowych czynników środowiska bezpieczeństwa międzynarodowego, w tym głównie mających wpływ na przyszłość Europy i Polski. Realizacji tak sformułowanego celu posłużyły następujące problemy badawcze:

1. Jakie są obecnie główne determinanty rozwoju środowiska bezpieczeństwa międzynarodowego i jakie czynniki wywierają największy wpływ na przyszłość Europy?

2. Jakie konsekwencje mogą z tego wynikać dla polityki bezpieczeństwa i obrony Rzeczpospolitej Polskiej?

Podstawową metodą, wykorzystywaną w przygotowywaniu publikacji, była analiza, ocena i synteza zgromadzonych źródeł naukowych. Ponadto zastosowano także wnioskowanie, aby sformułować najistotniejsze wyniki realizowanych badań.

W pierwszej części przedstawiono kluczowe czynniki dla rozwoju środowiska bezpieczeństwa międzynarodowego w dającej się przewidzieć przyszłości. Zwrócono w niej uwagę zarówno na rozwój globalnej polityki władzy, globalny rozwój gospodarczy i dystrybucję bogactwa, jak i rozwój konfliktów w Europie i wokół niej. Ponadto nakreślono prognozy rozwoju Unii Europejskiej, uwzględniając przy tym zarówno działania Federacji Rosyjskiej, Sojuszu Północnoatlantyckiego (NATO), a także dokonując oceny stabilności regionów sąsiadujących z Europą. Następnie, w oparciu o przeprowadzone wcześniej analizy i oceny kluczowych czynników wpływających na przyszłość Europy, przedstawiono możliwe konsekwencje dla polskiej polityki bezpieczeństwa i obrony.

Kluczowe czynniki dla rozwoju środowiska bezpieczeństwa międzynarodowego

Rozwój globalnej polityki władzy[1]

Wizja funkcjonowania światowej architektury bezpieczeństwa jest częścią tak ważnych obszarów, jak: bezpieczeństwo, gospodarka i sprawy społeczne, zakłócanego obecnie porządku, a raczej nieporządku światowego, przez ,,zamożne i potężne państwa'', które wkroczyły w daleką przyszłość. Pod względem geopolitycznym druga dekada XXI wieku, w odróżnieniu od poprzednich, charakteryzuje się dużą złożonością, współzależnościami oraz wysokim stopniem niestabilności. Na scenie politycznej, w obliczu wielu kryzysów mających obecnie miejsce w wielu regionach świata, następuje wyraźne wzmocnienie trendu do wielobiegunowej konfrontacji. Przy czym stabilny jest trend, jeśli chodzi o konfrontacyjny charakter globalnej polityki władzy, ale zmienny pod względem orientacji ze zmieniającą się polaryzacją. W związku z tym, z dzisiejszej perspektywy nie można wykluczyć, że obecna stabilizująca się wielobiegunowość z udziałem strategicznych graczy (USA, Chiny i Rosja) w perspektywie średnio i długoterminowej może powrócić do dwubiegunowości. Może mieć to miejsce w sytuacji, gdy Chiny i Rosja wzmocnią swoją dwustronną współpracę i wspólnie staną w opozycji do USA. Również możliwy, choć mało prawdopodobny, byłby scenariusz, w którym USA dążyłyby do zacieśnienia współpracy z Rosją, podejmując jednocześnie bardziej konfrontacyjny kurs wobec Chin. Istotnymi wskaźnikami takiego rozwoju są widoczne zmiany w polityce zagranicznej administracji USA pod przywództwem Donalda Trumpa i próżnia władzy w Unii Europejskiej, bez głównego aktora hegemonicznego. Pojawienie się rywali waszyngtońskich, zarówno w Pekinie, jak i w Moskwie, jest uderzające, co na poziomie geostrategicznym powoduje ,,pogłębienie się okopów''. Ma to miejsce w czasie, gdy Rosja koncentruje się na zminimalizowaniu wpływów innych potęg w przestrzeni proradzieckiej, a Chiny rozwijają się w skali globalnej, rozszerzając swój wpływ geoekonomiczny w Euroazji (projekt ,,jeden pas – jedna droga''). Ta konfrontacyjna wielobiegunowość jest napędzana przez bardzo kruchą i niestabilną sytuację geoekonomiczną, zdominowaną obecnie przez konkurencję o energię, kapitał i zasoby ludzkie, a także nowoczesne technologie. Współcześnie cyberataki stały się integralnymi elementami sprawowania władzy i odbywają się w przestrzeni, która jest w dużej mierze nieuregulowana.

[1] Zob. szerzej: Panek, Stawicki 2018.

W dającej się przewidzieć przyszłości ta konkurencyjna pozycja wyjściowa przyniesie trwałą rywalizację energetyczną oraz doprowadzi jednocześnie do sięgania po instrumenty projekcji siły, takie jak: sankcje gospodarcze lub zagrożenia militarne w spornych regionach granicznych (Korea Północna, Ukraina, Turcja, Iran, Półwysep Arabski, region MENA – Środkowy Wschód i Afryka Północna). Powyższe sprawia, że w najbliższej przyszłości nie można wykluczyć otwartego konfliktu zbrojnego. W sensie tzw. ,,pułapki Tukidydesa" z powodu niebezpieczeństwa, że wznosząca się potęga wejdzie w konflikt z obecnie dominującym supermocarstwem, która w naszej historii doprowadziła do konfliktów wojennych w 12 z 16 porównywalnych konstelacji.

Wraz z perspektywą nasilenia konfliktu regionalnego na peryferiach czterech globalnych bloków władzy (USA, Chiny, Rosja, Unia Europejska), brakuje również zdolności do rozwiązywania konfliktów, zwłaszcza na poziomie stale osłabianych organizacji międzynarodowych, głównie ONZ. Organizacje te nazywane są obecnie ,,infrastrukturami krytycznymi", które wymagają wysokiego poziomu polityki międzynarodowej. Jednak, jak to określa ,,pułapka Kindelbergera", jej znaczenie jest związane z powstaniem lub upadkiem hegemonicznych mocy, które ją niosą. Równie wielka jest zależność od gotowości wielkich mocarstw do wspierania zdolności organizacji międzynarodowych do działania i prowadzenia koncepcji skutecznego multilateralizmu.

Globalny rozwój gospodarczy i dystrybucja bogactwa

W perspektywie średnioterminowej należy się spodziewać ciągłej stagnacji światowej gospodarki i dominacji konkurencyjnych bloków gospodarczych. Zachód znalazł się w stagnacji w wyniku coraz bardziej protekcjonistycznej polityki handlowej. Urbanizacja rośnie w bardzo szybkim tempie, co w konsekwencji sprawia, że we wszystkich ważnych metropoliach świata powstają duże okręgi ubóstwa. Niektóre miasta z szeroką bazą dobrze wykształconych pracowników mają dobrze prosperującą gospodarkę i stają się prawdziwym globalnym centrum innowacji. Jednak większość innych megamiast, określanych mianem ,,nieudaczników postępu", nie będzie uczestniczyć w tym dobrobycie, zwiększając globalne nierówności społeczne. Wzrost migracji z sąsiednich krajów, a także z regionów objętych konfliktem, będzie nadal wzrastał. Ta sytuacja ma miejsce w zamożnych obszarach o coraz bardziej restrykcyjnych kontrolach granicznych. W związku z tym, uregulowanie przyszłej imigracji lub integracja już istniejącej pozostaje głównym wyzwaniem na nadchodzące lata.

W ostatnich latach wzrost PKB w Chinach spowolnił z czterech do sześciu procent. Znalazło to odzwierciedlenie i dotyczy to również gospodarek europejskich,

których rynki w większości reagują negatywnie. Istniejące przepływy handlowe i wolumeny spadają ze względu na protekcjonistyczne otoczenie legislacyjne, a także fakt, że Chiny zaczęły rozwijać własny przemysł wysokich technologii. Obecnie stosunki amerykańsko-chińskie w polityce gospodarczej są bardziej konkurencyjne niż kooperatywne. Powoduje to, że dwie największe gospodarki na świecie konkurują o podobne rynki docelowe i odpowiadające im akcje. Chiny przejmują stopniowo przywództwo w dużej mierze unipolarnej Azji. Pojawiają się oznaki zmiany w kierunku niezrównoważonego wzrostu (również z nasilonymi konfliktami) w wyniku globalnej konkurencji napędzanej przez polaryzację gospodarczą między USA a Chinami [Krumbein 2019, s. 4].

Unia Europejska pozostaje jednym z trzech największych globalnych graczy w handlu międzynarodowym (obok USA i Chin). Podkreślenia przy tym wymaga, że już obecnie UE jest najważniejszym partnerem handlowym Chin, a każdego dnia wymieniane są towary o wartości 1,6 mld euro. W czasach stagnacji na rynkach krajowych z jednej strony chiński biznes oferuje wielu europejskim firmom możliwość przeszacowania i zwiększenia ich bilansów, z drugiej zaś – Chiny wzywają do rozwoju rynku europejskiego. Dzięki projektom w ramach inicjatywy „jeden pas – jedna droga[2] Chiny chcą rozszerzyć swoją pozycję gospodarczą i strategiczną poza Azję i Europę i wzmocnić ją oraz zabezpieczyć w skali globalnej. Jednak istnieją różnice głównie w kwestiach handlowych (dumping, dyskryminacja europejskich przedsiębiorstw w Chinach). Konflikty determinują również stosunki Unii Europejskiej z coraz bardziej protekcjonistycznymi Stanami Zjednoczonymi Ameryki Północnej. Przy czym spór o otwarty handel wydaje się raczej mało prawdopodobny z powodu transatlantyckich powiązań kapitałowych, zależności od amerykańskich przedsiębiorstw na rynku Unii Europejskiej, a także negatywnych konsekwencji, takich jak: wyższe ceny i działania odwetowe.

W każdym razie ta dynamika geoekonomiczna może być wykorzystana do uzyskania znacznego potencjału konfliktu w sensie domniemanej wielobiegunowości w systemie międzynarodowym. Rozbieżne interesy w dziedzinie ekonomii mogą przekształcić się w spór przy wykorzystaniu środków militarnych. Ponadto, spowolnienie globalnego rozwoju gospodarczego, spowodowanego zmianami klimatycznymi i demograficznymi, znajduje odzwierciedlenie w masowej migracji i uchodźstwie. Obecnie ok. 795 mln ludzi na świecie cierpi z powodu głodu, 750 mln nie ma dostępu do czystej wody pitnej – a liczba ludzi dotkniętych tym problemem wzrasta.

[2] Bezpośrednie połączenie kolejowe ze wschodniego wybrzeża Chin przez Rosję i Białoruś do Wiednia, korytarz bałkański z portu w Pireusie przez Serbię i Węgry do Europy Zachodniej. Przypis własny.

W związku z globalnym ociepleniem przewiduje się utratę znacznej części gruntów rolnych w Afryce Subsaharyjskiej w ciągu najbliższych 15–20 lat, a to z kolei może spowodować duży napływ ludności z tego regionu do Europy.

Rozwój konfliktów w Europie i wokół niej[3]

Bardzo niebezpieczny i stabilny trend zmierza w kierunku konfliktów hybrydowych i asymetrycznych, które zwykle się toczą z dużą intensywnością, ale czasami z niskim progiem. Celem ataków hybrydowych nie jest już kontrola nad przejęciem terytoriów, lecz są one zorientowane na wywarcie wpływu na źródła decydujące o warunkach egzystencji społeczeństw, a także suwerenności i integralności państw. Państwowi i niepaństwowi agresorzy wykorzystują celowo luki w obszarach bezpieczeństwa, słabości w zarządzaniu kryzysowym państwa i brakujące zasoby obronne. Dochodzi do użycia środków wojskowych poza wojną konwencjonalną. Również instrumenty globalizacji są coraz częściej wykorzystywane do hybrydowego sprawowania władzy. Szczególną rolę odgrywa przestrzeń cybernetyczna i informacyjna, obejmująca wszystkie elementy infrastruktury informacyjnej, do których przez Internet można uzyskać dostęp na całym świecie. Poważne ataki przy pomocy cyberbroni (zautomatyzowane złośliwe oprogramowanie, backdoory, zagłuszanie, mikrofale) mogą spowodować poważne szkody dla warunków życia państw i społeczeństw. W cyberprzestrzeni niepaństwowi przeciwnicy działają obecnie na równi z zachodnimi siłami zbrojnymi i siłami bezpieczeństwa.

To z kolei oznacza, że wykorzystujące na szeroką skalę technologie (utechnicznione) społeczeństwa są coraz bardziej zależne od cyberprzestrzeni, a poprzez to bardziej podatne na cyberataki. W rezultacie staje się ona głównym miejscem konfliktów, a także obszarem operacji w ramach wojny klasycznej i hybrydowej, ponieważ w cyberprzestrzeni przy wykorzystaniu stosunkowo niewielkich nakładów można osiągnąć wspaniałe efekty w konfrontacji z pozornie przytłaczającym i dużo silniejszym przeciwnikiem.

Z kolei, w odniesieniu do klasycznych konfliktów zbrojnych, mają one coraz częściej miejsce na terenach zurbanizowanych (głównie w miastach). Ponadto pojawia się kolejna progresywna technologia (cyfryzacja, automatyzacja, robotyka) działań wojennych. Konflikty toczą się w bardzo asymetryczny sposób, a nierówność mniej odnosi się do nierównowagi sił niż do celowego przeciwdziałania regułom i normom (np. łamanie prawa wojennego) przez słabszą stronę. Skutkuje to pryncypialną anarchią, która będzie miała trwały wpływ na konflikty zbrojne.

[3] Na podstawie: *Sicherheitspolitische Jahresvorschau 2019* 2018.

Symptomem tego rozwoju jest: tzw. państwo islamskie – ISIS. W konsekwencji prowadzi to do podwójnej strategii – z jednej strony działa się nadal jak terrorystyczna milicja z paramilitarną farbą, a drugiej strony jak perfidna organizacja terrorystyczna, która będzie jeszcze długo wyzwaniem dla europejskiej walki z terroryzmem. Grupa dzihadystów, której pozycja jako gracza militarnego w Syrii i Iraku (w 2018 r.) została zachwiana, umiejętnie wykorzystuje elementy hybrydyzmu, asymetrii, konspiracji, anarchii i elastyczności. Na syryjskim polu bitwy działali jako nieregularne jednostki bojowe, a w europejskich metropoliach jako terroryści z niezwykle brutalnymi aktami przemocy.

Mając na uwadze przyszłość, bardzo ważnym wyzwaniem jest niebezpieczeństwo związane z systematycznym terroryzmem, który znacznie wykracza poza znany nam wcześniej potencjał zagrożenia. W przeciwieństwie do konwencjonalnych ataków terrorystycznych, dokonywanych przez małe grupy lub pojedynczych przestępców, jest to atak zagrażający suwerenności przez wyszkolonych i wyposażonych sił zbrojnych na państwo, społeczeństwo i ich źródła utrzymania.

Obecnie Europa dotknięta jest trzecią falą przemocy terrorystycznej, która ma trzy zasadnicze cele, a mianowicie: **po pierwsze** – utrwalenie trwałego poczucia braku bezpieczeństwa, **po drugie** – związanie sił bezpieczeństwa, a **po trzecie** – podział i radykalizację społeczeństw zachodnich. W tym celu są obecnie wykorzystywane trzy rodzaje ataków:

- ataki na dużą skalę, które są kierowane z zewnątrz;
- autonomiczne ataki na lokalne cele;
- zabójstwa dokonywane przez oportunistycznych przestępców i samozwańcze jednostki oraz zradykalizowane osoby.

W celu przeciwdziałania temu zjawisku potrzebna jest w pełni zintegrowana strategia antyterrorystyczna, która obejmie wspólne działania niezbędnych sił i środków policyjnych, wywiadowczych, sądowniczych i wojskowych.

Rozwój Unii Europejskiej

Przyszły scenariusz obecnego trendu na przyszłość wskazuje raczej na słabą Unię Europejską. Chociaż wiele najgorszych „czarnych scenariuszy", związanych z wyborami krajowymi niektórych jej państw członkowskich w 2017 roku, nie sprawdziło się, pozostaje bardzo duża nieufność do elit politycznych i instytucji. Ponadto, w Unii Europejskiej panuje także niezgoda co do pozycji zajmowanych w stosunku do USA i Rosji, a także działań podejmowanych w ramach masowych migracji. Generalnie, reagowanie na zmiany polityki bezpieczeństwa w ostatnich latach było

niepewną odpowiedzią, która jest związana z faktem, że nie znaleziono jeszcze wspólnej strategicznej odpowiedzi na nowe wyzwania. Jednak mimo tych negatywnych oznak, istnieją także pozytywne zmiany, które rozjaśniają nieco przedstawiony wcześniej negatywny trend i, pomimo wszystkich czynników zakłócających, sugerują konsolidację. Pozytywnym sygnałem są m.in. ważne decyzje podjęte w ramach Wspólnej Polityki Bezpieczeństwa w 2018 roku. „Godzina prawdy" jest uderzająca, ponieważ dzięki Stałej Współpracy Strukturalnej następuje zasadniczy zwrot przejścia z dobrowolnej wcześniej współpracy wojskowej do ukierunkowanej strategicznie integracji obronnej. Proces ten po raz pierwszy zostaje wzmocniony aktywną rolą Komisji Unii Europejskiej w sprawach obronnych oraz przez prawnie i politycznie wiążące kryteria (budżet, inwestycje, badania, uczestnictwo w projektach i operacje). Ponadto będą koordynowane zarówno Roczny Przegląd Obronny (ang. *Coordinated Annual Review on Defence* – CARD), jak i systematyczna wymiana informacji między państwami członkowskimi UE w sprawach dotyczących ich planów obronnych.

Jednocześnie nowo utworzony Europejski Fundusz Obronny oferuje zachęty finansowe do współpracy w pozyskiwaniu nowych zdolności wojskowych i projektów zbrojeniowych. Sukces całego projektu, który zakłada stworzenie Unii Obronnej o wspólnej puli zdolności (transport strategiczny, struktury dowodzenia, bazy szkoleniowe i logistyczne), będzie w dużym stopniu zależał od woli jego wdrożenia w Niemczech, Francji i Włoszech. Zbliżające się wyjście Wielkiej Brytanii z Unii Europejskiej może mieć mniej drastyczny wpływ na politykę bezpieczeństwa niż się to powszechnie zakłada, ponieważ BREXIT w perspektywie średnioterminowej może doprowadzić do konsolidacji oraz odrodzenia się Francji jako głównego gracza w UE i ożywienia relacji na osi francusko-niemieckiej. Decydujące znaczenie ma tu czynnik czasu, ponieważ przedstawione pozytywne kierunki zmian są dopiero na etapie wstępnym, a postępy, mające związek z ogólną sytuacją UE, muszą być ściśle monitorowane. Ponadto od czasu wstępnej analizy sprzed dwóch lat tendencje odśrodkowe w Unii Europejskiej zawsze były poważniejsze [Brockmann, Giegerich, Mecit 212].

Ruchy separacyjne m.in. w Katalonii, Szkocji oraz częściowo w Irlandii Północnej są obecnie dodawane do niepohamowanych ambicji renacjonalizacyjnych w niektórych państwach członkowskich UE. Pomimo tych wyzwań zakłada się powolną, ale zasadniczo stabilną Unię Europejską, także z powodu ponownego wzrostu jednolitego rynku. Ze względu na niepewność strukturalną UE, która jest wynikiem wyjścia Wielkiej Brytanii oraz sporów wewnętrznych jej państw członkowskich, istnieje oczywiście także możliwość (w najgorszym przypadku) utwo-

rzenia rdzenia Europy. Przy czym należy zakładać, że w okresie obserwacji UE będzie podejmowała dalsze wysiłki integracyjne. Świadczą o tym ostatnie sygnały, które wskazują na pełną konsolidację i „odnajdywanie się" w erze po Brexicie [Nuspliger 2018a, s. 4; 2018b].

Od 2016 roku podstawowe ramy Wspólnej Polityki Bezpieczeństwa i Obrony (WPBiO) tworzy Globalna Strategia UE (EUGS) z trzema głównymi priorytetami, do których należą: **reagowanie na zewnętrzne konflikty i kryzysy, budowanie zdolności partnerów oraz ochrona Unii i jej obywateli.**

W odniesieniu do przyszłości WPBiO przewodniczący Komisji Europejskiej Jean-Claude Juncker w 2017 roku opracował trzy scenariusze, z których **pierwszy to** „Współpraca w dziedzinie Bezpieczeństwa i Obrony". Zakłada on, że 27 państw członkowskich UE w obszarze bezpieczeństwa i obrony będą w przyszłości częściej ze sobą współpracować (na zasadzie dobrowolności) a w razie potrzeby będą podejmowane decyzje *ad hoc* w oparciu o skalę początkowych korzyści. W szczególności oznaczałoby to interoperacyjne siły zbrojne, zarządzanie kryzysowe i budowanie zdolności.

Drugi scenariusz opisuje „wspólną odpowiedzialność za bezpieczeństwo i obronę", zgodnie z którą 27 państw członkowskich stopniowo wykazuje większą solidarność i poprawia swoje zdolności w zakresie projekcji siły militarnej. Na poziomie sił zbrojnych oznaczałoby to opracowanie i wdrożenie programu innowacyjnych technologii, wymiany informacji, operacji o wysokiej intensywności oraz stałych wielonarodowych komponentów sił zbrojnych.

Natomiast ostatni, **trzeci scenariusz** – „Wspólna Obrona i Bezpieczeństwo" zakłada, że 27 państw członkowskich zacieśnia współpracę na rzecz bezpieczeństwa i obrony. Jego podstawę stanowi systematyczna i wspólna ocena zagrożeń i planowania awaryjnego, wspólne finansowanie i tworzenie wymaganych zdolności, poprawa odporności i żywotności sił oraz wysoki poziom integracji sił zbrojnych – tutaj byłyby liczone konkretne wyniki.

Z kolei, jeśli chodzi o europejskie wydatki na obronę, to one nadal rosną i w 2017 roku wyniosły 219 mld euro. Jednak przy wydatkach na obronę znacznie wyższy jest poziom inflacji niż wydatki ogólnie (z 4 do 7%) – tak więc nadmierne wydatki nie zdołały zrównoważyć inflacji. Wymagałoby to co najmniej 250 mld euro tylko w samym w 2017 roku. Podkreślenia przy tym wymaga, że budżety wojskowe i zamówienia mają bardzo różne wzorce regionalne. Spośród 15 krajów Europy Północnej i Wschodniej – 10 zwiększyło swoje inwestycje obronne, a w Europie Zachodniej i Południowej z dwunastu jedynie sześć. Dlatego też widać wyraźnie rewitalizację obecnego skupienia na interwencjach międzyna-

rodowych i nową, bardziej zrównoważoną relację pomiędzy „obroną w domu" a misjami międzynarodowymi. Powód powyższego stanu rzeczy jest oczywisty, ponieważ zróżnicowane postrzeganie zagrożeń trwa i określa, do czego będzie wykorzystywany budżet obronny. I tak w przypadku państw członkowskich UE, które obecnie to właśnie Rosję uważają jako główne zagrożenie dla ich bezpieczeństwa, główny nacisk kładzie się na systemy konwencjonalne. Natomiast państwa, które uważają terroryzm za priorytetowe wyzwanie, inwestują w szersze spektrum zorientowane na działania ekspedycyjne. Jednak to tylko duże państwa NATO zachowują szerokie krajowe spektrum zdolności, podczas gdy mniejsi sojusznicy koncentrują swoje ograniczone zasoby na „niszy wojskowej" i usługach wsparcia.

Z materiałów źródłowych wynika, że w europejskich programach obronnych 51% z 127 transakcji zakupu dotyczyło systemów lotniczych, 31% sił lądowych i 24% sił morskich (marynarki wojennej). Obecnie największe programy dotyczą natomiast śmigłowców wielozadaniowych i transportowych, pojazdów opancerzonych oraz okrętów przeznaczonych do obrony wybrzeża. Innym trendem rozwoju militarnego jest zwiększanie sił personelu wojskowego, czego przykładem jest nasz kraj, gdzie dąży się do stworzenia 50 tysięcznych sił obrony terytorialnej. Z kolei, w Bundeswehrze siła aktywnego składu zostaje zwiększona o 20 000 żołnierzy a w Wielkiej Brytanii i Francji powstają nowe siły rezerwowe dla potrzeb bezpieczeństwa wewnętrznego.

Federacja Rosyjska

Z przeprowadzonych analiz wynika, że nadszarpnięte i konfliktowe stosunki z Rosją utrzymają się jeszcze w perspektywie średnioterminowej. Obecny stan relacji pomiędzy Unią Europejską i Rosją z jednej strony, a UE i USA z drugiej, wynika głównie ze sprzecznych interesów, uzasadnionych i nierealnych obaw oraz pragnienia „zachowania twarzy". W ten sam sposób jest ona zdecydowanie zaostrzona przez skomplikowaną, czasami napiętą wewnętrzną sytuację polityczną wszystkich trzech aktorów. Ponadto, istnieją także wykluczające się wzajemnie narracje i brak wspólnej wizji przyszłości. W związku z tym, obecny system wzajemnych sankcji pozostawia niewiele miejsca na nową wersję polityki „zmiany poprzez zbliżenie".

Bez wątpienia priorytetowym celem strategicznym Rosji wobec Zachodu jest maksymalne osłabienie więzi transatlantyckiej i jej głównych filarów, czyli NATO i Unii Europejskiej. Wskazuje to, że w perspektywie krótko i średnioterminowej stosunki UE – Rosja będą charakteryzowały się konkurencją geopolityczną i geoekonomiczną dla przestrzeni proradzieckiej na Kaukazie Południowym, Europie

Wschodniej i w pewnym stopniu Bałkanach Zachodnich. Zdaniem Rosji Ukraina powinna zostać zinstytucjonalizowana i stworzyć neutralne państwo. To ostatnie powinno mieć miejsce także w Mołdawii.

Pozostałe cele Rosji obejmują niedopuszczenie do członkostwa Gruzji w NATO i UE, a także utrzymanie zależności Armenii od rosyjskiego bezpieczeństwa. Podkreślenia przy tym wymaga, że Europa Wschodnia jako całość jest otwartym bokiem Unii Europejskiej. Oprócz znajdujących się tam kruchych i słabych struktur państwowych, obok zamrożonego konfliktu na Ukrainie i częściowo w Górnym Karabachu, także trwające konflikty terytorialne (Naddniestrze, Abchazja, Osetia Południowa i Krym) wskazują, że w dającej się przewidzieć przyszłości nie należy oczekiwać trwałego rozwiązania tych problemów.

Kreml bez wątpienia dąży do utrzymania przyczółków na Morzu Śródziemnym w celu dostępu do starych baz wojskowych w Egipcie, Jemenie oraz Libii i na te potrzeby wykorzystuje strategie hybrydowe. Największym ryzykiem pozostaje jednak kryzys na Ukrainie z ciągłym, olbrzymim potencjałem do jego dalszej eskalacji. Powyższą sytuację pogarsza fakt, że administracja prezydenta Trumpa nie określiła jeszcze do tej pory jasnej wizji stosunków USA – Rosja. Ponadto, wydaje się, że kontrola zbrojeń zatrzymała się na długi czas po wygranych po raz kolejny przez Władimira Putina wyborach prezydenckich w 2018 roku. Można jednak założyć, że w najbliższej przyszłości Rosja będzie dążyć do zacieśnienia stosunków dwustronnych z poszczególnymi państwami UE, zwłaszcza w obliczu napięć z USA i starać się o zbliżenie między Unią Europejską a Euroazjatycką Unią Gospodarczą.

Przeprowadzone analizy i oceny wykazały, że jak dotąd gospodarka rosyjska okazała się odporna na system sankcji nałożonych na nią przez Zachód. Największy wpływ wywierają one w dziedzinie technologii, a w szczególności duże obciążenie stanowią w sektorze ropy naftowej i gazu ziemnego oraz przemyśle obronnym. Należy przy tym podkreślić, że pomimo sankcji powiązania gospodarcze pomiędzy Unią Europejską a Rosją pozostają szczególnie silne w sektorze energetycznym. Chociaż Unia Europejska będzie nadal utrzymywać swoje sankcje, to jest mało prawdopodobne, by któreś z państw członkowskich chciało ich zaostrzenia w 2020 roku. Czynnikami ryzyka dla Rosji pozostają nowe potencjalne sankcje ze strony USA i ogólnie konflikt z nimi. Chociaż ograniczona konfrontacja wojskowa z Rosją wydaje się teoretycznie możliwa na wschodnich peryferiach Europy, to kompleksowe wyzwanie dla całej Europy jest nierozpoznawalne. Jednak biorąc pod uwagę pragmatyczną politykę zagraniczną, bezpieczeństwa i gospodarki Kremla, scenariusz ten jest raczej mało prawdopodobny. Należy przy

tym zakładać z dużym stopniem prawdopodobieństwa, że Rosja nadal będzie aktywnie reprezentowała swoje interesy, ale z niewielką intensywnością konfliktu.

Sojusz Północnoatlantycki – NATO

NATO odzyskało rolę geopolitycznego gracza. Z jednej strony strategicznymi priorytetami są obrona sojusznicza, chociaż należy niestety podkreślić, że nie dla wszystkich państw członkowskich w równym stopniu. Z drugiej strony NATO pozostaje cały czas Sojuszem w działaniu, który oprócz misji szkoleniowych i wspierających, prowadzi operacje zwłaszcza w Afganistanie, Kosowie i regionie Morza Śródziemnego. Jednak jako organizacja *stricte* wojskowa nie jest w stanie w równym stopniu objąć wszystkich wymiarów konfliktu hybrydowego. Napięte stosunki z Rosją zatrzymały spadek budżetów obronnych i doprowadziły do nowych wojskowych programów inwestycyjnych. Obawy związane z potencjalnym odejściem USA, pod przywództwem Donalda Trumpa, z NATO zostały ostatecznie rozwiane. Stany Zjednoczone jak dotąd dotrzymały wszystkich zobowiązań dotyczących zwiększenia sił wojskowych w Europie. Nie odwróciły się od niej – pozostając niewygodnym, lecz wiarygodnym partnerem. Oczywiście presja na europejskich sojuszników będzie nadal zwiększać wydatki obronne do 2% PKB.

Wewnętrznie Sojusz Północnoatlantycki jest obecnie w trybie adaptacji i dyskusji strategicznej, co stanowi efekt napiętych stosunków z Rosją, będących wynikiem konfliktu na Ukrainie. NATO zareagowało na to zmianami w strukturze dowodzenia i zwiększoną obecnością wojskową w Europie Środkowej i Wschodniej. W konsekwencji napiętej sytuacji ostatni szczyt NATO w lipcu 2018 roku był zdominowany trzema następującymi problemami: relacje z Rosją, reformy strukturalne oraz budżet.

Niestety pomiędzy NATO i Wspólną Polityką Bezpieczeństwa i Obrony UE nie ma nadal bezpośredniej współpracy na poziomie dwóch równorzędnych partnerów i jest wręcz odwrotnie, ponieważ UE w kwestiach obronności staje się częścią NATO (obecnie istnieje 66 form współpracy). Niemniej jednak autonomia strategiczna Unii Europejskiej, w tym kwestie dotyczące bezpieczeństwa i obrony, powinny leżeć we wspólnym europejskim interesie i być realizowane bez niepotrzebnego dublowania na poziomie wojskowo-technicznym.

Stabilność sąsiadujących regionów europejskich[4]

Przeprowadzone analizy wykazały, że obecnie w eurostrategicznym regionie ma miejsce 20 konfliktów zbrojnych, co sprawia, że środowisko Europy będzie

[4] Na podstawie: Europäische Kommission 2017(a i b), 18 final, s. 5.

w dużym stopniu zdominowane przez niestabilność i konflikty w wymiarze średniookresowym. Przejawiają się one między innymi w postaci konfliktów o zróżnicowanym natężeniu, nieskonsolidowanych stanów pokoju i niestabilnej państwowości, działaniach terrorystycznych i zwiększonej presji migracyjnej na Europę. To wszystko sprawia, że obecnie ten „nieporządek polityczny" w sąsiednich regionach, co prawda ograniczony i niezagrażający bezpośrednio egzystencji, wywiera bardzo duży wpływ na stabilność Unii Europejskiej. Jeśli jednak w sąsiednich regionach nie zostanie odwrócony ten negatywny trend – to w perspektywie średnioterminowej można sobie wyobrazić poważne zagrożenie dla UE i jej państw członkowskich, co ma znaczący wpływ na bezpieczeństwo Unii. Z kolei, kompleksowe zagrożenie wojskowe ze strony nieeuropejskiej w powyższej perspektywie wydaje się mało prawdopodobne.

Ukraina

Od 2014 roku tli się konflikt zbrojny na granicy między Rosją a Ukrainą i nadal stanowi wysokie ryzyko. Podczas gdy nie było otwartej wojny pomiędzy Rosją a Ukrainą – to trwa nieprzerwanie stan między „wojną a pokojem". Na razie wydaje się, że zarówno Rosja, jak i Ukraina w dużej mierze zaakceptowały *status quo*. Powyższa sytuacja daje Ukrainie możliwość zwrócenia się o pomoc zachodnią i odroczenie na jakiś czas reform wewnętrznych kraju. Jednocześnie został powstrzymany proces integracji Ukrainy ze strukturami Zachodu, co z kolei przynosi korzyści Rosji. Próby znalezienia pokojowego rozwiązania na razie zamrożonego konfliktu w perspektywie krótkoterminowej wydają się mało prawdopodobne. Działania misji pokojowych ONZ będą jedną z kluczowych kwestii w rozwiązywaniu konfliktów, jednak wiele pytań pozostaje otwartych. Ponowna eskalacja przemocy w 2019 roku wydaje się mało prawdopodobna, ale nie jest całkowicie wykluczona. Kolejna próba Kijowa rozwiązania konfliktu donbaskiego przy wykorzystaniu środków militarnych, a być może nawet ze wsparciem zachodnim, byłaby dla Rosji „czerwoną linią" do wejścia w otwarty konflikt zbrojny. Jednak biorąc pod uwagę trudną sytuację społeczno-ekonomiczną Ukrainy, utrzymanie stabilności wewnętrznej wydaje się ważniejsze od reintegracji dwóch samozwańczych Republik Doniecka i Ługańska do wspólnoty narodu.

Bałkany Zachodnie

Z przeprowadzonych analiz i ocen sytuacji w regionie Bałkan Zachodnich wynika, że w perspektywie średnioterminowej utrzyma się nadal zagrażająca stabilności stagnacja. Odpowiedzialne są za to tendencje nacjonalizmu i secesja, brak zaufania, autorytarne zmiany i uporczywe problemy społeczno-gospodarcze, a także

postępy politycznego islamizmu. Z powodu tych niestabilności politycznych i gospodarczym możliwe są konflikty między etniczne. Jednak wybuch nowych, gwałtownych konfliktów jest raczej mało prawdopodobny ze względu na prowadzoną przez Unię Europejską politykę włączenia regionu. Podkreślenia przy tym jednak wymaga, że stopniowe osłabianie UE mogłoby potencjalnie zaostrzyć wrodzone antagonizmy na Bałkanach Zachodnich. Bezpiecznik „beczki z prochem" znajduje się w rękach Brukseli, ponieważ perspektywa UE pozostaje kluczowym czynnikiem konsolidacji i stabilności regionu. Dlatego potrzebne jest bardziej aktywne zaangażowanie UE w regionie i ciągła obecność wojskowa.

Turcja

Prowadzona w ostatnich latach analiza sytuacji wskazuje, że w najbliższej przyszłości Turcja pozostanie strefą problemową i hamulcem dla europejskiej polityki zewnętrznej i integracyjnej. Nawet, jeśli dotychczas rząd Turcji podtrzymał porozumienie dotyczące uchodźców, to fakt ten prawdopodobnie nie wystarczy, by pozytywnie ukształtować przyszłe relacje z jej zachodnimi partnerami. Były one i są nadal naznaczone wzajemną alienacją i nieufnością od czasu nieudanego zamachu stanu w 2016 roku. Biorąc pod uwagę politykę wewnętrzną, Turcja dalej rozwija się w kierunku islamsko-konserwatywnym, co może mieć również negatywne konsekwencje dla napiętych stosunków z Europą, a co gorsze, realizowany przez nią program regionalny destabilizuje jej bezpośrednie otoczenie.

Bliski i Środkowy Wschód

Bliski i Środkowy Wschód odznacza się szczególnie wysoce wybuchowym i niestabilnym bezpieczeństwem oraz sytuacją gospodarczą. Obecnie w konflikty na tym obszarze zaangażowana jest bardzo duża liczba podmiotów państwowych i niepaństwowych. Szczególne znaczenie ma pogłębienie się dyfuzji potęg regionalnych, w tym przede wszystkim Iranu i Arabii Saudyjskiej, do podmiotów niepaństwowych. Ze względu na rozbieżne interesy kluczowych graczy (USA, Rosja, Iran, Arabia Saudyjska, Zjednoczone Emiraty Arabskie, Katar, Turcja i Egipt) na Bliskim i Środkowym Wschodzie, a także brak zdolności ONZ do rozwiązywania konfliktów, nie ma żadnych pozytywnych prognoz na stabilizację regionów w okresie krótko- i średnioterminowym. Ponadto terroryzm, który w trwały sposób destabilizuje region, osłabia także jego zdolność do rozwiązywania własnych problemów politycznych i gospodarczych.

Podkreślenia przy tym wymaga, że pomimo niestabilności na Bliskim i Środkowym Wschodzie, czynniki te mają niewielki czy też ograniczony wpływ na

Europę. Zagrożenia dla Europy w tym kontekście to ataki terrorystyczne przeprowadzane przez tzw. państwo islamskie – w wyniku utraty zajętego wcześniej terytorium w Syrii i Iraku. Ataki te są przeprowadzane przez zdalnie sterowane komórki terrorystyczne lub w przeważającej mierze przez zradykalizowane pojedyncze osoby, a także zwiększone przepływy uchodźców, zwłaszcza z Syrii, Iraku, Palestyny lub Egiptu. Jednak głównym niebezpieczeństwem pozostaje to, że wojny w Syrii, Jemenie, Iraku i Libii przeradzają się w poważną międzynarodową wojnę religijną (Sunnici kontra Szyici) lub hegemoniczną wojnę (Iran kontra Arabia Saudyjska). Jest to wynikiem coraz bardziej aktywistycznej polityki zagranicznej obecnego księcia koronnego Mohammeda bin Salmana. Po interwencji militarnej w Jemenie (2015) można zaobserwować teraz rozszerzenie konfliktu irańsko-saudyjskiego na Liban, co w konsekwencji może spowodować dalsze wzmocnienie potencjału eskalacji i prowadzić do wzmocnienia grup terrorystycznych.

Afryka Północna

Generalnie w Afryce Północnej nie należy się spodziewać znaczących zmian w polityce bezpieczeństwa w nadchodzących latach. Chaotyczna zmiana na szczytach władzy w Algierii i związane z nią zawirowania polityczne mogą w krótkim okresie zwiększyć presję migracyjną w Europie. Z kolei, w Libii rozdrobnienie instytucji i zużycie rezerw finansowych reżimu Kadafiego utrudniają znalezienie rozwiązania politycznego i zagranicznego zarządzania kryzysowego. Jednak ograniczone terytorialnie konflikty w Libii nie mają jeszcze potencjału, by doprowadzić do destabilizacji całego regionu. Natomiast na poziomie strategicznym – wojskowym na pierwszym planie znajduje się rosnące zagrożenie konfliktem hybrydowym i rosnąca potrzeba sił stabilizacyjnych lub też interwencyjnych w celu zwalczania masowo tłumionego tzw. państwa islamskiego (ISIS).

Konsekwencje dla polskiej polityki bezpieczeństwa i obrony

Scenariusz przedstawionych tendencji powyżej charakteryzuje się eskalacją kryzysów geopolitycznych i konfliktów w Europie. Prawie 15-letni okres względnego pokoju w Europie od zakończenia wojny na Bałkanach i dywidendy pokojowej dobiegł końca. Rozpoczął się nowy wiek niepewności, który charakteryzują: wojny hybrydowe, cyberataki, międzynarodowy terroryzm, przestępczość zorganizowana,

masowe migracje, niestabilne regiony sąsiadujące oraz zmienny globalny rozwój polityczny i gospodarczy.

W przypadku masowej migracji można ogólnie przyjąć, że będzie ona kontynuowana w okresie następnych lat. Istnieje jednak ryzyko gwałtownego wzrostu w kontekście rozwoju sytuacji w Turcji i tendencji dezintegracyjnych w Afryce Północnej (Egipt, Algieria i Libia). Możliwe konsekwencje to zwiększenie migracji, jak i przemyt terrorystów do Europy, a także Polski. Z powodu nowych zagrożeń hybrydowych Polska jest dziś w wielu dziedzinach życia bardziej niepewna niż w okresie zimnej wojny. Podczas gdy ten drugi był przewidywalny, konflikty hybrydowe występują bez wcześniejszego ostrzeżenia i mają wysoki potencjał eskalacyjny. Polska jest już celem i miejscem konfliktów hybrydowych na poziomie politycznym, gospodarczym i wojskowym. W zależności od aktora, intencji i potencjału, konfrontacja odbywa się na różnych poziomach eskalacji. W sferze gospodarczej oznacza to sankcje dla polskich firm, inwestycje zagranicznych państwowych funduszy majątkowych i firm w przedsiębiorstwa o infrastrukturze krytycznej w Polsce oraz związaną z tym utratę kontroli, a także budowę zależności technologicznych od podmiotów spoza Europy.

Natomiast, jeśli chodzi o aspekt polityki zagranicznej dotyczący zagrożeń hybrydowych Polska stoi w obliczu ukierunkowanych procesów destabilizacji w środowisku europejskim. Możliwe konsekwencje to straty gospodarcze, izolacja w polityce zagranicznej Polski w organizacjach międzynarodowych, destabilizacja sąsiedztwa, pojawienie się radykalnych struktur politycznych i celowe wykorzystanie działań hybrydowych przeciwko polskim i europejskim interesom bezpieczeństwa. W dziedzinie społeczno-politycznej zagrożenia hybrydowe można przedstawić następująco: infiltracja fundamentalizmu religijnego i radykalizacja, zwłaszcza w środowisku islamistycznym, instrumentalizacji organizacji pozarządowych (stowarzyszenia kulturalne i fundacje), rozpowszechnianie fałszywych wiadomości, finansowanie sieci zorganizowanej przestępczości i rekrutacja terrorystów dla Dżihadu.

Obecnie, a także w przyszłości, bardzo dużym wyzwaniem dla Polski są cyberataki, których celem może być doprowadzenie do ogromnej awarii zasilania i infrastruktury krytycznej oraz masowe ataki cybernetyczne na suwerenność Polski, co miałoby bardzo poważne konsekwencje. Według badań przeprowadzonych przez Instytut Oceny Technologii (ang. Institute for Technology Assessment)

w 2017 roku „Blackout" [Strzoda, Skrzypiec 2007][5] wpływa „nie tylko na wszystkie infrastruktury krytyczne, które zależą od dostaw energii, ale także wszyscy obywatele stwarzają dodatkowe zagrożenia dla społeczeństwa". W takich sytuacjach tylko siły zbrojne mogą chronić integralność cybersystemów państwowych.

Kolejne zagrożenia stanowią pandemie, przy których wysoce zakaźny patogen może zabić w ciągu jednego roku ok. 30 mln ludzi na całym świecie. Pandemie są chorobami zakaźnymi, które się bardzo szybko rozprzestrzeniają i nie zatrzymują się na granicach państw czy kontynentów. Teoretycznie pandemie mogą być wywołane atakami terrorystycznymi i atakami broni biologicznej. Zakres niebezpieczeństwa, jakie stanowi pandemia, wykazano w kilku przypadkach z nie tak odległej przeszłości: świńska grypa (2009/2010) oraz gorączka Ebola (2014–2016). Gdyby Polska została dotknięta pandemią, polskie Siły Zbrojne byłyby niezbędne jako rezerwa strategiczna do działania ze względu na niszczycielskie skutki dla ludności, strategicznej infrastruktury i ważnych procesów w usłudze powszechnej.

Terroryzm nadal stanowi poważne zagrożenie dla bezpieczeństwa Polski, ponieważ wraz z powrotem zagranicznych bojowników, mogą przybywać wojskowo zorganizowani i wyszkoleni bojownicy również do Polski. Chociaż w Polsce nie miały jeszcze miejsca ataki terrorystyczne, to nastąpił wzrost przemocy terrorystycznej na szczeblu międzynarodowym. Ma to quasi militarny poziom organizacji, której celem jest szerzenie trwałego braku bezpieczeństwa i podział społeczeństw zachodnich. Jednocześnie dostęp do ciężkiej broni i innych środków z potencjałem do masowego niszczenia staje się łatwiejszy. Tak więc w Polsce mogą wystąpić ataki terrorystyczne, które są jakościowo i ilościowo równoważne atakowi, który zagrażałby suwerenności tzw. terroryzm systemowy.

Słabość Unii Europejskiej pozostaje ciężarem, ponieważ przyszły przebieg Polityki Zagranicznej i Bezpieczeństwa UE pozostaje otwarty, pomimo pozytywnej perspektywy Stałej Współpracy Strukturalnej (PESCO). W związku z tym, Polska nie może w pełni polegać na kompetencyjnych rozwiązaniach Unii w kluczowych kwestiach i musi podjąć środki ostrożności samodzielnie, niezależnie lub wspólnie

[5] **Blackout** – rozległa awaria zasilania nazywana jest *blackoutem*. Awarię taką definiuje się jako utratę napięcia w sieci elektroenergetycznej na znacznym obszarze. Każda awaria typu blackout ma inne przyczyny, ale można mówić o schemacie dochodzenia do blackoutu. W wyniku sekwencji kilku losowych zdarzeń (awarie sieciowe, wyłączenia elektrowni, ekstremalne warunki atmosferyczne) dochodzi do przekroczenia krytycznych wartości podstawowych parametrów technicznych pracy systemu (częstotliwość, napięcie), automatycznego odłączenia się od sieci elektrowni i utraty napięcia na całym obszarze objętym zakłóceniem.

z państwami o podobnych poglądach, co z kolei wymaga odpowiednich zdolności krajowych. Rozwijająca się Europejska Współpraca Wojskowa (PESCO) nie stanowi potencjalnej oszczędności dla Polski, ponieważ kto chce być wiarygodnym partnerem, musi mieć odpowiednie zasoby i silną narodową armię.

Na poziomie globalnym coraz powszechniejsze stają się konfrontacyjna wielobiegunowość, zbrojenia i zagrożenia. Stany Zjednoczone Ameryki pod przywództwem Trumpa zdecydowały się obrać kurs unilateralny (rezygnując z multilateralizmu), który jest wykorzystywany przez Chiny i Rosję. Z drugiej strony Unia Europejska wydaje się słaba, choć istnieją pozytywne tendencje. Na Ukrainie i w Syrii prowadzone są wojny zastępcze tzw. *proxy* wojny. Podobnie „peryferiom Europy" zagraża dalsza dezintegracja, upadek państw i pojawienie się „próżni mocy". Pojawiają się regionalne strefy wpływów, na obrzeżach których toczy się konflikt (Bałkany, Bliski i Środkowy Wschód, Afryka Północna). Ogólnie rzecz biorąc, współcześnie istnieje ogromny potencjał militarny, gdy spirala uzbrojenia się wciąż obraca, a polityczna wola tej mocy może się zmienić. Z tych względów w przyszłości istnieje konwencjonalne ryzyko wojskowe także dla Polski.

Stosunki między Rosją a Europą należy uważnie obserwować, szukając kompleksowej możliwości konfrontacji militarnej w dłuższej perspektywie. Obecnie tak nie jest, jednak, gdyby w dalszej przyszłości miałoby do niej dojść, wiązałoby się to z poważną reorientacją polityki obronnej Unii i jej państw członkowskich. W związku z tym, należy niezwłocznie podjąć działania, które spowolnią dalszą eskalację i umożliwią odwrócenie trendu w kierunku drogi współpracy. Biorąc pod uwagę konfrontację między USA i Rosją oraz upadek programu zbrojeń w Europie, szczególne znaczenie mają środki budowy zaufania w ramach Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE). W 2017 roku ustanowiono „zorganizowany dialog na temat obecnych i przyszłych wyzwań i zagrożeń w ramach bezpieczeństwa OBWE". W dłuższej perspektywie należy między innymi ustanowić ewentualne negocjacje w sprawie kontroli zbrojeń w Europie.

W środowisku eurostrategicznym zarówno operacje militarne, jak i mające po nich miejsce stabilizacyjne w przeszłości, tylko częściowo doprowadziły do sukcesu. Obecnie będące do dyspozycji siły zbrojne państw europejskich, biorąc pod uwagę ich żywotność (zdolność do przetrwania), ze względu na różnorodność operacji prowadzonych poza granicami kraju, a także zadania realizowane w kraju, muszą posiadać szerokie spektrum zdolności do działania. Ta nadmierna ekspansja staje w obliczu rosnącej potrzeby sił zbrojnych i sił bezpieczeństwa.

W kontekście przyszłości należy przy tym oczekiwać, że brak międzynarodowej woli interwencyjnej oraz nadmierne obciążenie sił zbrojnych doprowadzą do dalszego pogorszenia sytuacji w zakresie bezpieczeństwa w środowisku eurostrategicznym.

Zakończenie

Z przedstawionych wyzwań i ryzyk na poziomie koncepcyjnym wynika, że zarówno Strategia Bezpieczeństwa RP, jak i jej strategia sektorowa (Strategia Obronności), a także struktury Podsystemu Kierowania Bezpieczeństwem muszą być poddane analizie i ocenie, a następnie dostosowane do zmieniającej się sytuacji środowiska europejskiego. Polska polityka obronna musi być kompleksowo przemyślana i rozwijana w kierunku przyszłych wyzwań i zagrożeń. W centrum jej wysiłków powinna znaleźć się obrona przed zagrożeniami hybrydowymi, ponieważ należy założyć, że będzie miało miejsce strategiczne przygotowanie, planowanie i koordynacja działań hybrydowych przez siły militarne przeciwnika. Obrona przed tym zagrożeniem wymaga wysokiego stopnia wiedzy na poziomie strategiczno-wojskowym (ang. *know-how*, czyli wiedzieć jak) i koordynacji wszystkich środków. Szczególnym wyzwaniem jest równoczesne wystąpienie kryzysów, katastrof i ataków hybrydowych, co wymaga skoordynowanego użycia wszystkich sił i środków bezpieczeństwa narodowego.

Nadrzędnym celem jest przygotowanie i zapewnienie strategicznych działań, w tym zdolności do reagowania na nowe zagrożenia hybrydowe. W przypadku natychmiastowych, nadzwyczajnych zagrożeń należy zapewnić i zagwarantować przetrwanie polskiego systemu politycznego, społecznego i gospodarczego. Ważnym jest także wzmocnienie działających sił w przypadku poniesienia strat, a ochrona ludności powinna być w centrum wszystkich rozważań. Na poziomie operacyjnym radzono sobie dotychczas z łatwymi kryzysami i sytuacjami klęsk żywiołowych w ramach konstytucyjnie uregulowanej ochrony cywilnej i środków wspieranych przez siły zbrojne. W przyszłości jednak mogą się pojawić nadzwyczajne zagrożenia, które będą wymagały kompleksowego działania wyspecjalizowanych sił i środków na szczeblu państwowym i międzynarodowym. Konflikty hybrydowe, terroryzm systemowy lub sabotaż infrastruktury krytycznej mogą być tak nagłymi kryzysami, że obecnie nie ma odpowiednich struktur do zarządzania nimi.

Przedstawione rozważania pozwalają na sformułowanie następujących wniosków końcowych dla polskiej polityki bezpieczeństwa i obrony:

1. Polska jest objęta ryzykiem zagrożeń hybrydowych i dlatego nie jest już tak bezpieczna, jak miało to miejsce w ostatnich dziesięcioleciach.
2. Strategia bezpieczeństwa RP, strategie sektorowe, dyrektywa polityczno-strategiczna oraz pozostałe dokumenty normatywne dotyczące obronności RP muszą być poddane dogłębnej analizie i ocenie, a następnie dostosowane do zmienionej sytuacji w środowisku bezpieczeństwa międzynarodowego i narodowego.
3. Polska polityka obronna powinna zostać dostosowana do konfliktu hybrydowego i udziału w rozwoju Wspólnej Polityki Bezpieczeństwa i Obrony UE.
4. Istotne jest odnowienie intelektualnej obrony kraju. W przeszłości ważne było, by ludzie „motywowali się defensywnie", dlatego dziś ważne jest, aby najpierw edukować i komunikować ryzyko w wiarygodny sposób.
5. Zdarzenia, które uzasadniają obronę, muszą zostać odpowiednio zinterpretowane. Nie jest już kluczowe, czy ma miejsce atak zewnętrzny czy wewnętrzny, ale czy zagrożeniem można zająć się wyłącznie środkami wojskowymi.

Bibliografia

Brockmann K., Giegerich B., Mecit H. (2012), *EU Security Foresight 2030. Szenarien als methodischer Ansatz zur Erforschung der sicherheitspolitischen Rolle der Europäischen Union 2030*, Stiftung neue Verantwortung e.V., Beisheim Center, Berlin.

Europäische Kommission (2017a), *Weissbuch zur Zukunft Europas*, Die EU der 27 im Jahr 2025 – Überlegungen und Szenarien, Europäische Kommission COM (2017) 2025, 1. März 2017.

Europäische Kommission (2017b), *Gemeinsamer Bericht an das europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionem, Bericht über die Umsetzung der überprüften Europäischen Nachbarschaftspolitik,* Brüssel, den 18.5.2017 JOIN(2017) 18 final.

Gaub F. (2019), *Global Trends to 2030: Challenges and choices for Europe***,** an Inter-Institutional EU Project, April.

Krumbein F. (2019), *China im Wettstreit mit den USA um globalen Einfluss*, Stiftung Wissenschaft und Politik Deutsches Institut für Internationale Politik und Sicherheit - SWP- Aktuell 27 April.

Nuspliger N. (2018a), *NZZ Global Risk: Das Weltgeschehen in Szenarien,* NZZ-Korrespondent in Brüssel, Februar.

Nuspliger N. (2018b), *NZZ Global Risk: Zukunft der EU: Eine neue Spaltung zwischen Ost und West?,* NZZ-Korrespondent in Brüssel, Februar.

Panek B., Stawicki R. (red. nauk.) (2018), *Świat wobec wyzwań i zagrożeń w drugiej dekadzie XXI wieku*, Difin, Warszawa.

Sicherheitspolitische Jahresvorschau 2019, *Sicher. Und Morgen?*, Bundesminister für Landesverteidigung, Wien 2018.

Strzoda J., Skrzypiec M. (2007), *Czy jesteśmy przygotowani na blackout?*, Koncern – luty.

Ziegler J. (2003), *Die neuen Herrscher der Welt und ihre globalen Widersacher*, C. Bertelsmann Verlag, München.

Jan Zych
jan.zych@cyberman.com.pl
Uniwersytet Jana Kochanowskiego w Kielcach,
Wydział Nauk Społecznych

W czym przejawia się rozumienie procesu zarządzania bezpieczeństwem w środowisku sieciowym?

Istotą myślenia twórczego w nauce
jest formułowanie nowych płodnych pytań.
Karl Raimund Popper

Wstęp

Problem naukowy zawarto w pytaniu otwartym o charakterze proceduralnym, które brzmi następująco: „W czym przejawia się rozumienie procesu zarządzania bezpieczeństwem w środowisku sieciowym?".

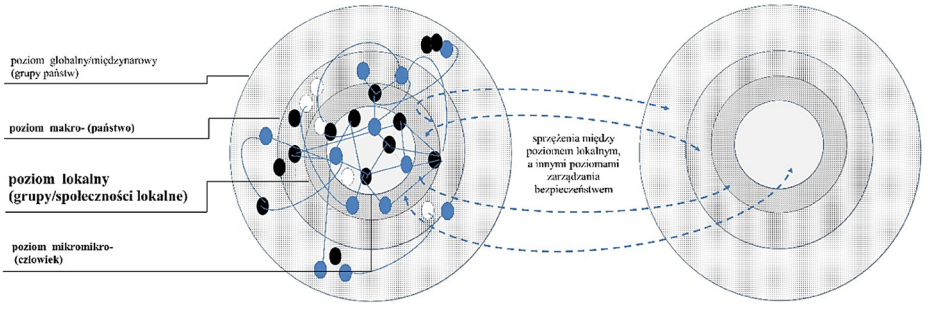
Wiele symptomów wskazuje na to, że trzecia dekada XXI wieku będzie dekadą sieci. Środowisko sieciowe, bez wyraźnie określonego centrum decyzyjnego, ujawnia nowe możliwości oddziaływań na sferę bezpieczeństwa. Struktury o charakterze hierarchicznym, z wyraźnie wydzielonym centrum, zastępowane są nowymi niehierarchicznymi strukturami bez centrum. W środowisku sieciowym wszystkie podmioty mogą wchodzić ze sobą w relacje i mogą się z tych relacji w dowolnym momencie wycofywać [Noga 2014, ss. 122–123].

Sieć to środowisko, dzięki któremu możemy wykreować i utrzymać odpowiedni poziom bezpieczeństwa, w tym lepiej antycypować zagrożenia oraz odpowiednio

sobie z nimi radzić. Żyjemy oplątani wszechobecnymi sieciami: technicznymi (zwanymi technosferą), społecznymi (tzw. antroposferą), biologicznymi (tj. biosferą), które nieustannie oddziałują na siebie. Coraz trudniej jest zaspokoić jakąkolwiek potrzebę człowieka, całkowicie abstrahując od sieci i technologii z nimi związanych. Coraz intensywniej wtapiamy się w środowisko sieciowe.

Społeczeństwo sieciowe znaczy więcej, niż prosta suma składających się nań jednostek. Współpraca w sieci umożliwia nowe formy realizacji wspólnych celów, jak również pozwala na efektywną specjalizację. Nowe zjawiska, charakterystyczne dla środowiska sieciowego, można postrzegać pozytywnie, jako szanse i wyzwania, ale można, a nawet trzeba dostrzegać też zagrożenia, skutkujące zjawiskami negatywnymi dla skutecznego i efektywnego zarządzania bezpieczeństwem [Zych, Stępnicka 2020, s. 7].

Rysunek 1. Sprzężenia między poziomem lokalnym zarządzania bezpieczeństwa w środowisku sieciowym a innym poziomami (wariant)



Źródło: opracowanie własne.

Przedstawiając problematykę zarządzania bezpieczeństwem, przyjęto założenie, że bezpieczeństwo jest procesem [Skrzyp 2005, s. 122], a nie stanem w określonym momencie czasowym. Każdy z elementów tego procesu można przedstawić za pomocą struktury sieciowej, w której zmiana któregokolwiek elementu zazwyczaj implikuje wprowadzenie korekty w kilku, a czasami nawet we wszystkich jego komponentach. Koncentrując się zarządzaniu bezpieczeństwem w środowisku sieciowym, ze szczególnym uwzględnieniem poziomu lokalnego, warto zauważyć, że z poziomu lokalnego poprzez Sieć można oddziaływać na inne poziomy zarządzania bezpieczeństwem (i zazwyczaj tego typu implementacje mają miejsce we współczesnym zarządzaniu) (por. rysunek 1).

Termin „środowisko sieciowe 4.0"

Czwarta rewolucja przemysłowa – z rosnącym znaczeniem Internetu rzeczy, cyfryzacją, automatyzacją i robotyzacją, staje się naturalnym środowiskiem funkcjonowania współczesnego człowieka. Fraza „4.0" zyskuje nowe znaczenie, gdy coraz powszechniej wykorzystywane są nowoczesne technologie dla kreowania i utrzymania wysokiego poziomu bezpieczeństwa.

Termin „środowisko sieciowe 4.0" to synonim zbioru nowych technologii, które zapoczątkowały kolejną wielką zmianę w radzeniu sobie z problemami dotyczącymi funkcjonowania w sieci. Frazę „4.0.", symbolizującą kolejny poziom zaawansowania technologicznego, poprzedziły tzw. ery: „1.0" (wiek pary i rewolucja przemysłowa), „2.0" (wynalezienie elektryczności, nowoczesnej chemii i silnika spalinowego) i „3.0" (rewolucja informatyczna). „Środowisko sieciowe 4.0" to również związane z zarządzaniem bezpieczeństwem kompetencje i stan umysłu, nowe formy organizacji zorientowane na analizę dużych zbiorów danych (ang. *Big Data*), ale także myślenie sieciowe (ang. *Network Thinking*), implementacja mechanizmów sztucznej inteligencji (ang. *Artificial Inteligence*), wykorzystanie chmury obliczeniowej (ang. *Cloud Computing*), Internet rzeczy (ang. *Internet of Things*), Wirtualna Rzeczywistość (ang. *Virtual Reality*), Rozszerzona Rzeczywistość (ang. *Augmented Reality*), autonomiczne i półautonomiczne roboty wykorzystywane w zarządzaniu bezpieczeństwem, myślenie korelacyjne, medycyna genetyczna, bionika i fizyka kwantowa, technologie podwójnego przeznaczenia. To wreszcie utrzymanie w ryzach zagrożeń, opisywanych w literaturze przedmiotu z przedrostkiem „cyber-" [Zych, Stępnicka 2020, s. 8].

Problem ze rozumieniem środowiska sieciowego, w którym i poprzez które jest realizowane zarządzanie bezpieczeństwem, to duże wyzwanie dla menedżerów bezpieczeństwa. W narracjach naukowych tego typu procesy określa się mianem „otwartych", dziejących się „w trybie continuum". To, że nie są to procesy „zamknięte" czy historyczne, sprawia, że wiedza o nich jest nieugruntowana, a względnie „świeży" dorobek naukowy w tej materii podlega permanentnej weryfikacji. Może to powodować niepożądane efekty, np. upublicznianie sprzecznych narracji, wyrażanych hermetycznym stylem i językiem z zawiłą retoryką [Zych, Stępnicka 2020, s. 9].

Trzeba też zauważyć, że monodyskursywność dotyczy zazwyczaj faktów, które nie budzą sporów i nie są wartościowane. Proces zarządzania bezpieczeństwem w Sieci i z Sieci nie podlega tej regule. Z tego też powodu narracje naukowe dotyczące zarządzania bezpieczeństwa są wielodyskursywne, w różnych warian-

tach określane przedrostkami: trans-, pluri- multi-, inter-, syn- i poli- [Zych 2018, ss. 183–199; Zych 2019b, s. 20; Zych 2019a, s. 19].

W sensie ontologicznym, w środowisku sieciowym, w którym żyjemy, rośnie liczba oraz intensywność różnorakich współzależności. W cybernetyce [Mazur 1996] tego typu wzajemne relacje rozpatruje się poprzez modele sieciowe. We współczesnych modelach sieciowych każdy z tych bytów reprezentowanych w Sieci ma określony cel do realizacji: zazwyczaj wyrażony wieloparametrycznym wektorem, zamiast skalarem. To istotne utrudnienie w analizach badających zarządzanie bezpieczeństwem. Zatem w środowisku sieciowym należy dostrzegać zarówno wyzwania i szanse, ale należy też mieć na względzie zagrożenia i niebezpieczeństwa, jakie to środowisko generuje.

Autor rozdziału reprezentuje stanowisko, że Sieć i bezpieczeństwo są ze sobą wzajemnie sprzężone poprzez sieć wzajemnych relacji, a ich separowanie prowadziłoby do zafałszowanego obrazu rzeczywistości. Środowisko sieciowe, szczególnie jego cyfrowe egzemplifikacje, zwielokrotniają i intensyfikują te relacje.

Żyjemy oplątani różnego rodzaju sieciami: materialnymi (np.: Internet, sieć telekomunikacyjna, media) i niematerialnymi (np. relacje międzyludzkie, sieci społecznościowe). Jeśli zatem chcemy zrozumieć etymologię współczesnych zagrożeń, powinniśmy znaleźć odpowiedzi na ważne pytania:

- „Jaki wpływ na zarządzanie bezpieczeństwem ma Sieć?",
- „Jaki aparat pojęciowy zaproponować, który mógłby być efektywnie wykorzystany w środowisku sieciowym?",
- „W jaki sposób identyfikować sytuacje niepożądane mające źródło w Sieci, a objawiające się w sferze bezpieczeństwa?",
- „Jak identyfikować, eliminować, ograniczać i/lub łagodzić skutki kryzysów w środowisku sieciowym lub/i za pośrednictwem tego środowiska?",
- „Jakie działania podjąć, a z jakich zrezygnować w sytuacjach związanych z deficytem lub nadmiarem informacyjnym?".

Udzielenie satysfakcjonujących odpowiedzi na powyższe pytania wymaga wcześniejszego rozumienia, czym są i jak działają sieci.

Główna oś narracji

Główna oś narracji wyraża się w stwierdzeniach, że cyfryzacja i środowisko sieciowe to charakterystyczne cechy kończącej się drugiej dekady XXI wieku, w którym

realizowane są żywotne interesy człowieka, grup społecznych, społeczności lokalnych i państwa. Zmieniają one w sposób istotny metody i techniki zarządzania bezpieczeństwem. Jednym z głównych determinantów, mających wpływ na kreowanie i utrzymanie współczesnego bezpieczeństwa, jest Sieć.

Wątki uzupełniające główną oś narracji to:

1. Problemy dotyczące zarządzania bezpieczeństwa można klasyfikować według różnych kryteriów, ale największą wartość dodaną, zarówno dla teorii, jak i praktyki wnoszą te, które do tej pory nie zostały opracowane. Względnie nowym obszarem dociekań jest środowisko sieciowe.

2. Zarządzanie bezpieczeństwem może być realizowane na różnych poziomach: indywidualnym, grupowym, lokalnym, narodowym, międzynarodowym i globalnym. Na każdym z tych poziomów warunkiem koniecznym racjonalnego zarządzania bezpieczeństwem jest uwzględnianie środowiska sieciowego.

3. Względnie nowym środowiskiem, w którym aktualnie występują mało znane zjawiska, ewidentnie mające wpływ na zarządzanie bezpieczeństwem, jest sieć w różnych postaciach: PAN (ang. *Personal Area Network*), LAN (ang. *Local Area Network*), MAN (ang. *Metropolitan Area Network*), WAN (ang. *Wide Area Network*), WLAN (ang. *Wireless Local Area Network*) oraz Internet.

Współczesne (koniec drugiej dekady XXI wieku) pojmowanie sieci intuicyjnie kojarzone jest z siecią komputerową. Przyjmuje się, że sieć komputerowa to zbiór komputerów i innych urządzeń połączonych ze sobą kanałami komunikacyjnymi oraz oprogramowanie wykorzystywane w tej sieci. Umożliwia ona wzajemne przekazywanie informacji oraz udostępnianie zasobów własnych między podłączonymi do niej urządzeniami, zwanymi punktami sieci. Matematyczną notację opisywania sieci zawdzięczamy żyjącemu w XVIII wieku w Królewcu Leonardowi Eulerowi (1707–1783), który opisywał sieci językiem grafów. Problematyką grafów i sieci zajmuje się w szczególności jeden z działów matematyki dyskretnej (teoria grafów i sieci). Ze względu na dużą użyteczność mechanizmów, którymi posługuje się ten dział matematyki, znajdują one zastosowanie w rozwiązywaniu wielu praktycznych problemów, np.:

- harmonogramowanie i szeregowanie zadań;
- routing i analiza sieci semantycznych;
- analiza sieci typu: PERT (ang. *Program Evaluation and Review Technique*) i GERT (ang. *Graphical Evaluation and Review Technique*);
- rozpoznawanie wzorców strukturalnych i anomalii;
- analiza procesów w sieciach rozległych i heterogenicznych typu Internet czy sieci społeczne [Zych, Stępnicka 2020, ss. 71–72].

Grafy są reprezentacją punktów – węzłów, połączonych łukami (krawędziami). Sieć reprezentowana językiem grafów definiowana jest poprzez przypisanie węzłom i łukom atrybutów (cech). Innymi słowy, sieć to graf, czyli zbiór węzłów i łączących je łuków, dla którego zostały określone funkcje na zbiorze węzłów i łuków (np. funkcja kosztów transmisji, niezawodność, poziom ryzyka). Zatem graf odwzorowuje realną sieć, rozumianą jako zbiór węzłów i zbiór relacji między węzłami. Sieć można też nazwać systemem, z różnego rodzaju relacjami sieciowymi [Pawłowski 2009, s. 89].

Innymi słowy, graf to nie to samo, co sieć. Sieć definiuje się jako graf opisany ilościowo (tzw. graf ważony), tzn. taki, w którym na wierzchołkach i/lub na krawędziach/ łukach opisano funkcje, które mają interpretację zależną od rodzaju bytu (obiektu) odwzorowywanego przez sieć (np. sieć drogowa, na której pracują służby ratownicze, opisana jest konkretnymi wartościami: czasem przejazdu po odcinku x przez krawędź/ łuk, długość tego odcinka). Z formalnego punktu widzenia traktowanie pojęć „graf" i „sieć", jako synonimów jest niedopuszczalne. Graf opisuje wyłącznie strukturę odwzorowywanego bytu (wycinka systemu rzeczywistego), a sieć, oprócz struktury, zawiera w sobie charakterystyki ilościowe tego rozpatrywanego bytu.

Współczesne cyfrowe środowisko sieciowe 4.0 cechuje permanentna zmiana, ponieważ bez przerwy zachodzą w nim liczne, nowe zdarzenia, w tym pojawiają się nowe informacje. Informacje te mogą pochodzić z wielu różnorodnych źródeł, z różnych domen. W sieci każda informacja może służyć do wypracowania optymalnej decyzji (w sensie przyjętego kryterium rozwiązania, np.: względem kryterium kosztowego). Informacje są dynamicznie przetwarzane przez wszystkie podmioty koegzystujące ze sobą w sieci i współtworzące w danym momencie czasowym sieć zależności.

Nakreślone przez autora rozdziału punkty odniesienia (cyfryzacja oraz usieciowienie procesów dotyczących zarzadzania bezpieczeństwem) w dobie Internetu i globalizacji, przebijają się do głównych narracji w naukach o bezpieczeństwie i coraz bardziej zyskują na znaczeniu. Nowe środowisko sieciowe odgrywa coraz większą rolę w postrzeganiu problematyki bezpieczeństwa. Sieć stała się nowym środowiskiem kreowania tegoż bezpieczeństwa.

W środowisku sieciowym, jak to opisał Jacek Bartosiak, realizacja własnych celów strategicznych w kwestii bezpieczeństwa oznacza „(…) poszerzanie strefy własnych wpływów w innych państwach, nawiązywanie kontaktów biznesowych i/lub posiadanie dostępu do rynków zbytu. Środowisko sieciowe wymaga odnajdywania się relacyjnym świecie, w sieci powiązań, wpływów, lobbystów, agentów,

partnerów, informatorów, przedstawicieli handlowych, egzekutorów praw i nadzorców interesów, którzy zawsze gdzieś w przestrzeni są zlokalizowani, najczęściej w punktach węzłowych sieci" [Bartosiak 2018, s. 27].

Wymagany jest układ monitorujący kluczowe węzły (ang. *hub*) w sieci, w szczególności, gdy przekraczana jest ludzka i instytucjonalna odporność tych systemów i gdy potrzebna jest adekwatna reakcja układu korekcyjnego, działającego na zasadzie układu sprzężenia zwrotnego, który bez zbędnej zwłoki (w czasie rzeczywistym) dostraja system do zmieniających się warunków zewnętrznych. Od analityków/ menedżerów bezpieczeństwa wymaga się antycypowania, z odpowiednim wyprzedzeniem czasowym, stanów przyszłych, aby się do nich odpowiednio przygotować. Stany te mogą mieć walencję pozytywną (należy wykorzystać szanse) lub walencję negatywną (należy przeciwdziałać zagrożeniom) [Zych, Stępnicka 2020, ss. 74–75].

Warto mieć świadomość, że nowe środowisko sieciowe niesie ze sobą nowe podatności, nowe możliwości prowadzenia działań destrukcyjnych, którym nie umiemy się jeszcze w pełni przeciwstawić. Stanowi to wciąż wyzwanie dla naukowców zgłębiających zagadnienia optymalizujące zarządzanie bezpieczeństwem.

Otaczający nas świat jest pełen różnorodnych sieci, których jesteśmy kreatorami, użytkownikami, a także aktorami. W sieciach tych wytworzyły się swoiste prawa/ reguły/ zasady koegzystencji. Jako naukowcy zajmujący się problematyką bezpieczeństwa jesteśmy zobowiązani, aby dogłębnie poznać te prawa/ reguły/ zasady, aby być świadomym podmiotem działania w tym środowisku sieciowym.

Środowisko sieciowe 4.0 jest definiowane jako zbiór lub grupa powiązanych ze sobą elementów – rzeczy bądź ludzi. Świat sieci to złożony system sieci fizycznych, np.: telekomunikacyjnych, transportowych, energetycznych oraz sieci niefizycznych – sieci społecznych, np.: organizacje proobronne, proekologiczne.

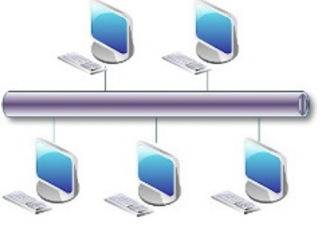
Problemy społeczeństwa sieciowego opisał w znanej na polskim rynku wydawniczym książce Manuel Castells [Castells 2010], pt. *Społeczeństwo sieci*, w której wyjaśnia, jak nowe technologie, przede wszystkim te wspomagające powstawanie nowych technik komunikacji i zapewniających lepszą niż dotychczas wymianę informacji, redukują, a nawet usuwają relacje związane z hierarchią bytów i procesów. Według M. Castellsa współczesna multimedialna kultura wzmacnia pragnienie każdego podmiotu bycia w sieci. Wieloparametryczne porównanie, którego dokonał M. Castells, polegało na zestawieniu społeczeństwa i Sieci, które to byty były dla M. Castellsa formami organizacji. To umaszynowienie, w szczególności cyfryzacja, jaką muszą zaakceptować: człowiek, grupy społeczne, społeczności

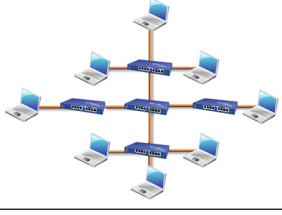
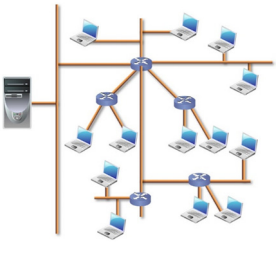
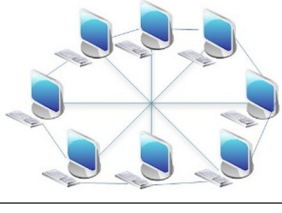
lokalne i państwa, to warunek konieczny implementacji nowoczesnej ideologii, łączącej marzenia o demokratycznej emancypacji oświecenia, z racjonalizmem. Dla Castellsa przyszłość jawi się jako Sieć, w której będzie się realizowało rozwinięte społeczeństwo informacyjne [Castells 2010].

Manuelowi Castellsowi zawdzięczamy też upowszechnienie określenia „netyzm", co oznacza postawę metodologiczną zogniskowaną na badanie bytów, mechanizmów, zależności, koincydencji, korelacji czy związków przyczynowo-skutkowych w środowisku sieciowym. W Sieci występują powszechnie zjawiska, inne niż w środowisku pozasieciowym, np.: bezskalowość, fraktale, nieliniowa dynamika, chaos czy społeczeństwo ryzyka i bifurkacje [Zych, Stępnicka 2020, s. 77].

Różne atrybuty Sieci, właściwie lub niewłaściwie wykorzystywane, stwarzają lub nie szanse lub zagrożenia dla bezpieczeństwa. Sieć może przyjmować różne fizyczne struktury topologiczne (tabela 1).

Tabela 1. Przykłady fizycznych struktur topologicznych sieci

Nazwa struktury topologicznej sieci w języku polskim	Nazwa struktury topologicznej sieci w języku angielskim	Wizualizacja topologii
topologia magistrali, topologia szyny	bus	
topologia liniowa	linear bus topology	
topologia pierścienia	ring topology	

Nazwa struktury topologicznej sieci w języku polskim	Nazwa struktury topologicznej sieci w języku angielskim	Wizualizacja topologii
topologia podwójnego pierścienia	dual ring topology	
topologia gwiazdy	star topology	
topologia gwiazdy rozszerzonej	extended star topology	
topologia hierarchiczna	hierarchical topology, tree topology, star-bus topology	
topologia siatki	mesh topology	

Źródło: opracowanie własne na podstawie: *Vademecum Teleinformatyka cz. III…* 2004.

Niezależnie od topologii fizycznej, środowisko sieciowe stanowi specyficzną rodzinę podzbiorów otwartych, wyróżnionych w obrębie zbioru, spełniających określone aksjomaty:

1. tworzone są w nim temporalne relacje między bytami wcześniej ze sobą niepowiązanymi;
2. po każdej transakcji relacja między bytami może ulegać modyfikacji (przyłączenie nowego bytu lub zerwanie połączenia);
3. między bytami w sieci nie występuje relacja nadrzędności/ podległości;
4. niezależnie od miejsca w sieci, każdy byt w sieci może nawiązać/ zerwać relację z każdym innym bytem tego środowiska, nawet jeśli przynależy do innego podzbioru;
5. każdy byt w sieci może jednocześnie funkcjonować w różnych subsieciach, realizując różne cele;
6. technologie wspomagają i zwiększają efektywność działań w środowisku sieciowym, poprzez:
   a) szybkość przekazywania danych oraz informacji;
   b) wymianę informacji w czasie rzeczywistym;
   c) możliwość zarządzania dużymi woluminami danych;
   d) działanie 24h/dobę;
7. do sieci można się podłączyć (odłączyć) w dowolnym momencie czasowym [Zych, Stępnicka 2020, ss. 79–80].

Współczesne społeczeństwo można porównać do ewoluującego dynamicznego systemu o złożonej strukturze, którego podsystemy są permanentnie ewoluującymi, względnie autonomicznymi sieciami. Uogólniając, każdą strukturę społeczną umownie można podzielić na mniejsze struktury. W ramach każdej mniejszej struktury łatwiej jest zidentyfikować specyficzną klasę problemów, np. problemy dotyczące zarządzania bezpieczeństwem. Jerzy Wolanin [Wolanin 2005, ss. 361–362] według kryterium podmiotowego wyszczególnia problemy dotyczące:

1. bezpieczeństwa indywidualnego;
2. bezpieczeństwa grup społecznych oraz społeczności lokalnych;
3. bezpieczeństwa państwa.

Podział taki jest umowny i łatwo go rozszerzyć do większej liczby klas, np. rozbijając na dwa podzbiory problemy dotyczące bezpieczeństwa grup społecznych i społeczności lokalnych oraz tworząc nową kategorię – bezpieczeństwo międzynarodowe.

Każde z wymienionych subśrodowisk funkcjonuje w Internecie, który jest siecią globalną, tworzoną przez wzajemnie sprzężone sieci lokalne. Internet ma strukturę hierarchiczną, tj. na każdym poziomie funkcjonuje określona liczba sprzężonych sieci lokalnych. Internet stanowi syntezę sieci funkcjonujących na poszczególnych poziomach. Synteza nie oznacza prostej agregacji sieci lokalnych, lecz powoduje

ustanowienie relacji poziomych, w ramach subśrodowisk tego samego poziomu, jak i pionowych pomiędzy poziomami. Można wyróżnić ważne aspekty działania Internetu, które konstytuują swoiste struktury sieciowe. Są to:

- sieć połączeń komunikacyjnych, odzwierciedlająca gęstość struktury społecznej;
- sieć informacyjna, pozwalająca zidentyfikować punkty węzłowe w strukturze społecznej;
- sieć techniczna, konstytuująca warunki brzegowe, w jakich funkcjonuje dana struktura społeczna [Zych, Stępnicka 2020, ss. 81–82].

Podsumowanie

Podjęta przez autora tematyka wyjaśniania procesów charakteryzujących współczesne środowisko sieciowe 4.0 i ich adaptacji do zarządzania bezpieczeństwem może aspirować do tzw. nowego nurtu zgłębiania problematyki bezpieczeństwa, wypracowującego nową, poszerzoną siatkę pojęciową dla lepszego niż dotychczas zarzadzania bezpieczeństwem. Dla przykładu, może to być koncentracja na zarządzaniu bezpieczeństwem na poziomie lokalnym. Za każdym razem chodzi jednak o wypracowanie i zaakceptowanie nowych warunków brzegowych w kwestii zarządzania bezpieczeństwem. Być może trzeba się pogodzić z tezą, że nie pojawi się jedna, niebanalna teoria w naukach o bezpieczeństwie spajająca wiele narracji, a jeśli się pojawi, będzie na tak wysokim poziomie abstrakcji, że nie da się jej zoperacjonalizować dla zarządzania bezpieczeństwem, pod tym względem będzie bezużyteczna.

Dzięki Sieci rozwiązujemy problemy dotyczące bezpieczeństwa, ale Sieć generuje nowe zagrożenia, np. cyberataki, wirusy, „konie trojańskie", spam, hejt, bomby logiczne, inwigilacje, kradzieże tożsamości, „cyberwojny". Istnieje pewnie szczególny aspekt myślenia o zarządzaniu bezpieczeństwem, a mianowicie wiążący się z bezpieczeństwem jego cyberprzestrzeni i dotyczący swoistości zmieniającej się socjosfery. Życie społeczne kolejny raz w historii ludzkości wyprzedza zasady i normy polityczne, prawne i obyczajowe. Nietrudno przewidzieć powstanie nowej przestrzeni konfliktów i kryzysów społecznych, zagrożeń, ale również wyjątkowych szans. Tą nową przestrzenią, tym nowym środowiskiem, jest Sieć. Aby efektywnie i skutecznie zarządzać współczesnym bezpieczeństwem, musimy zrozumieć, czym jest środowisko sieciowe oraz jak działają sieci.

Bibliografia

Bartosiak J. (2018), *RP między lądem, a morzem o wojnie i pokoju*, Wydawca ZonaZero, Warszawa.

Castells M. (2010), *Społeczeństwo sieci*, Wydawnictwo Naukowe PWN, Warszawa.

Mazur M. (1996), *Cybernetyka i charakter. Psychologia XXI wieku*, Wydawnictwo Aula, Podkowa Leśna.

Noga A. (2014), *Sieci w ujęciu teorii ekonomii* [w:] *Relacje międzyorganizacyjne w naukach o zarządzaniu*, red. A.K. Koźmiński, D. Latusek-Jurczak, Wolters Kluwer Business, Warszawa.

Pawłowski P. (2009), *Czy jesteśmy scale-free?*, ,,Kosmos", nr 1–2(282–283).

Skrzyp J. (2005), *Geoinformacje w zarządzaniu bezpieczeństwem (cz. 1)*, ,,Zeszyty Naukowe" (numer specjalny), nr 1(58)A, Akademia Obrony Narodowej, Warszawa.

Vademecum Teleinformatyka, cz. III (2004), *Sieci nowej generacji, technologie internetowe, metrologia sieciowa*, Wydawnictwo IGD, Warszawa.

Wolanin J. (2005), *Zarys teorii bezpieczeństwa obywateli: ochrona ludności na czas pokoju*, Wydawnictwo ,,DANMAR", Warszawa.

Zych J. (2018), *Interdyscyplinarność badań w naukach o bezpieczeństwie, postulat czy konieczność* [w:] *Wykorzystanie nowoczesnych narzędzi informatycznych w identyfikacji zagrożeń*, red. Ł. Roman, K. Krassowski, S. Sagan, D. Wróblewski, Wydawnictwo Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi, Józefów.

Zych J. (2019a), *Teleinformatyka dla bezpieczeństwa 2.0*, Fundacja na Rzecz Czystej Energii, Poznań.

Zych J. (2019b), *Wytwarzanie systemów informatycznych dla bezpieczeństwa zdrowotnego – perspektywa cybernetyka*, w trakcie procesu wydawniczego [w:] red. J. Konieczny, L. Dajerlich, Wydawnictwo Uniwersytetu Adama Mickiewicza, Poznań.

Zych J., Stępnicka N. (2020), *Ekonomizacja bezpieczeństwa w środowisku sieciowym 4.0.* (w trakcie procesu wydawniczego), Wydawnictwo Difin, Warszawa.

Agnieszka Białek
bialek.agnieszka803@gmail.com
Uniwersytet Jana Kochanowskiego w Kielcach,
Wydział Prawa, Administracji i Zarządzania

Cyberbezpieczeństwo w prawie polskim – analiza wybranych zagadnień

Wstęp

Poniższy rozdział ma na celu przybliżenie problematyki cyberprzestrzeni przez przedstawienie jej historii aż do obecnego jej kształtu. Analizie poddana zostanie kwestia cyberbezpieczeństwa i związanych z nim cyberzagrożeń, a następnie omówione zostaną regulujące je polskie akty prawne.

Obecnie żyjemy w świecie zdominowanym przez różnego rodzaje innowacje, który przyjęło się nazywać globalną wioską[1]. Dużą rolę w tempie jego rozwoju odgrywa technologia IT (ang. *Information Technology*). Jest to dziedzina wiedzy, obejmująca swoim zasięgiem zagadnienia, środki i działania związane z przetwarzaniem informacji. Początki technologii IT sięgają lat 60. ubiegłego wieku, kiedy wskutek toczonej wówczas zimnej wojny nastąpił postęp techniczny oparty początkowo na militariach. Bliższy nam Internet komercyjny i szeroko pojmowana telekomunikacja rozwinęła się natomiast w latach 90. XX wieku. Wzrost

[1] Za Wikipedią – termin wprowadzony przez Herberta Marshalla McLuhana, opisujący trend, w którym masowe media elektroniczne obalają bariery czasowe i przestrzenne, umożliwiając komunikację na skalę masową.

popularności technologii łączy się z uzależnieniem od ich obecności większości sfer naszego życia. Użytkownicy uzyskali dostęp nie tylko do stron WWW (ang. *Word Wide Web*), ale również do wszelkiego rodzaju urządzeń umożliwiających komunikację w czasie rzeczywistym, nagrywanie i odtwarzanie obrazu, ale także sterowanie różnorodnymi procesami na odległość [Karatysz 2013, s. 140]. Połączenie tych innowacji uformowało zorganizowaną infrastrukturę. W konsekwencji utworzyła się różnorako definiowana cyberprzestrzeń, umożliwiająca ewolucję przestępczości. Należy zatem zadać pytanie, czy regulacje prawne w obrębie cyberprzestrzeni i system cyberbezpieczeństwa w Polsce rozwijają się w sposób dostateczny, aby stanowić ochronę przed przyszłymi, związanymi z tą przestrzenią, zagrożeniami?

Cyberprzestrzeń

Odpowiedź ma powyższe pytanie będzie możliwa dopiero po zapoznaniu się z kilkoma, dość nowymi w świecie, zagadnieniami. Termin „cyberprzestrzeń" został użyty po raz pierwszy w 1982 r. przez Williama Gibsona w powieści science fiction[2]. Jest on również pierwszym autorem definicji tego zjawiska[3], wskazującej na jego najistotniejsze cechy – i to jeszcze przed jego całkowitym zaistnieniem [Wasilewski 2013, s. 226]. Są to: ogólnoświatowy zasięg, gromadzenie danych w jednej, obszernej bazie, brak możliwości porównania cyberprzestrzeni z realnymi, (np. geograficznymi) wymiarami, pomimo że jest ona nazywana kolejną przestrzenią. Pojęcie cyberprzestrzeni, mimo używania od niemalże 40 lat, podlega ciągłej modyfikacji. Następstwem tego jest tworzenie wielu, różniących się zakresem definicji. Na przykład Ronald J. Deibert[4] definiował cyberprzestrzeń jako „nieuniknioną rzeczywistość, która owija naszą planetę złożoną skórą informacji i komunikacji. Kształtuje nasze działania i wybory, nieubłagalnie zbliżając nas do siebie. [...] Współdzielona przestrzeń, globalna gmina, rozrośnięty plac publiczny" [Lakomy 2015, s. 71]. Jednakże poza definicjami wywodzącymi się z literatury science fiction napotykamy na wiele definicji legalnych, gdyż wzrost liczby użytkowników niejednokrotnie skutkuje konfliktami na tle światopoglądowym czy gospodarczym i służy rozwojowi przestępczości, a nawet terroryzmu.

[2] Opublikowana została w magazynie *Omni*.

[3] Cyberprzestrzeń została definiowana w powieści *Neuromancer* wydanej w 1984 roku.

[4] Fragment wstępu do książki *Black Code: Inside the Battle for Cyberspace* wydanej w 2011 roku.

Badania statystyczne z 2018 r. [WeAreSocial UK] wskazują, że:

- liczba internautów wynosiła 4 021 mld, co oznacza wzrost o 7% rok do roku,
- liczba użytkowników mediów społecznościowych wynosiła 3 196, co oznacza wzrost o 13% rok do roku,
- liczba użytkowników telefonów komórkowych wynosiła 5 135 mld, co oznacza wzrost o 4% rok do roku,
- przeciętny użytkownik spędza 6 godzin przy użyciu urządzeń i usług internetowych, czyli około 1/3 życia.

Tematyka cyberprzestrzeni kształtuje się inaczej na obszarze Stanów Zjednoczonych, Unii Europejskiej oraz Polski.

Uzupełnianie się definicji i definicji legalnych

W Stanach Zjednoczonych funkcjonują dwie rożne charakterystyki cyberprzestrzeni – węższa i szersza. Pierwsza [DOD Dictionary…] z nich jest definicją stworzoną na potrzeby wojskowe. Nie uwzględniono więc w niej środowiska użytkowników, a jedynie wyróżniono elementy technologiczne, wśród których prym wiedzie Internet. Druga definicja [National Strategy…] opracowana została dla strategii bezpieczeństwa. Zawarto w niej wielość i różnorodność elementów oraz powiązania z krajową infrastrukturą krytyczną [Wasilewski 2013, s. 228].

Na Starym Kontynencie podstawowe znaczenie ma regulacja prawna wprowadzona przez Komisję Europejską, według której cyberprzestrzeń to „wirtualna przestrzeń, w której krążą elektroniczne dane przetwarzane przez komputery PC z całego świata”[5] [Słownik Komisji Europejskiej]. Wąskie pojęcie Internetu zastąpiono tu wirtualną przestrzenią, a nazwa ta obejmuje zarówno wszelkie pliki i dane, jak również aplikacje i procesy.

Dokument wydany w Wielkiej Brytanii [The UK Cyber…] podkreśla, że cyberprzestrzeń jest złożoną infrastrukturą informatyczną, zawierającą w sobie nie tylko Internet, ale i telekomunikację sieci, systemy komputerowe, podłączone do Internetu urządzenia i osadzone procesory i kontrolery.

W Polsce zagadnienie cyberprzestrzeni uregulowane zostało w ustawie, nie w dokumencie rządowym, jak w przypadku wyżej wymienionych krajów. Akt prawny z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego

[5] W oryginale: *Virtual space in which the electronic data of worldwide PCs circulate*.

Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej [Dz. U. z 2018 r., poz. 1932] wskazuje jako cyberprzestrzeń „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne", natomiast systemem teleinformatycznym w rozumieniu Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne [Dz. U. z 2019 r., poz. 700] nazywa się „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego".

Ustawodawstwo polskie, w odróżnieniu od państw zachodnich, umiejscawia cyberprzestrzeń jako wyodrębniony obszar, oddziałujący na rzeczywistość [Wasilewski 2013, s. 231]. Nie ogranicza jego funkcji jedynie do wymiany informacji, ale wskazuje także na udział tej przestrzeni w ich wytwarzaniu, modyfikacji oraz najprostszym odtwarzaniu.

Analizując wszystkie wymienione wyżej definicje, można zauważyć, że przeważnie się one uzupełniają. Aby zatem zrozumieć istotę cyberprzestrzeni, należy uwzględniać każdą z nich, stosownie do okoliczności.

Cyberbezpieczeństwo

Wraz ze wzrostem liczby użytkowników oraz obszarów zależnych od technologii IT, wzrosła liczba zagrożeń powiązanych z cyberprzestrzenią. Wymusiło to rozpoczęcie prac nad nową sferą zabezpieczeń dla państw – bez wprowadzania odpowiednich regulacji prawnych oraz taktyki działań, odparcie jakiegokolwiek ataku jest wyzwaniem [Górny, Krawiec 2016, s. 2]. Konsekwencją tego było powstanie nowej dziedziny – cyberbezpieczeństwa (ang. *Cybersecurity*). Najprościej rzecz ujmując, jest to zespół czynności i procedur związanych z zapewnieniem ochrony w cyberprzestrzeni. System ten jest również powiązany z ochroną fizyczną i gwarancją bezpieczeństwa osobistego poprzez realizację podstawowych atrybutów informacji: poufności, dostępności i integralności. W Polsce jego legalną definicję zawiera Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa [Dz. U. z 2018 r., poz. 1560]. W art. 2. wspomnianej ustawy, cyberbezpieczeństwo to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy".

Opracowanie koncepcji szybkiego i skutecznego reagowania jest odpowiedzią na różnorodność i dynamikę rozwoju zagrożeń cyberprzestrzeni. Środowisko IT niesie ze sobą wiele niebezpieczeństw, dlatego konieczne są dotyczące go regulacje ustawowe. Warto przybliżyć parę kwestii występujących w tym obszarze zagrożeń.

Po pierwsze zagrożenia wynikają z charakterystycznych dla cyberprzestrzeni zagadnień technicznych. Jednym z nich są tak zwane ciasteczka (pliki cookie) umieszczane na stronach WWW, śledzące czynności użytkownika na witrynie internetowej. Warto również zwrócić uwagę na aplikacje, które w celu prawidłowego działania żądają od użytkowników dostępu do ich lokalizacji oraz na występujące powszechnie algorytmy, zbierające różnorakie informacje w celach konsumenckich. Po drugie każda sfera powiązana z działalnością IT niesie za sobą niebezpieczeństwo związane z wymienionymi powyżej rozwiązaniami. Dane, często także te wrażliwe, mogą dostać się w niepowołane ręce[Lakomy 2015, ss. 91–92]. Ryzyko to związane jest z tym, że z systemów teleinformatycznych korzysta wiele różnorodnych podmiotów – od typowych, niestanowiących zagrożenia użytkowników, przez organizacje międzynarodowe czy państwa, aż po hakerów i grupy przestępcze.

Negatywne w skutkach działania mogą mieć różnorakie oblicza, wśród których wyróżniamy parę podstawowych grup [Wrona 2017, s. 57]. Do pierwszej z nich zaliczamy poczynania, których skutek jest niematerialny i brak jest informacyjnych korzyści. Są to sabotaż (dezintegracja, czynniki destrukcyjne) i zagrożenia nieumyślne (awaria zasilania energetycznego). Grupę drugą cechuje aktywność w przestrzeni wirtualnej osób nieuprawnionych do pozyskiwania określonych treści. Posługują się one zróżnicowanymi środkami, aby wniknąć do systemów informatycznych, a ich celem jest osiągnięcie korzyści majątkowych lub niemajątkowych ze zdobytych informacji.

Cyberprzestępstwa

Ostatecznie dochodzimy do potrzeby unormowania zagadnienia cyberprzestępstw. Przed zdefiniowaniem cyberprzestrzeni posiłkowano się określeniami takimi, jak: „przestępstwa z użyciem komputera", „przestępstwa związane z wykorzystaniem komputera" lub „przestępstwa komputerowe". Jednakże stworzenie kompletnej definicji legalnej przy ciągłym rozwoju i zmianach w tej materii wymagało dużej elastyczności. Pierwotnie pojmowano te czyny dwojako. Po pierwsze konieczne było,

aby narzędziem przestępstwa był komputer, a szkoda musiała powstać w prawnie chronionych dobrach lub interesach. Po drugie konieczną przesłanką było posiadanie przez sprawcę specjalnej wiedzy z zakresu IT. Aktualnie w użyciu jest definicja łącząca niejako dwie powyższe. Zgodnie z nią przestępstwem komputerowym są „wszelkie zachowania przestępne związane z funkcjonowaniem elektronicznego przetwarzania danych, polegające zarówno na naruszeniu uprawnień do programu komputerowego, jak i godzące bezpośrednio w przetwarzaną informację, jej nośnik i obieg w komputerze oraz cały system połączeń komputerowych, a także w sam komputer".

Bazując na powyższej definicji przestępstw komputerowych, można wskazać definicje cyberprzestępstw, na których prawną regulację największy wpływ miały działania Rady Europy, Organizacji Narodów Zjednoczonych (ONZ) czy też Organizacji Współpracy Gospodarczej i Rozwoju (OECD). Podczas jednego z kongresów[6] wskazano wąskie i szerokie określanie tej materii. W wąskim rozumieniu jest to przestępstwo komputerowe, z tym że charakterystyczne jest posługiwanie się operacjami elektronicznymi oraz cel, czyli systemy oraz dane komputerowe. W szerszym spojrzeniu posługiwanie się działaniami IT nie jest bezwzględną przesłanką, aby dana czynność została zakwalifikowana jako cyberprzestępstwo. Mogą być to czyny popełnione przy użyciu technologii, jak i te przeciwko niej skierowane.

Zgłębiając powyższe próby skategoryzowania tego rodzaju przestępstw, dostrzec można, że najistotniejszy w tej nielegalnej działalności jest obszar jej występowania, a mianowicie cyberprzestrzeń. Następnie w definicjach skupiono się na środkach używanych w celu dokonania szkód lub uzyskania korzyści. Dopiero na końcu wskazuje się przedmiot ochrony, podkreślając, że urządzenia mogą być nie tylko narzędziem, ale również celem [Karatysz 2013, s. 140].

Aby uwidocznić powagę opisanych powyżej zjawisk, posłużę się przykładem. Do pierwszego znaczącego cyberataku doszło w 2007 r. w Estonii [Nowak 2013, s. 10]. Działania hackerów trwały od 27 kwietnia do 18 maja, a ich skutkiem było m.in. zablokowanie stron WWW należących do rządu i istotniejszych gazet. Spowodowało to chaos informacyjny w całym kraju. Należy podkreślić, że już w 2007 roku Estonia była nazywana E-stonią ze względu na stopień rozwoju infrastruktury informatycznej. Kolejną uciążliwością dla mieszkańców było sparaliżowanie systemów bankowych. Na szczęście poczynania te nie miały długotrwałych następstw, jednakże ze względu na ich powagę, wydarzenia te określa się pierwszą wojną internetową.

[6] X Kongres ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców.

Normy prawne w Polsce

Po zapoznaniu się z ogólnymi informacjami na temat cyberprzestrzeni, oczywistym staje się potrzeba unormowania zagadnień związanych z bezpieczeństwem na tej płaszczyźnie. Ma ona zasięg globalny, tak więc i globalne są regulacje prawne. Wyróżniamy rozwiązania międzynarodowe oraz krajowe.

Niezależnie od tego, czy naruszenie infrastruktury IT następuje globalnie czy lokalnie ma to ogromny wpływ na poczucie bezpieczeństwa obywateli, stabilność gospodarki oraz sprawność funkcjonowania wszelkich instytucji. Dlatego też normy prawa polskiego, regulujące tę materię są rozbudowane oraz mieszczą się w różnych gałęziach prawa. Dla przykładu prawo cywilne normuje kontakty w umowach zawieranych na odległość lub poza lokalem przedsiębiorstwa, w ustawie o prawach konsumenta [Dz. U. z 2014 r., poz. 827]. Kodeks karny [Dz. U. z 2019 r., poz. 1950] zawiera artykuł 287 o oszustwie komputerowym, który przewiduje karę za „wpływ na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmianę, usunięcie albo wprowadzenie nowego zapisu danych informatycznych". Prawo administracyjne reguluje tę kwestię między innymi w Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej [Dz. U. z 2019 r., poz. 162]. Sądy również coraz częściej rozstrzygają w sprawach dotyczących problematyki cyberprzestrzeni. W bazie orzeczeń sądów powszechnych znajdują się tysiące orzeczeń. Z reguły dotyczą one wykonywania zobowiązań wynikających z umów zawieranych z operatorem [I C 1668/16]. Jednakże często spotykane są również czyny z art. 287 Kodeksu karnego [II K 164/17] oraz art. 107 Kodeksu karnego skarbowego [IV Ka 1675/12].

Głównym aktem prawnym w zakresie cyberprzestrzeni jest Ustawa z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa [Dz. U. z 2018 r., poz. 1560], która wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) [Dz. Urz. UE L 194 z 19.07.2016, str. 1]. Aby w pełni zrozumieć zadania realizowane przez ten akt prawny, niezbędne jest przeanalizowanie paru kluczowych zagadnień. Regulacje ustawy mają na celu zapewnić bezpieczeństwo, co szerokim, słownikowym rozumieniu jest „stanem niezagrożenia" [https://sjp.pwn.pl/]. W kontekście tej ustawy skupiamy się jednakże na bezpieczeństwie konkretnych procesów – usług kluczowych i cyfrowych. Jako usługę cyfrową rozumiemy usługę świadczoną drogą elektroniczną. Należy się tu odnieść do Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną [Dz.U.2019.123]. Posługiwanie się drogą elektroniczną oznacza, w rozumieniu tego aktu, przesyłanie i odbieranie danych za pośrednictwem systemów

teleinformatycznych, za pośrednictwem sieci publicznych, na indywidualne żądanie usługobiorcy, istotny jest tu także fakt braku jednoczesnej obecności stron. Za kluczową natomiast uważa się usługę, która ma „znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej" [Dz. U. z 2018 r., poz. 1560]. Wielość zinformatyzowanych sektorów oznacza dla państwa konieczność prowadzenia sprawnego zarządu. Dlatego też w Polsce za każdy z tych sektorów odpowiedzialny jest właściwy minister, o czym mówi art. 41 ustawy o krajowym systemie cyberbezpieczeństwa [Dz. U. z 2018 r., poz. 1560].

Jako organ właściwy do spraw cyberbezpieczeństwa, minister ma wiele obowiązków, zajmuje się także strefą operatorów usług kluczowych. Do jego zadań w tej materii należy przede wszystkim bieżąca analiza spełnienia warunków niezbędnych do uznania podmiotu za takiego operatora oraz wydawanie decyzji w tej kwestii. Monitoruje także stosowanie przepisów ustawy przez zakwalifikowane podmioty oraz jest uprawniony do stwierdzenia wygaśnięcia wydanej wcześniej decyzji. Minister sprawuje również pieczę nad danymi zawartymi w wykazie operatorów kluczowych, składa wnioski o wpis, jak i zmianę zawartych tam informacji. Przetwarza informacje, w tym dane osobowe, w takim zakresie, w jakim jest to konieczne do realizacji innych ustawowo określonych zadań. Minister może także, jeżeli uzna to za konieczne, zlecić zadania podległym mu jednostkom oraz tym, które pozostają pod jego nadzorem.

Jak już wspomniano, usługi kluczowe odgrywają ważną rolę w funkcjonowaniu wszelkiego rodzaju sektorów gospodarki, dlatego też właściwy minister współtworzy z jednostkami stworzonymi do reagowania na incydenty bezpieczeństwa komputerowego „rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów" [Dz. U. z 2018 r., poz. 1560, art. 42, punkt 5]. Jednostki te to Zespoły Reagowania na Incydenty Bezpieczeństwa (*Computer Security Incident Response Team* – CSIRT). CSIRT NASK zarządzana jest przez Szefa Agencji Bezpieczeństwa Wewnętrznego, CSIRT GOV – Ministra Obrony Narodowej, a CSIRT MON, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Razem tworzą one Zespół do spraw Incydentów Kryzysowych. Poprzez współpracę z wieloma podmiotami działającymi lub mającymi styczność ze strefą cyberprzestrzeni zespół ten tworzy zorganizowany i w pełni funkcjonalny system zapobiegania i reagowania w sytuacjach ryzyka i niebezpieczeństwa oraz odpowiadający za koordynację zgłoszeń.

Incydenty są zdarzeniami, które zagrażają lub mogą zagrozić cyberbezpieczeństwu. Bardzo istotna jest szybka reakcja na nie. Procedura reagowania składa

się z następujących etapów: wykrywania, rejestracji lub analizy, następnie odpowiedniego zakwalifikowania incydentu i nadania mu adekwatnego priorytetu. Później, w zależności od rozwoju sytuacji, prowadzi się działania naprawcze oraz zmierzające do ograniczenia skutków lub tylko jedno z nich. Wszystkie te czynności nazywane są obsługą incydentu. Same incydenty, ze względu na powagę wywoływanych przez nie skutków, można podzielić na:

- obniżające jakości lub przerywające realizację zadania publicznego realizowanego w podmiocie publicznym,
- istotne, odnoszące się do usług cyfrowych i mające wpływ na ich świadczenie,
- poważne, dotyczące usługi kluczowej, których skutkiem jest obniżenie jakości lub przerwanie ciągłości usług,
- krytyczne, a jego skutki wychodzą poza interes krajowy i mogą dotyczyć interesów gospodarczych na poziomie międzynarodowym, funkcjonowania instytucji publicznych, a także życia lub zdrowia ludzi.

Poza współpracą z właściwymi ministrami, zespoły te mają obszerny katalog obowiązków oraz uprawnień. Jest to konsekwencją wzrostu ryzyka i różnorodności zagrożeń. Ustawa o krajowym systemie cyberbezpieczeństwa definiuje również samo pojęcie ryzyka, jako „kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji" [Dz. U. z 2018 r., poz. 1560]. Co ważne, właściwy zespół może w przypadku zgłoszenia incydentu poważnego, po konsultacji ze zgłaszającym, opublikować w Biuletynie Informacji Publicznej informacje o zagrożeniu. Ma to na celu, w miarę możliwości, zapobiegnięcie jego wystąpieniu lub zapewnienie obsługi tego incydentu. W przypadku incydentów istotnych, zespół ma również możliwość zgłoszenia się z poleceniem publikacji do odpowiedniego operatora cyfrowego. Jednakże do rutynowych zadań tych jednostek należy przede wszystkim monitorowanie zagrożeń przy szacowaniu ryzyka ich wystąpienia oraz przeprowadzanie dynamicznych analiz ryzyka.

Całe przedsięwzięcie nadzoruje minister właściwy do spraw informatyzacji. Jest on zobowiązany do utrzymania i wspierania rozwoju systemu teleinformatycznego wspomagającego współpracę w ramach krajowego systemu cyberbezpieczeństwa. Sporządzanie rocznych sprawozdań jest bardzo ważnym elementem funkcjonowania każdej instytucji, jak i wszelkich systemów. Ich analiza pozwala na obiektywne spojrzenie na osiągnięcia i trudności, co zwykle wpływa na poprawę ich skuteczności. Za sprawozdanie odpowiedzialny jest właśnie minister informatyzacji. Zawiera ono również informacje o incydentach, których zasięg wykraczał poza terytorium Rzeczpospolitej Polskiej.

Prowadzony przez ministra do spraw informatyzacji punkt kontaktowy jest istotnym elementem szybkiego reagowania. Zapewnia on współpracę z Komisją Europejską oraz reprezentuje Polskę we współpracy międzynarodowej. Gwarantuje także łączność w przypadku wystąpienia incydentu, czy to na terenie kraju czy poza jego granicami.

Za realizację polityki rządu w zakresie cyberbezpieczeństwa odpowiada pełnomocnik. Funkcję tę pełni sekretarz lub podsekretarz stanu, powołany przez prezesa Rady Ministrów. Przy współpracy z właściwymi ministrami prowadzi działania mające na celu podniesienie świadomości społeczeństwa w tematyce technologii i związanych z nią zagrożeń oraz wspiera badania naukowe dotyczące tych zagadnień. Kolejną z czynności profilaktycznych jest inicjacja ćwiczeń na szczeblu krajowym. Współpraca pełnomocnika z rządem przejawia się między innymi w przekładaniu Radzie Ministrów rocznych sprawozdań oraz opiniowaniu rządowych dokumentów.

Jak przy każdym większym projekcie, tak również przy zarządzaniu w tej strefie, istnieje powołane opiniodawcze kolegium. Odgrywa ono dużą rolę w sprawnym działaniu Krajowego Systemu Cyberbezpieczeństwa. Między innymi opiniuje współpracę wszystkich zaangażowanych w tą działalność podmiotów i poświęca szczególną uwagę realizacji zadań przez wszystkie trzy zespoły CSIRT. Rada Ministrów uprawniona jest zaś do wydawania wiążących wytycznych regulujących sposób prowadzenia polityki cyberbezpieczeństwa na podstawie rekomendacji opracowanych przez kolegium.

Ustawa o krajowym systemie cyberbezpieczeństwa przewiduje wprowadzenie w drodze uchwały strategii cyberbezpieczeństwa. Aktualnie w Rzeczpospolitej Polskiej realizowana jest strategia na lata 2017–2020 [https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09], opracowana przez przedstawicieli pięciu resortów:

- Cyfryzacji,
- Obrony Narodowej,
- Spraw Wewnętrznych i Administracji,
- Agencji Bezpieczeństwa Wewnętrznego,
- Rządowego Centrum Bezpieczeństwa,
- Biura Bezpieczeństwa Narodowego.

Akt ten wskazuje podmioty odpowiedzialne za wdrażanie postanowień strategii oraz określa jej cele – zarówno główne, jak i szczegółowe. Wskazuje także na kierunki rozwoju edukacji, działalności badawczo-naukowej oraz współpracy międzynarodowej.

Celem głównym strategii jest „zapewnienie wysokiego poziomu bezpieczeństwa sektora publicznego, sektora prywatnego oraz obywateli w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych" [https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09] . Cele szczegółowe (cztery) zaś zmierzają do ustanowienia silnej, międzynarodowej pozycji Polski w cyberprzestrzeni. Ich realizacja rozpoczyna się od wzmocnienia na szczeblu krajowym, poprzez wypracowanie skoordynowanego programu zapobiegania, wykrywania i zwalczania zagrożeń. Istotne jest również zwiększenie potencjału narodowego i kompetencji w tej strefie. W konsekwencji wzmocni to zdolność do odpierania cyberzagrożeń.

Podsumowanie

Chęć ciągłego rozwoju sprawia, że ludzkość staje naprzeciw nowym wyzwaniom, także w XXI wieku. Wprowadzanie nowych technologii wymusza opracowanie coraz to nowszych i precyzyjniejszych sposobów ochrony przed wiążącymi się z nimi niebezpieczeństwami. Jak pokazuje dotychczasowy rozwój prawa, jest ono przede wszystkim odpowiedzią na pojawiające się problemy. Ciężko jest przewidzieć przyszłe wydarzenia i proponować rozwiązania prawne jeszcze przed ich wystąpieniem. Analizując akty prawne, można zauważyć, że ustawodawca jest tego świadomy. Rozbudowana siatka organów działających w kwestii cyberzagrożeń oraz współdziałanie na skalę międzynarodową świadczą o dużym zaangażowaniu wielu podmiotów w tworzenie sprawnie działającego systemu bezpieczeństwa. Wracając więc do pytania, czy regulacje prawne i system cyberbezpieczeństwa rozwijają się w sposób dynamiczny, Polska poprzez wprowadzane rozwiązania i programy rozwoju spełnia wysokie standardy ochrony. W związku z powyższym należy stwierdzić, że istnieje duże prawdopodobieństwo, że reakcja w przypadku wystąpienia cyberzagrożenia będzie szybka i odpowiednia.

Bibliografia

DOD Dictionary of Military and Associated Terms [online], https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf, dostęp: 05.02.2019.

Słownik Komisji Europejskiej [online], http://ec.europa.eu/ information_society/tl/help/glossary/index_en.htm#c, dostęp: 05.02.2019.

Dziennik Urzędowy UE (Dz. Urz. UE L 194 z 19.07.2016, str. 1) [online], https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=OJ%3AL%3A2016%3A194%3ATOC, dostęp: 05.02.2019.

Słownik języka polskiego [online], https://sjp.pwn.pl, dostęp: 05.02.2019.

Górny P., Krawiec J. (2016), *Cyberbezpieczeństwo – podejście systemowe, obronność*, ,,Zeszyty Naukowe", z. 2(18), s. 2.

https://www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09, dostęp: 14.02.2019.

Karatysz M. (2013), *Zjawisko cyberprzestępczości a polityka cyberbezpieczeństwa w regulacjach prawnych Rady Europy, Unii Europejskiej i Polski*, ,,Refleksje. Pismo naukowe studentów i doktorantów WNPiD UAM", nr 7, Wydawnictwo Naukowe WNPiD UAM, Poznań, s. 140.

Lakomy M. (2015), *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice, s. 71.

National Strategy to Secure Cyberspace [online], https://www.dhs.gov/national-strategy-secure-cyberspace, dostęp: 05.02.2019.

Nowak A. (2013), *Cyberprzestrzeń jako nowa jakość zagrożeń*, ,,Zeszyty naukowe AON", nr 3(92), ss. 6–10.

Schreier F., 2015, *On Cyberwarfare*, ,,DCAF Horizon 2015 Working Paper", vol. 7.

The UK Cyber Security Strategy [online], https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf , dostęp: 05.02.2019.

Wasilewski J. (2013), *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego", z. 5, nr 9, ss. 226–228.

Wrona J. (2017), *Cyberprzestrzeń a Prawo Międzynarodowe Status Quo i Perspektywy*, rozprawa doktorska, przygotowana pod kierunkiem naukowym dr. hab. Macieja Perkowskiego, prof. UwB , Uniwersytet w Białymstoku, Wydział Prawa Zakład Prawa Międzynarodowego Publicznego, Białystok [online], https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/5875/1/J_Worona_%20Cyberprzestrzen_a_%20prawo_miedzynarodowe_Status_quo_i_perspektywy.pdf, dostęp: 05.02.2019.

WeAreSocial UK., *Digital in 2018: World's internet users pass the 4 billion mark* [online], https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018, dostęp: 05.02.2019.

Akty prawne

Kodeks Karny (Dz. U. z 2019 r., poz. 1950).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r., poz. 700).

Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2019.123).

Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2018 r., poz. 1932).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2018 r., poz. 1560).

Ustawa z dnia 5 września 2016 r.o usługach zaufania oraz identyfikacji (Dz. U. z 2019 r., poz. 162).

Orzecznictwo

Wyrok Sądu z dnia 27.12.2017 r., Sygn. Akt: IC 1668/16 [online], http://orzeczenia.ms.gov.pl/details/$N/155020050000503_I_C_001668_2016_Uz_2018-01-18_001, dostęp: 05.02.2019.

Wyrok Sądu z dnia 11.01.2018r., Sygn. Akt: II K 164/17 [online], http://orzeczenia.ms.gov.pl/details/$N/153510600001006_II_K_000164_2017_Uz_2018-01-11_001, dostęp: 05.02.2019.

Wyrok Sądu z dnia 24.01.2013r., Sygn. Akt: IV Ka 1675/12 [online], http://orzeczenia.ms.gov.pl/details/$N/155515000002006_IV_Ka_001675_2012_Uz_2013-01-24_001, dostęp: 05.02.2019.

Kamil Martyniak
kamil.m.martyniak@gmail.com
Krakowska Akademia im. A. Frycza Modrzewskiego,
Wydział Nauk o Bezpieczeństwie

Internet jako źródło zagrożeń bezpieczeństwa indywidualnych transakcji walutowych

Wstęp

Nowoczesne technologie w cyberprzestrzeni są najszybciej rozwijającymi się przejawami i przestrzeniami aktywności człowieka. Jednak, oprócz niewątpliwych szans dla rozwoju cywilizacyjnego, kulturowego i gospodarczego, niosą pewne zagrożenia dla bezpieczeństwa państwa, w tym także dla zasobów jego obywateli. Przestępczość występująca w cyberprzestrzeni jest nowym zagrożeniem, obserwowanym przez organy ścigania, służby specjalne, przedsiębiorców czy uczelnie zajmujące się zagadnieniem bezpieczeństwa w cyberprzestrzeni. Najbardziej znanym motywem działania sprawców tego rodzaju przestępstw jest ukierunkowanie działań na osiągnięcie zysku – korzyści majątkowych. Osoby zaangażowane w działania przestępcze, oprócz stworzenia pełnej anonimowości w sieci, w celu ukrycia, zalegalizowania korzyści pochodzących z cyberprzestępstw, uchylenia się od opodatkowania, korzystają z ukrytej tożsamości, a ich działalność przestępcza opiera się również na socjotechnice.

Wszechobecna działalność Internetu spowodowała, iż także użytkownicy portali społecznościowych stali się idealnym przedmiotem zysku dla działających w celu osiągnięcia korzyści majątkowej hakerów. Aczkolwiek haker nie będzie

w niniejszym rozdziale utożsamiany z mianem osoby, która w sposób techniczny ingeruje w zasoby ofiary, lecz z psychologicznym manipulatorem zachowania konsumenta bankowości elektronicznej. Istotnym elementem treści rozdziału będzie zobrazowanie skali, jaką w dobie aktualnego posługiwania się Internetem stanowi socjotechniczne wykorzystanie uzyskanych w ten sposób danych od osób niebędących świadomymi tego, że padły ofiarą oszustów.

Celem rozdziału jest przedstawienie Internetu jako źródła zagrożeń bezpieczeństwa indywidualnych transakcji walutowych. Jego treść przybliża czytelnikowi m.in. modele działania sprawców kradzieży pieniędzy z rachunków bankowych użytkowników bankowości elektronicznej, a zarazem osób korzystających z powszechnych portali społecznościowych, artykuł ukazuje ponadto nowe oblicze hakingu jako działania psychologicznego.

Problem badawczy, jaki autor stawia w dyskursie z tematem opracowania, brzmi: jakie działania wykorzystują cyberprzestępcy w dążeniu do zmanipulowania użytkowników Internetu, w celu pozyskania informacji, które pozwolą im zyskać dostęp do zasobów materialnych?

W rozdziale omówiono kwestie związane z teorią socjotechniki i socjoinformatyki. Opisano różne ich definicje i zakres w powiązaniu z działaniami w cyberprzestrzeni. Zestawiono fundamentalne reguły, na których opiera się socjotechnika. Autor opisał także pojęcie kradzieży tożsamości w sieci. Wskazuje m.in. elementy, jakimi użytkownicy Internetu „chętnie" dzielą się z cyberprzestępcami. Meritum opisane zostało dzięki wskazaniu metod, jakimi najczęściej posługują się sprawcy grabieży internetowych.

Możliwości wykorzystania socjotechniki i socjoinformatyki w działaniach cyberprzestępców

W teorii socjotechnika może być rozumiana wielowątkowo. Ch. Hadnagy w swojej książce pt. *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, prezentuje owo pojęcie jako: „Posługiwanie się kłamstwem w celu pozyskania informacji od innych ludzi", (...) „Socjotechnika to nic innego jak dobre kłamstwo", (...) „Socjotechnika to umiejętność zdobywania różnych rzeczy za darmo" [Hadnagy 2017, ss. 26–27].

W *Słowniku Języka Polskiego* PWN pod hasłem „Socjotechnika" można wskazać definicje [*Słownik Języka Polskiego PWN* 2019]:

1. „Ogół metod i działań zmierzających do uzyskania pożądanego zachowania jednostek i grup ludzkich";
2. „Nauka o sposobach i wynikach świadomego wpływania na rzeczywistość społeczną".

Angielska Wikipedia definiuje socjotechnikę jako „Manipulowanie ludźmi w celu nakłonienia ich do podjęcia określonych działań lub ujawnienia poufnych informacji. Socjotechnika nie różni się zatem wyraźnie od przekrętu czy pospolitego oszustwa, jednak termin ten jest zwykle stosowany na określenie sztuczek lub podstępów stosowanych w celu gromadzenia informacji, dokonywania oszustw lub uzyskiwania dostępu do systemów komputerowych. W większości przypadków osoba dokonująca ataku nie spotyka się twarzą w twarz ze swoją ofiarą" [*Słownik Języka Polskiego PWN* 2019]. W Polsce za *sui generis* ojca – założyciela uznawany jest A. Podgórecki, który rozpowszechnił termin socjotechnika w polskiej literaturze przedmiotu. Co więcej, stwierdził, że dziedziną socjotechniki są metody działania, strategie i taktyki postępowania w przypadkach nie tymczasowych oraz określone sposoby funkcjonowania [Karwat 2014, s. 16]. Synonimem socjotechniki jest pojęcie inżynierii społecznej, która zajmuje się możliwościami przebudowy społeczeństwa. Według A. Podgóreckiego i jego kontynuatorów, socjotechnika jest określana jako:

1. Techniczne możliwości nauk społecznych i planowania i skutecznego kreowania zmian społecznych;
2. Celowe postępowanie, którego efektem mają być potrzebne systemowi sterującemu zmiany w obiekcie sterowanym;
3. Nauka praktyczna, której przedmiotem jest celowe postępowanie, a zadaniem projektowanie oparte na przyjętym systemie wartości uznanych twierdzeń teoretycznych.

K. Churska, po analizie koncepcji Podgóreckiego, podkreśla, że socjotechnikę można formułować z punktu widzenia zaradności zbiorowej zastanej i racjonalnej, a więc takiej, która funkcjonuje w życiu społecznym oraz tej, która powinna być stosowana [Pawełczyk 2015, s. 13]. Można również definiować socjotechnikę rozumiejąc ją przez pryzmat klasyfikacji nauk, której celem jest uporządkowanie nagromadzonych doświadczeń, refleksji i badań z obszaru socjotechniki [Podgórecki 1972, s. 36].

Kolejną próbę zdefiniowania terminu socjotechnika podjął M.K. Mlicki. Według badacza „termin inżynierii społecznej należy rozumieć przez zespół dyrektyw

dotyczących racjonalnych i celowych przemian społecznych mających podwaliny w ocenach i wartościach. Celowość i racjonalność należy tu rozpatrywać z punktu widzenia obiektu sterującego" [Mlicki 1988, s. 51].

Z kolei J. Goćkowski mówi o socjotechnice jako „metodzie budowania i przekazywania reguł oddziaływania na grupy i jednostki w celu nauczenia adaptacji cywilizacyjnej. Chodzi tu o opracowane sposoby socjalizacji. Podobieństwo do procesu socjalizacji jest tym większe, im silniejsze jest dążenie do jego doskonalenia". Zwracając uwagę na relacje pomiędzy socjotechniką a władzą, Goćkowski wskazuje, że „oddziaływanie socjotechniki na grupy i jednostki jest środkiem walki o zdobycie, utrzymanie, umocnienie i rozszerzenie oraz przekształcenie kontroli i decydowania o losie innych jednostek, przez co zasługuje na miano władzy politycznej" [Goćkowski 2000, s. 38].

Natomiast T. Koćkowski dzieli termin na:

- „socjotechnikę pierwszego stopnia, polegającą na tworzeniu zespołu bodźców, które skłaniają ludzi do określonych zachowań przy bezpośrednim wykorzystaniu systemu kar i nagród";
- „socjotechnikę drugiego stopnia, definiowaną jako sposób wytwarzania w ludziach określonej motywacji lub kształtowania odpowiednich cech osobowości" [https://mfiles.pl/pl/index.php/Socjotechnika]. Końcowym założeniem przyjętej przez Koćkowskiego tezy jest zbliżone oddziaływanie w obu przypadkach, z tą różnicą, że socjotechnika drugiego stopnia polega na niebezpośrednim oddziaływaniu przy użyciu norm prawnych, poprzez ich internacjonalizację w świadomości jednostki.

Podstawowe metody socjotechniki to np. perswazja, manipulacja, intensyfikacja lęku. Mimo, że wymienione różnią się od siebie sposobem i skutkiem działania, łączą się w nacisku wywieranym na drugiego człowieka. Oparte są na emocjach (strach, współczucie, miłość), ale i na intelekcie (pokazywanie danych statystycznych, powoływanie się na autorytety i społeczny dowód słuszności). To także okryte złą sławą techniki NLP – programowanie neurolingwistyczne. W uproszczeniu nazwę neurolingwistyczne programowanie można tłumaczyć następująco: pierwsza część odnosi się do związku sposobu przetwarzania informacji ze strukturą języka, jaką posługuje się dana osoba. Chodzi m.in. o to, że nieświadomie stosowane nawyki językowe wywierają potężny wpływ na percepcję, myślenie i generalnie na ludzkie doświadczenie (i odwrotnie). Indywidualne wzorce tych związków tworzą subiektywny świat osoby i swego rodzaju „programy", które wpływają na jej działania. Pojęcie „programowanie" wskazuje, że celowa zmiana owych wzorców jest możliwa, zwłaszcza gdy mają one ograniczający charakter, stają się źródłem problemów

czy cierpienia. Biorąc pod uwagę miejsce, jakie od lat NLP zajmuje w różnych dziedzinach ludzkiej aktywności oraz funkcje, jakie w nich pełni, najtrafniej można je obecnie określić jako jedną ze szkół psychologii stosowanej, dostarczającą wiedzy i metod na temat usprawniania komunikacji, wprowadzania zmian i realizacji celów. Jak każda nauka stosowana, NLP skupia się przede wszystkim na swoich praktycznych odkryciach, a w mniejszym stopniu angażuje się w rozwój teorii (choć samo czerpie inspiracje z różnych dyscyplin teoretycznych). I to właśnie pragmatyczny charakter NLP stanowi o jego atrakcyjności [Skała 2015, s. 36].

Autor niniejszej pracy, po analizie powyższego, zdefiniował socjotechnikę na własny sposób jako działanie polegające na takim manipulowaniu drugą osobą, aby podjęła określone działania wbrew własnemu interesowi, bądź które mogą leżeć w interesie tej osoby. Może chodzić tu o pozyskiwanie informacji, uzyskiwanie dostępu do czegoś lub nakłanianie ofiary do podjęcia konkretnych działań.

Socjoinformatyka obejmuje elementy socjotechniki i informatyki lub też socjologii, psychologii i najnowszych technik komputerowych. To, co ją odróżnia od typowych ataków informatycznych, to fakt, że socjotechnik nie musi być specjalistą z zakresu technologii informacyjnej (ang. *information technology* – IT). Najczęściej nim jest, a przynajmniej posiada na ten temat ogólną wiedzę, lecz nie jest to obligatoryjne. Musi natomiast znać cały wachlarz narzędzi wpływu oraz technik manipulacyjnych oferowanych przez socjotechnikę – być świetnym aktorem, umieć doskonale kontrolować emocje i dysponować wieloma innymi umiejętnościami, całkowicie niezwiązanymi z informatyką. Rozgraniczenie socjotechniki od socjoinformatyki jest dość proste. Kiedy mówimy o manipulowaniu ludźmi w dowolnym celu, to mamy do czynienia z socjotechniką. Jeżeli celem tym jest włamanie do komputera lub systemu informatycznego, kradzież poufnych danych, kradzież tożsamości lub inne naruszenie bezpieczeństwa – to mówimy o socjoinformatyce [Trejderowski 2013, s. 11–12].

Jeden człowiek, odpowiednio wyszkolony, stosujący socjoinformatykę i wykorzystujący niewiedzę oraz naiwność ludzką, nie ujawniając swojej prawdziwej (często) tożsamości, może doprowadzić do wielomilionowych strat firmy. Nie musi być geniuszem komputerowym. Może to osiągnąć dzięki doskonałemu wyszkoleniu i wiedzy o psychice ludzkiej, socjologii i socjotechnice. Według niektórych źródeł cyberprzestępczość przynosi obecnie większe zyski niż handel narkotykami [*Ataki na informację* 2018, s. 12]. Jest przy tym nieporównywalnie łatwiejszą, tańszą i bezpieczniejszą działalnością. Teoria podstaw socjoinformatyki mówi, że najbardziej zawodnym, niebezpiecznym i kosztochłonnym elementem każdej firmy są ludzie. Firma, agenda rządowa, organizacja lub fundacja może wydać miliony na

wdrożenie najnowocześniejszych zabezpieczeń informatycznych czy telekomunikacyjnych, lecz i tak łatwo padnie ofiarą socjotechnika, który do ataku wykorzysta źle lub wcale nieprzeszkolonego pracownika [Trejderowski 2013, ss. 15–16]. Równie popularnym celem socjotechników jest kradzież tożsamości oraz dostęp do danych przechowywanych na komputerach prywatnych, na przykład numerów kart kredytowych lub loginów i haseł do serwisów internetowych. Najsłabszym ogniwem jest nie tylko pracownik firmy, ale każdy człowiek. Badania przeprowadzone w 2017 roku przez RSA Security ujawniły, że aż 79% ankietowanych było skłonnych podać przypadkowo spotkanej osobie dane osobowe wystarczające do kradzieży tożsamości. Respondenci przyznawali, że nie mieli większych oporów przed ujawnieniem daty urodzenia czy nazwiska panieńskiego swojej matki. 33% badanych przyznało, że przynajmniej raz w życiu złamało podstawową zasadę bezpieczeństwa, nosząc zapisane hasło lub inne kluczowe dane do konta internetowego w portfelu, albo w innym równie łatwo dostępnym miejscu. Prawie 2/3 pytanych (64%) przyznało, że używa tego samego loginu i hasła we wszystkich usługach internetowych, od portali społecznościowych przez fora dyskusyjne i pocztę elektroniczną po bankowość internetową [*Wielkiej Brytanii grozi fala przestępstw…* 2017].

Praktycznie cała socjoinformatyka opiera się na socjotechnice, czyli na wywieraniu wpływu na ludzi, skłanianiu ich do podejmowania decyzji lub działań, których świadomie mogliby nie podjąć. Socjotechnika opiera się z kolei na siedmiu fundamentalnych regułach [Trejderowski 2009, s. 35]:

- **Reguła wzajemności** mówi o tym, że w odpowiedzi na otrzymane od kogoś każde dobro (pomoc, wsparcie, podarunek), czujemy natychmiastową i nieodpartą chęć odwzajemnienia. Socjotechnik, pomagając lub sugerując, że pomógł swojej ofierze w rozwiązaniu jakiegoś problemu, może wydobyć istotną dla siebie informację. W ten sposób socjotechnicy mogą przełamywać pierwotny opór pracowników firm – na przykład pracownik znacznie chętniej wyjawi jakieś poufne dane, jeśli atakujący tak zaaranżuje sytuację, by ofiara czuła chęć odwzajemnienia się. W ramach reguły wzajemności określa się również pojęcie „wzajemność ustępstw". Jeśli ktoś rezygnuje z czegoś, co mogłoby być dla nas negatywne, my również pragniemy zrewanżować się mu, rezygnując z czegoś, co mogłoby być negatywne dla niego.
- **Reguła konsekwencji** – w myśl tej reguły, angażując się w coś, będziemy konsekwentnie dążyć do realizacji zamierzonego celu. Jej sens oddaje powiedzenie: „Jeśli się powiedziało A, trzeba także powiedzieć B". Socjotechnik może sztucznie zaaranżować impuls aktywujący, za którym manipulowana ofiara konsekwentnie podąży i wykona to, czego oczekuje od niej manipulator.

• **Reguła społecznego dowodu słuszności** – zgodnie z nią łatwiej jest nas przekonać do czegoś, jeśli zostanie udowodnione, że inni również myślą bądź zachowują się w ten sam sposób.
• **Reguła sympatii** – jeśli kogoś lubimy lub wydaje się nam sympatyczny, to dużo chętniej ulegamy jego prośbom niż prośbom osoby obojętnej i pozwalamy sobie na „naginanie zasad". To dlatego w okresie wojny niewinnie wyglądające śliczne dziewczyny przenosiły nielegalne druki i broń. Budzenie sympatii, wywoływanie pozytywnych wrażeń i skojarzeń, chęci niesienia pomocy, to podstawa działania każdego socjotechnika. Należy jednak pamiętać, że kryje się za tym perfidny plan.
• **Reguła autorytetu** mówi, że trudno sprzeciwiać się komuś, kto jest mądrzejszy, bardziej doświadczony, „postawiony wyżej" niż my. Często czujemy podświadomy strach przed osobami obdarzonymi autorytetem. Jeśli socjotechnik wywoła wrażenie, że wykonuje polecenie „z góry" lub posiada autorytet albo władzę, to ofierze ciężko jest przeciwstawić się takiej manipulacji. Doświadczenie uczy, że rzadziej neguje się opinie i decyzje osób uznanych za autorytet, nawet jeśli wiele wskazuje na to, że owe opinie czy decyzje są błędne. Z innej jednak strony, jeśli socjotechnik wmówi komuś, że uważa go za autorytet, to połechta próżność tej osoby i dużo łatwiej uda mu się namówić ją na określone działanie czy czasowe wyłączenie zdrowego rozsądku.
• **Reguła niedostępności** – to bodaj najczęściej stosowana reguła socjotechniczna. Zgodnie z nią, wzrasta przekonanie o wartości czegoś, co jest czasowo lub długotrwale niedostępne. Stąd bezpośrednio wynika ciekawość. Jeśli socjotechnik wywoła w ofierze wrażenie, że „coś wie", ma dostęp do poufnych informacji, może łatwo zdobyć jej zaufanie, uległość lub chociaż zainteresowanie. Istnieje również odwrócona reguła niedostępności, w myśl której rzeczy łatwo dostępne mają w naszych oczach niewielką wartość. Socjoinformatyka zadaje kłam tej regule. U jej podstaw leży założenie, że nie ma informacji nieistotnych lub bezwartościowych. Dla socjotechnika każda informacja ma wartość.
• **Reguła wartości** – zwana też regułą maksymalizacji własnego zysku – mówi o tym, że o rzeczy wartościowe (zarówno materialne, jak i niematerialne, takie jak cześć, honor, dobre imię, sława) walczymy chętniej i częściej niż o te mniej wartościowe. Często wpadamy w tym zakresie w pułapki, a nawet uciekamy się do działań z pogranicza zdrowego rozsądku. Jeśli socjotechnik wywoła w nas wrażenie zagrożenia istotnych wartości, łatwo może skłonić nas do korzystnego dla siebie działania. Reguła wartości jest silnie związana ze skłonnością do przeceniania pożytków psychologicznych płynących z posiadania danego dobra (w tym możliwości pochwalenia się przed innymi) względem jego faktycznej

wartości użytkowej lub konsumpcyjnej. To klasyczny snobizm. Jest on rzadziej wykorzystywany w aktach socjotechnicznych, ale nie może być zupełnie ignorowany.

Kradzież tożsamości w sieci

Zjawisko kradzieży tożsamości zawsze towarzyszy działalności socjotechników. Mają z nim do czynienia zarówno przy rozpoznaniu przed właściwym atakiem, podczas tkania sieci, w trakcie przygotowań do niego, jak i w trakcie samego ataku. To najważniejsze po oszustwie narzędzie ich działania. Stanowi czasem efekt misternego, przygotowywanego miesiącami ataku socjotechnicznego.

To, że na portalach i w sieciach społecznościowych chętnie informujemy o wszystkim, jest rzeczą oczywistą. Aczkolwiek, czy zdajemy sobie sprawę z faktu, ile informacji jest tam dostępnych? Znając tylko imię i nazwisko ofiary oraz ewentualnie nazwę miasta, w którym ona mieszka, można [Liderman 2012, s. 56]:

- zobaczyć jej zdjęcie lub zdjęcia, a także zdjęcia jej rodziny lub znajomych;
- poznać wiek, a na jego podstawie przybliżoną datę urodzenia (rok);
- poznać całe zastępy jej znajomych, kolegów z pracy, członków rodziny, itp.;
- jeśli wypełni swój profil szczegółowo – zyskać dodatkowe informacje o tej osobie i o tym, czym się aktualnie zajmuje, gdzie pracuje lub studiuje;
- poznać dokładny przebieg jej edukacji – szkoły, uczelnie, odbyte kursy;
- poznać numer Gadu-Gadu, Skype'a i telefonu, jeśli takie dane ujawni;
- poznać stan cywilny: po nazwisku, fotografiach lub porównując nazwiska znajomych;
- analizując fotografie i ewentualnie listę znajomych, dowiedzieć się, czy ma dzieci, a także często poznać ich płeć i oszacować wiek;
- jeżeli ktoś publikuje zdjęcia ze ślubu i są to fotografie dobrej jakości (lub na przykład oznaczone geotagiem), to dobry socjotechnik odkryje, gdzie para brała ślub lub gdzie się bawiła na weselu;
- szczegółowo porównując nazwiska na liście znajomych można odkryć powiązania rodzinne – rodzeństwo, kuzynostwo, bliżsi i dalsi krewni i powinowaci;
- porównując szkoły i uczelnie, w których się uczy ze znajomymi, poznać znajomych z jej konkretnych szkół i uczelni;
- czytając podpisy pod fotografiami, komentarze do nich i do profilu, poznać wiele szczegółów z życia prywatnego ofiary – gdzie spędzała wakacje, w jakich

klubach lubi się bawić, jakie preferuje formy spędzania wolnego czasu, jakie ma hobby, itd.;

- analizując daty i godziny dodawania kolejnych fotografii lub udzielania odpowiedzi na komentarze, poznać w jakich porach korzysta z Internetu, czy ma dostęp do niego w pracy, czy może tylko wieczorem lub w nocy.

Na podstawie informacji dostępnych jawnie (większość wymienionych powyżej) socjotechnik bez większego problemu przekona ofiarę, że jest jej dawnym znajomym. Po dodaniu go do listy – uzyskuje dostęp do owych rzekomo poufnych i chronionych danych. Biorąc przykład mechanizmu „Like" („Lubię to!") z Facebooka, odpowiednio zanalizowany przez socjotechnika, może być dla niego kopalnią informacji. O tym, co ofiara lubi, jakie są jej poglądy i zainteresowania oraz jej znajomych. To bezcenne źródło informacji dla stosowania socjotechnicznej reguły sympatii, która mówi, że znacznie bardziej lubimy i ufamy osobom, które są do nas podobne i mają takie same poglądy. Nic przecież nie stoi na przeszkodzie, by socjotechnik, który chce zaatakować swoją ofiarę, skłamał, że również jest na przykład fanem ostrej muzyki rockowej [Kosiński 2015, s. 54].

Najchętniej odwiedzanym portalem przez socjotechników i złodziei tożsamości jest niewątpliwie Facebook. Portal ten jest atakowany kilkaset tysięcy razy dziennie. Ile spośród tych ataków przeprowadzono dla samej blokady serwisu, a ile dla kradzieży danych użytkowników? To są właśnie wątpliwe dary „Web 2.0" i wszystkich usług internetowych typu *stay connected*. Dzięki temu, pojęcia ochrony własnej prywatności i tożsamości nabierają zupełnie nowego znaczenia. Teraz niewinne strony internetowe, portale i usługi pozwalające szerszemu gronu ujawniać prywatne informacje, wcale już nie są takie „niewinne". Bezapelacyjne królowanie urządzeń mobilnych, które wydatnie ułatwiają takie dzielenie się prywatnością z całym światem, znacznie pogarsza sytuację. Usługi takie, jak Twitter oraz wiecznie aktywne moduły GPS w urządzeniach mobilnych, dokładają do tego jeszcze bardzo dokładne informacje o aktualnym miejscu przebywania. Złodziej bez problemu dowie się, że ofiara wyjeżdża na weekend, na wczasy bądź inny wypoczynek [Trejderowski 2013, s. 151–152].

Zagrożenie waluty w ramach przetwarzania danych w sieci Internet

Ostatnie ćwierćwiecze to okres niezwykle szybkiego rozwoju technik komputerowych oraz rozprzestrzenienia się dostępu do Internetu. Przez okres 12 lat – pomię-

dzy rokiem 1990, a 2002 – liczba osób korzystających z Internetu wzrosła 224-krotnie i w 2002 r. wyniosła ponad 631 mln użytkowników [http://www.worldmapper.org/posters/worldmapper_map336_ver5.pdf]. Szacuje się również, że pomiędzy rokiem 2000 a 2010 liczba osób korzystających z zasobów Internetu wzrosła pięciokrotnie, zbliżając się do 2 mld. Największe procentowe przyrosty liczby użytkowników Internetu miały miejsce na obszarze Afryki – 2357% wzrostu pomiędzy rokiem 2000 a 2010, Bliskiego Wschodu – 1825%, Ameryki Południowej – ponad 1033% oraz Azji – 622%. Oczywiście taki przyrost był wynikiem niskiej bazy dla tych kontynentów w roku 2000. Dla porównania, wzrost liczby użytkowników Internetu w Ameryce Północnej wyniósł tylko 146%, a w Europie – 352%, przy czym oba te kontynenty w 2000 r. charakteryzowała podobna liczba osób korzystających z sieci [http://royal.pingdom.com/2010/10/22/incredible-growth-of-the-internet-since-2000]. Powyższe dane posłużyć mają jako ilustracja zjawiska, które stało się obecnie dla ogromnej części mieszkańców naszego globu czymś tak oczywistym, jak jedzenie czy sen. Internet zmienił nasze codzienne życie, ma również wpływ na upowszechnianie się nowych zjawisk społecznych, politycznych czy prawnych [Janowski 2014, s. 143]. Wystarczy wskazać, że w trzecim kwartale 2015 r. samych użytkowników portalu społecznościowego Facebook było ponad 1,5 mld – prawie trzykrotnie więcej niż wszystkich użytkowników Internetu w 2000 r. [http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide]. Stały postęp techniczny spowodował, że współcześnie w zasadzie wszystkie przejawy życia społecznego i gospodarczego powiązane są z wykorzystaniem komputerów i dostępem do Internetu.

Cyberprzestępcy od zawsze starali się sięgać po pieniądze, m.in. te zgromadzone na internetowych rachunkach bankowych. W tym celu wykorzystują nie tylko socjotechnikę, ale także aplikacje, które niepostrzeżenie podmieniają numer rachunku bankowego podczas kopiowania go do formularza przelewu online.

Zakończenie

Przedstawione wybiórczo zagrożenia oraz ich skala dowodzą wysokiej szkodliwości działań przestępczych, która jest widoczna w wielu obszarach, aczkolwiek sprowadzają się do jednego – przetwarzania danych w sieci Internet. Nieustannemu i bardzo szybkiemu rozwojowi oraz doskonaleniu się nowych technologii niemal równolegle towarzyszy rozwój „złych" technologii, które wykorzystywane są do

nadużyć i przestępstw. Należy odnotować, iż w bankowości nacisk na ostrożność i bezpieczeństwo jest dużo większy niż w innych sektorach, bo tu incydent przynosi skutki odczuwalne natychmiast. Ponadto istnieje duża przestrzeń do powstawania zagrożeń – szacuje się, że obecnie w Polsce mamy do czynienia z 32 milionami rachunków internetowych i 35 milionami kart płatniczych. Te dwa obszary są bardzo narażone na ataki. Dlatego ważne jest dokładne zlokalizowanie segmentów, w których takie ataki mogą wystąpić, a następnie podjęcie działań mających na celu możliwie jak największe wyeliminowanie zagrożeń.

Warto mieć na uwadze, że mimo coraz to nowszych zagrożeń i wzrastającej liczby ataków cyberprzestępców, zarówno w Polsce, jak i na całym świecie, wzrasta świadomość wagi problemu oraz towarzyszą temu nieustanne próby przeciwdziałania ze strony najważniejszych instytucji finansowych. Warto także pamiętać, iż za poprawę bezpieczeństwa odpowiada sam użytkownik, który jest tym elementem, który obecnie bywa najczęściej narażony na potencjalny atak ze strony hakerów. Stąd tak ważne jest stosowanie podstawowych zasad bezpieczeństwa.

Związek Banków Polskich opublikował na swojej stronie internetowej informację na temat podstawowych zasad związanych z korzystaniem z kanałów elektronicznych, zatytułowany *Cyberbezpieczeństwo Twoich pieniędzy* [https://zbp.pl/aktualnosci/Archiwalne-wydarzenia/cyberbezpieczenstwo-twoich-pieniedzy]. W informacji odnaleźć można podstawowe zasady bezpieczeństwa, którymi powinien się kierować każdy użytkownik produktów bankowych. Przedstawiono także najczęstsze błędy, jakie popełnia statystyczny klient banków przy korzystaniu z produktów elektronicznych. Komunikat ma na celu ustrzec klientów instytucji finansowych przed niewłaściwym korzystaniem ze swoich produktów, co mogłoby skutkować narażeniem na utratę posiadanych pieniędzy.

Bibliografia

Ataki na informację (2018), „Boston IT Security Review", nr 3(4).

Goćkowski J. (2000), *Ludzie systemu i ludzie problemu*, Wydawnictwo SECESJA 2000.

Hadnagy C. (2017), *Socjotechnika. Sztuka zdobywania władzy nad umysłami*, Wydawnictwo HELION, Gliwice.

Janowski J. (2014), *Globalna cyberkultura polityki i prawa*, Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław.

Karwat M. (2014), *Podstawy socjotechniki dla politologów, polityków i nie tylko*, Warszawa.

Kosiński J. (2015), *Paradygmaty cyberprzestępczości*, Warszawa.

Liderman K. (2012), *Bezpieczeństwo informacyjne*, Warszawa.

Mlicki M.K. (1988), *Świadome człowieczeństwo*, Wałbrzych.

Pawełczyk P. (2015), *Kampanie społeczne jako forma socjotechniki*, Wydawnictwo Wolters Kluwer, Warszawa.

Podgórecki A. (2012), *Rozmaite rozumienia socjotechniki i zakres jej stosowalności,* „Roczniki Historii Socjologii", vol. 2, Warszawa.

Skała M. (2015), *Manipulacja odczarowana. 777 skutecznych technik wpływu*, Wydawnictwo HELION, Gliwice.

Słownik Języka Polskiego PWN (2019), pod red. L. Drabik, E. Sobol, Wydawnictwo Naukowe PWN.

Trejderowski T. (2009), *Socjotechnika. Podstawy manipulacji w praktyce*, Wydawnictwo Psychologii i Kultury ENETEIA, Warszawa.

Trejderowski T. (2013), *Kradzież tożsamości. Terroryzm informatyczny*, Wydawnictwo Psychologii i Kultury ENETEIA, Warszawa.

Wielkiej Brytanii grozi fala przestępstw związanych z kradzieżą tożsamości w Internecie (2017), „Gazeta IT", nr 24.

Źródła internetowe

https://mfiles.pl/pl/index.php/Socjotechnika, dostęp: 26.10.2019.

http://royal.pingdom.com/2010/10/22/incredible-growth-of-the-internet-since-2000, dostęp: 26.10.2019.

http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide, dostęp: 26.10.2019.

http://www.worldmapper.org/posters/worldmapper_map336_ver5.pdf, dostęp: 26.10.2019.

Jerzy Gut
jerzygut60@interia.pl
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego,
Wydział Nauk o Bezpieczeństwie

Sławomir Mazur
smazur@orange.pl
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego,
Wydział Nauk o Bezpieczeństwie

Bogdan Tworkowski
bogtwo@wp.pl
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego,
Wydział Nauk o Bezpieczeństwie

Siły Zbrojne w Systemie Zarządzania Kryzysowego

Wstęp

Jednym z ważniejszych zadań nowoczesnego państwa jest zapewnienie obywatelom poczucia bezpieczeństwa oraz ochrony przed zagrożeniami powodowanymi siłami natury lub działalnością człowieka. Wynikają one z norm zwyczajowych i prawnych, których celem jest realizacja podstawowych praw człowieka – prawa do życia i jego permanentnej ochrony. Szeroki wachlarz występujących zagrożeń

naturalnych, jak i będących efektem działalności ludzkiej, wymaga ścisłej specjalizacji i profesjonalizacji całej sfery administracji publicznej i jej służb, co wymusza na rządzących konieczność weryfikowania posiadanych sił i dostępnych środków. Działania te doprowadziły do opracowania kompleksowego systemu do zarządzania kryzysowego – Ustawy o zarządzaniu kryzysowym, która dała podstawy prawne do usankcjonowania systemu zarządzania kryzysowego w Polsce [Dz. U. z 2019 r. poz. 1398, t. j.].

„Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej" [Ustawa o zarządzaniu kryzysowym, Dz. U. z 2019 r. poz. 1398, t. j., art. 2].

Celem rozdziału jest przedstawienie podstaw prawnych dotyczących użycia Sił Zbrojnych, funkcjonowania systemu zarządzania kryzysowego Ministerstwa Obrony Narodowej, a także sił oraz środków, które polskie siły zbrojne mogą wyznaczyć do podjęcia zadań w systemie zarządzania kryzysowego. Dodatkowo ukazano główne płaszczyzny współdziałania wojska i policji oraz zaprezentowano możliwości współpracy w sytuacjach kryzysowych przez nowy rodzaj SZ – Wojska Obrony Terytorialnej z komponentami wojskowymi i cywilnymi.

W badaniach wykorzystano metodę analizy dokumentów, której poddano obowiązujące ustawy, rozporządzenia i decyzje z zakresu zarządzania kryzysowego oraz dokumenty regulujące zasady funkcjonowania instytucji państwowych kierujących tymi procesami.

Podstawy prawne wsparcia militarnego administracji publicznej i społeczeństwa w sytuacjach o charakterze kryzysowym

Najwyższy rangą akt prawny naszego kraju określa, że „Siły Zbrojne Rzeczypospolitej Polskiej służą ochronie niepodległości państwa i niepodzielności jego terytorium oraz zapewnieniu bezpieczeństwa i nienaruszalności jego granic" [Konstytucja Rzeczypospolitej Polskiej, art. 26.1]. Wynikają z niego zadania do realizacji najważniejszego celu Sił Zbrojnych – obrony kraju przed agresją zewnętrzną. Natomiast w Ustawie o powszechnym obowiązku obrony zawarto już, że „Siły Zbrojne

mogą ponadto brać udział w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, działaniach antyterrorystycznych i z zakresu ochrony mienia, akcjach poszukiwawczych oraz ratowania lub ochrony zdrowia i życia ludzkiego, oczyszczaniu terenów z materiałów wybuchowych i niebezpiecznych pochodzenia wojskowego oraz ich unieszkodliwianiu, a także w realizacji zadań z zakresu zarządzania kryzysowego" [Ustawa o powszechnym obowiązku obrony, Dz. U. z 2019 r. poz. 1541, 2020, t. j.]. W art. 60.8.2 tejże Ustawy zawarto, że „Powołanie do odbycia ćwiczeń wojskowych, przeprowadzanych w trybie natychmiastowego stawiennictwa, może nastąpić w celu… udziału jednostek wojskowych w zwalczaniu klęsk żywiołowych i likwidacji ich skutków" [Dz. U. z 2019 r. poz. 1541, 2020, t. j.].

Podstawowy dokument z zakresu zarządzania kryzysowego, Ustawa o zarządzaniu kryzysowym, w art. 25. 1. stanowi: „Jeżeli w sytuacji kryzysowej użycie innych sił i środków jest niemożliwe lub może okazać się niewystarczające, o ile inne przepisy nie stanowią inaczej, Minister ON, na wniosek wojewody, może przekazać do jego dyspozycji pododdziały lub oddziały SZ RP…, wraz ze skierowaniem ich do wykonywania zadań z zakresu zarządzania kryzysowego" [Dz. U. z 2019 r. poz. 1398, t. j]. Podobnie użycie Sił Zbrojnych traktuje Ustawa o stanie klęski żywiołowej – w art. 18 określa, że „w czasie stanu klęski żywiołowej, jeżeli użycie innych sił i środków jest niemożliwe lub niewystarczające, Minister ON może przekazać do dyspozycji wojewody, na którego obszarze odpowiedzialności występuje klęska żywiołowa, pododdziały lub oddziały SZ RP, wraz ze skierowaniem ich do wykonywania zadań związanych z zapobieżeniem skutkom klęski żywiołowej lub ich usunięciem" [Ustawa o stanie klęski żywiołowej, Dz. U. z 2017 r. poz. 1897, t. j.]. W przypadku poważnych zagrożeń dla bezpieczeństwa wewnętrznego kraju, Ustawa o stanie wyjątkowym określa, że Prezydent RP, na wniosek Prezesa RM, może postanowić o użyciu SZ RP do przywrócenia normalnego funkcjonowania państwa, jeżeli dotychczas zastosowane siły i środki zostały wyczerpane. Oddziały i pododdziały SZ RP pozostają w trakcie realizacji zadań pod dowództwem przełożonych służbowych. Zakres działania i zadania określa Minister ON, stosownie do ich specjalistycznego przygotowania i wyposażenia oraz możliwości wykonawczych kierowanych sił [Ustawa o stanie wyjątkowym, Dz. U. z 2017 r. poz. 1928, t. j.]. Poważne zadania stoją przed Siłami Zbrojnymi w razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami o charakterze terrorystycznym, skutkiem czego Prezydent Rzeczypospolitej Polskiej może, na wniosek Rady Ministrów, wprowadzić stan wojenny na części albo na całym terytorium państwa. W tej sytuacji oraz kolejnej, związanej z utrzymaniem lub przywróceniem naruszonego porządku publicznego,

działania wojska polegać będą często na współdziałaniu lub wspieraniu działań policji [Zapałowski 2018, s. 257]. W celu uproszczenia procedur użycia oddziałów i pododdziałów SZ RP, Ustawa o policji przewiduje, że „W przypadkach niecierpiących zwłoki decyzję o udzieleniu pomocy oddziałom policji podejmuje Minister ON, na wniosek Ministra SWiA". Wymagane jest w takim przypadku powiadomienie Prezydenta RP. Użycie SZ RP może następować jedynie w sytuacji realnego zagrożenia bądź dokonania przestępstwa o charakterze terrorystycznym, przy zachowaniu obowiązującej zasady, że oddziały, pododdziały SZ RP mają prawo użyć środków przymusu bezpośredniego i broni palnej w przypadkach oraz na warunkach i w sposób, jak oddziały Policji [Ustawa o Policji, Dz. U. z 2020 r. poz. 360, t.j.].

Siły Zbrojne, realizując zadania konstytucyjne, w pierwszej kolejności powołane są do ochrony niepodległości państwa, niepodzielności jego terytorium oraz zapewnienia bezpieczeństwa i nienaruszalności jego granic, co stawia pewne ograniczenia w wykorzystaniu ich do spraw wewnętrznych. W celu ułatwienia użycia SZ RP do udziału w sytuacjach kryzysowych, Rada Ministrów wydała Rozporządzenie, które określa:

1. rodzaje działań ratowniczych lub prewencyjnych, wykonywanych w celu zapobieżenia skutkom klęski żywiołowej lub ich usunięcia, w których mogą brać udział pododdziały i oddziały Sił Zbrojnych Rzeczypospolitej Polskiej;

2. sposób koordynowania i dowodzenia oddziałami Sił Zbrojnych, biorącymi udział w działaniach, o których mowa w pkt 1;

3. sposób zabezpieczenia logistycznego oddziałów Sił Zbrojnych, biorących udział w działaniach, o których mowa w pkt 1. [Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad pododdziałów i oddziałów SZ RP w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu, Dz. U. z 2003 r. Nr 41 poz. 347].

Zasadnicze obszary działania i zadania Sił Zbrojnych RP w zarządzaniu kryzysowym

Zakres użycia Sił Zbrojnych w kontekście zagrożeń niemilitarnych obejmuje szeroki wachlarz zagadnień. Wspomniane powyżej Rozporządzenie Rady Ministrów zalicza do nich:

1. współudział w monitorowaniu zagrożeń;
2. wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń;
3. wykonywanie zadań poszukiwawczo-ratowniczych;
4. ewakuowanie poszkodowanej ludności i mienia;
5. wykonywanie zadań mających na celu przygotowanie warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach;
6. współudział w ochronie mienia pozostawionego na obszarze występowania zagrożeń;
7. izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej;
8. wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych dobrach kultury;
9. prowadzenie prac wymagających użycia specjalistycznego sprzętu technicznego lub materiałów wybuchowych będących w zasobach Sił Zbrojnych Rzeczypospolitej Polskiej;
10. usuwanie materiałów niebezpiecznych i ich unieszkodliwianie, z wykorzystaniem sił i środków będących na wyposażeniu Sił Zbrojnych Rzeczypospolitej Polskiej;
11. likwidowanie skażeń i zakażeń biologicznych;
12. wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej;
13. współudział w zapewnianiu przejezdności szlaków komunikacyjnych;
14. udzielanie pomocy medycznej i wykonywanie zadań sanitarno-higienicznych i przeciwepidemicznych [Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad pododdziałów i oddziałów SZ RP w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu, Dz. U. z 2003 r. Nr 41 poz. 347].

Do realizacji ww. zadań wydziela się odpowiednie elementy Sił Zbrojnych, stosownie do ich przygotowania specjalistycznego, a biorąc pod uwagę hierarchiczny charakter organizacji wojskowej, dowodzenie oddziałami i pododdziałami wydzielonymi do działań w sytuacjach kryzysowych odbywa się na zasadach określonych w regulaminach wojskowych i według procedur obowiązujących w Siłach Zbrojnych RP. Wprowadzenie oddziałów i pododdziałów wojska do akcji kryzysowej może odbywać się na 3 sposoby:

1. Podstawowa procedura działania określa, że wojewoda zwraca się z wnioskiem do Ministra Obrony Narodowej o wydzielenie sił i środków do

przeciwdziałania sytuacji kryzysowej. Wojewoda podczas przygotowywania wniosku może zasięgać opinii właściwego w danym regionie terenowego organu administracji wojskowej.

2. Procedura nakazowa działania określa, że kierowanie do akcji sił i środków Sił Zbrojnych następuje na podstawie decyzji Ministra Obrony Narodowej lub na rozkaz szefa Sztabu Generalnego WP. Podstawą takiej decyzji będzie wniosek Ministra Spraw Wewnętrznych lub Plan użycia Sił Zbrojnych RP w sytuacjach kryzysowych.

3. Skierowanie do działania sposobem alarmowym może nastąpić podczas gwałtownego rozwoju sytuacji kryzysowej o lokalnym zasięgu. Polega na tym, że dowódca jednostki wojskowej (w szczególnych przypadkach) samodzielnie podejmuje decyzję o przystąpieniu do akcji, następnie melduje o powyższym fakcie bezpośredniemu przełożonemu [Kuśmierek 2014].

Użycie oddziałów Sił Zbrojnych w sytuacji kryzysowej nie może zagrozić ich zdolności do realizacji zadań wynikających z Konstytucji Rzeczypospolitej Polskiej i ratyfikowanych umów międzynarodowych. Zakres zadań dla Sił Zbrojnych w sytuacjach kryzysowych w tym samym układzie zawiera podstawowy dokument normatywny – Ustawa o zarządzaniu kryzysowym [Dz. U. z 2019 r. poz. 1398, t. j., art. 25, ust. 3]. Z przedstawionych zadań wynika, iż system zarządzania kryzysowego w Polsce obejmuje wyłącznie kwestie zagrożeń niemilitarnych, a w praktyce skupia się na ratownictwie i ochronie ludności. Odpowiedni system w wielu krajach, w tym system NATO-wski, traktuje zaś zarządzanie kryzysowe znacznie szerzej. Obejmuje swoim obszarem zainteresowania całokształt zagrożeń, w tym również te o charakterze polityczno-militarnym. Pomimo tych różnic, z uwagi na nasze członkostwo w NATO i Unii Europejskiej, Krajowy System Zarządzania Kryzysowego powinien sprostać zagrożeniom bezpieczeństwa na terytorium kraju oraz poza jego granicami (w ramach Art. 5 Traktatu Waszyngtońskiego). Wiąże się to z wdrażaniem rozwiązań obowiązujących w tych organizacjach w celu uzyskania kompatybilności z Systemem Reagowania Kryzysowego NATO (*NATO Crisis Response System – NCRS*). Aby sprostać tym wymaganiom, w przeciwdziałaniu zagrożeniom niemilitarnym oraz w usuwaniu skutków klęsk żywiołowych i katastrof SZ RP powinny być w gotowości do użycia wyspecjalizowanych sił i środków. Skala zadań dla sił zbrojnych w tej dziedzinie ciągle wzrasta. Istotny i stały charakter zadań ratowniczych dla wojska wymaga od niego ciągłego dostosowywania liczby, struktury, dyslokacji, wyposażenia i wyszkolenia części jednostek wojskowych do potrzeb ratowniczych. Znaczącą rolę we wspieraniu niemilitarnych elementów w sytuacjach kryzysowych odgrywają wojska inżynieryjne, szczególnie w akcjach ratowniczych oraz usuwaniu

skutków klęsk żywiołowych i katastrof. Ich głównym atutem jest zdolność niesienia natychmiastowej pomocy społeczeństwu w sytuacjach, gdy zagrożone jest życie i zdrowie ludzkie. W okresie pokoju utrzymują cześć sił i środków w gotowości do użycia w akcjach ratowniczych i ewakuacyjnych. Po ich zakończeniu mogą realizować odbudowę obiektów drogowych i mostowych. Pododdziały saperów można także wykorzystać do prac wyburzeniowych podczas porządkowania terenów dotkniętych klęską żywiołową. W celu zwiększenia zdolności wojsk inżynieryjnych, w 2012 roku rozpoczęto tworzenie Wojskowych Jednostek Odbudowy (WJO). Są to nieetatowe struktury zadaniowe w jednostkach inżynieryjnych, przeznaczone do wykonywania specjalistycznych usług wojskowych oraz realizacji zadań w zakresie usuwania skutków sytuacji kryzysowych, zgodnie z ich przygotowaniem specjalistycznym w zakresie inżynierii wojskowej. Przygotowane i wyposażone stosownie do udziału w konkretnej sytuacji kryzysowej czy też specjalistycznej usługi wojskowej. W latach 2013–14 zostało utworzonych dziesięć nieetatowych Wojskowych Jednostek Odbudowy na bazie istniejących jednostek inżynieryjnych. Utworzenie WJO pozwala zwiększyć możliwości ewakuacyjne oraz odbudowy infrastruktury drogowo-mostowej, zdolności likwidacji skutków katastrof komunikacyjnych, budowlanych, huraganów i nawałnic, zapewnienie mobilności oraz usamodzielnienie wyspecjalizowanych pododdziałów w realizacji zadań. WJO otrzymały dodatkowe łodzie hybrydowe, zestawy narzędzi pneumatycznych, mosty składane, generatory elektryczne dużej mocy, samochody transportowe (w tym wielotonażowe) i zestawy niskopodwoziowe. Łącznie we wszystkich dziesięciu WJO około 1,2 tys. stanowisk oraz ponad 900 egzemplarzy sprzętu[1].

Innym rodzajem wojsk, odgrywającym istotną rolę we wsparciu układu pozamilitarnego, są wojska chemiczne. Do ich zadań należy uczestnictwo w monitoringu zmian zachodzących w sytuacji chemicznej i radiologicznej w określonym obszarze (okręgu, regionu, kraju), utrzymywanie w gotowości do użycia i wydzielanie do akcji ratowniczej, chemicznych i radiacyjnych zespołów awaryjnych (ChRZA), współdziałanie z jednostkami ratowniczymi w usuwaniu skutków awarii chemicznych, wypadków radiacyjnych i zagrożeń epidemiologicznych (np. po powodziach).

Oprócz wyspecjalizowanych formacji w sytuacjach kryzysowych, szczególnie klęsk żywiołowych, dużą rolę odgrywa szybkość w podejmowanych działaniach i orientacja w sytuacji. Nową jakość w tym zakresie i silne wsparcie społeczności

[1] WJO nie są jednostkami nowo sformowanymi. Zasada ich tworzenia polega na przeszkoleniu w drugiej (i kolejnej) specjalności oraz doposażeniu w dodatkowy sprzęt.
Wg danych resortu ON wydatkowano na ten cel ponad 160 mln PLN.

cywilnej może przynieść, a w zasadzie już przynosi, nowy rodzaj wojsk – Wojska Obrony Terytorialnej (WOT).

Podpisana 25 kwietnia 2016 roku przez Ministra Obrony Narodowej, Antoniego Macierewicza, Koncepcja utworzenia wojsk obrony terytorialnej (etap I – okres 2016–2017), zakończyła prowadzone na różnych poziomach polityczno-wojskowych dyskusje co do potrzeby i kształtu WOT. Do najważniejszych zadań piątego rodzaju sił zbrojnych zaliczono:

1. prowadzenie działań zbrojnych we współdziałaniu z wojskami operacyjnymi,
2. ochronę ludności przed skutkami klęsk żywiołowych,
3. udział w realizacji przedsięwzięć z zakresu zarządzania kryzysowego,
4. współpracę z elementami systemu obronnego państwa, w szczególności z administracją rządową i organami samorządu terytorialnego,
5. ochronę społeczeństwa przed skutkami dezinformacji i destabilizacji sytuacji w państwie,
6. propagowanie idei wychowania patriotycznego w społeczeństwie [Ministerstwo Obrony Narodowej 2017, *Zadania WOT*].

Z dniem 1 stycznia 2017 roku weszła w życie Ustawa z dnia 16 listopada 2016 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw, wprowadzająca piąty rodzaj sił zbrojnych – Wojska Obrony Terytorialnej oraz terytorialną służbę wojskową jako formę czynnej służby wojskowej. Ustawodawca określił następujące zadania, które postawił Dowódcy WOT [Ustawa z dnia 16 listopada 2016 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw, Dz. U. z 2016 r., poz. 2138, Art. 11c]:

„1. Dowódca Wojsk Obrony Terytorialnej jest właściwy w zakresie dowodzenia jednostkami wojskowymi i związkami organizacyjnymi Wojsk Obrony Terytorialnej.

2. Do zakresu działania Dowódcy Wojsk Obrony Terytorialnej należy w szczególności:

1) realizacja programów rozwoju Sił Zbrojnych;

2) planowanie, organizowanie i prowadzenie szkolenia podległych jednostek wojskowych i związków organizacyjnych;

3) planowanie oraz organizowanie mobilizacyjnego i operacyjnego rozwinięcia oraz użycia Wojsk Obrony Terytorialnej;

4) przygotowanie sił i środków Wojsk Obrony Terytorialnej do działań bojowych;

5) wykonywanie zadań związanych z udziałem oddziałów i pododdziałów Wojsk Obrony Terytorialnej w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, ochrony mienia, akcjach poszukiwawczych oraz ratowania lub ochrony zdrowia i życia ludzkiego, a także udziału w realizacji zadań z zakresu zarządzania kryzysowego;
6) współpraca z innymi organami i podmiotami w sprawach związanych z obronnością państwa;
7) zarządzanie i przeprowadzanie kontroli podległych jednostek wojskowych i związków organizacyjnych na zasadach i w trybie określonych w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej [Dz. U. poz. 1092]".

Zarówno w koncepcji (pkt 3 i 4), jak i w ustawie (pkt 5), przewidziano zaangażowanie WOT w przedsięwzięcia z zakresu zadań funkcjonującego systemu zarządzania kryzysowego. Naturalnym jest, że w opracowywaniu wojskowych dokumentów normatywnych (doktrynalnych) precyzuje się i rozwija zadania z tego zakresu. Podstawowy dokument doktrynalnym dla WOT to *Wojska Obrony Terytorialnej w operacji (DD-3.40)* [Ministerstwo Obrony Narodowej 2018].

W rozdziale drugim, przedstawiającym WOT w systemie obronnym państwa, przełożeni określają, że „Celem działań OT jest współuczestniczenie w powszechnym przygotowaniu oraz wykorzystaniu sił i środków znajdujących się w dyspozycji państwa na szczeblu samorządu terytorialnego (zasobów ludzkich i materialnych, infrastruktury, terenu itp.) do zapobiegania i przeciwdziałania wszelkiego rodzaju zagrożeniom o charakterze militarnym i niemilitarnym oraz katastrofom naturalnym i cywilizacyjnym oraz pomoc w usuwaniu ich skutków" [Ministerstwo Obrony Narodowej 2018, s. 10]. W kolejnym rozdziale, określając cele dla WOT, podkreślono ich przeznaczenie do realizacji zadań z zakresu wsparcia zarządzania (reagowania) kryzysowego. Prawodawca przewiduje udział w tych przedsięwzięciach w stanie stałej gotowości obronnej państwa, a konkretne zadanie brzmi: „ wspieranie lokalnych społeczności i elementów podsystemu niemilitarnego w realizacji zadań zarządzania (reagowania) kryzysowego, tj. osiągnięcia gotowości oraz udziału w niezwłocznym i powszechnym reagowaniu na sytuację zagrożenia o charakterze niemilitarnym w celu zapobieżenia lub przeciwdziałania mu, minimalizacji i usuwania jego skutków, a także przywracania stanu sprzed jego wystąpienia" [Ministerstwo Obrony Narodowej 2018, s. 14].

Załącznik A dokumentu DD-3.40, *Zakres działań na poziomie taktycznym Wojsk Obrony Terytorialnej*, w części *Działania na rzecz władz cywilnych* precyzuje konkretne działania, do których zalicza:

- Współudział w zwalczaniu katastrof naturalnych i cywilizacyjnych oraz ich skutków;
- Współudział w monitorowaniu zagrożeń;
- Wykonywanie zadań związanych z oceną skutków zjawisk zaistniałych na obszarze występowania zagrożeń;
- Wsparcie zadań poszukiwawczo-ratowniczych;
- Ewakuacja poszkodowanej ludności i mienia;
- Współudział w przygotowaniu warunków do czasowego przebywania ewakuowanej ludności w wyznaczonych miejscach;
- Współudział w ochronie pozostawionego mienia na obszarze występowania zagrożeń;
- Izolowanie obszaru występowania zagrożeń lub miejsca prowadzenia akcji ratowniczej;
- Wykonywanie prac zabezpieczających, ratowniczych i ewakuacyjnych przy zagrożonych obiektach budowlanych;
- Prowadzenie prac wymagających specjalistycznego sprzętu lub materiałów wybuchowych będących w zasobach Sił Zbrojnych RP;
- Usuwanie materiałów niebezpiecznych i ich unieszkodliwianie z wykorzystaniem sił i środków będących na wyposażeniu Sił Zbrojnych RP;
- Wykonywanie zadań związanych z naprawą i odbudową infrastruktury technicznej;
- Współudział w zapewnieniu przejezdności szlaków komunikacyjnych;
- Udzielanie pomocy medycznej i wykonywanie zadań sanitarnohigienicznych i przeciwepidemicznych;
- Wsparcie Policji w sytuacji wystąpienia zagrożenia bezpieczeństwa i porządku publicznego [Ministerstwo Obrony Narodowej 2018][2].

Przedstawiony zakres zadań jest bardzo szeroki i o wysokim poziomie ogólności. W punkcie np. mówiącym o przejezdności szlaków komunikacyjnych nie jest sprecyzowane, czy dotyczy to budowy lub naprawy dróg, mostów itp., czy realizacji zadań z zakresu regulacji ruchu. Gdy poddamy analizie struktury WOT, nie wydaje się możliwe osiągnięcie zdolności do szybkiej realizacji zadań z zakresu

[2] Siły i środki Wojsk Obrony Terytorialnej od jesieni 2018 r. są włączone do systemu zarządzania kryzysowego resortu obrony narodowej. Procedura ich uruchomienia jest taka sama jak w przypadku innych rodzajów sił zbrojnych i jest realizowana zgodnie z Ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a wydzielone siły są przekazane w podporządkowanie Dowództwa Operacyjnego RSZ [Polska Zbrojna online, 2018, http://polska-zbrojna.pl/home/articleshow/26551?t=-Parasol-WOT-u# dostęp: 27.10.2019].

przeznaczonego dla wojsk inżynieryjnych, chemicznych, służby zdrowia. Autorzy nie podważają tu sensu tych zadań, a same działania ze strony WOT (wszystkich szczebli) pokazują, że są one traktowane poważnie. Dowodem na to jest szereg przedsięwzięć z zakresu szkolenia, logistyki i konkretne akcje. Przykłady:

- 30 żołnierzy WOT z trzynastu brygad OT oraz Centrum Szkolenia WOT w okresie 15.07–02.08.2019 r. w Szkole Specjalistów Pożarnictwa na terenie Centrum Szkolenia Logistyki w Grudziądzu szkoliło się z zakresu ratownictwa w czasie akcji ratowniczo–gaśniczych[3].

  Żołnierze z 3. Podkarpackiej Brygady Obrony Terytorialnej wzięli udział w ćwiczeniach z reagowania kryzysowego w dniu 25.10.2019 roku. Szkolenie zakładało katastrofę samolotu, a uczestniczyły w nim również straż pożarna, OSP i policja. Zakres ćwiczenia obejmował lokalizację miejsca katastrofy statku powietrznego, gaszenie pożaru i prowadzenie akcji ratowniczej po awarii i upadku samolotu w kompleksie leśnym oraz transport poszkodowanych w bardzo trudnych warunkach terenowych. W jednym z epizodów akcji udział wzięli żołnierze z 34. Batalionu Lekkiej Piechoty z Jarosławia, a dotyczył on informowania społeczności lokalnej o zagrożeniu i potrzebie ewakuacji po wyznaczonych drogach [Rzeszów. Eska–info 2019, MSPO 2019, Zarządzanie kryzysowe tematem stoiska WOT na targach obronnych, https://www.se.pl/rzeszow/katastrofa-lotnicza-powiat-przeworski-2019-cwiczenia-sluzb-na-wypadek-sytuacji-kryzysowej-zdjecia-aa-8gG8-yaLX-87Q3.html, dostęp: 29.10.2019].
- Tematem przewodnim tegorocznego (2019 r.) stoiska Wojsk Obrony Terytorialnej podczas Międzynarodowego Salonu Przemysłu Obronnego (MSPO) w Kielcach było zarządzanie kryzysowe. Żołnierze WOT są formacją często kierowaną do poszukiwań osób zaginionych i do pomocy ludności cywilnej w przypadku klęsk żywiołowych. Na MSPO zaprezentowano szeroką gamę sprzętu i wyposażenia, będącą w użytkowaniu WOT oraz oferowanego do nabycia [Info Security 24 2019, MSPO 2019: Zarządzanie kryzysowe tematem stoiska WOT na targach obronnych, https://www.infosecurity24.pl/mspo-2019-zarzadzanie-kryzysowe-tematem-stoiska-wot-na-targach-obronnych, dostęp: 29.10.2019].

[3] Dowódca WOT gen. dyw. Wiesław Kukuła: „Przeprowadzone szkolenie w istotny sposób przyczynia się do budowy kompetencji żołnierzy OT w zakresie prowadzenia działań gaśniczych i ratowniczych. Kompetencje te nie tylko wzmacniają potencjał Sił Zbrojnych, ale również czynią silniejszymi i bezpieczniejszymi lokalne społeczności. Są klasycznym przykładem kwalifikacji i zdolności podwójnego zastosowania niezbędnych dla obywateli-żołnierzy wchodzących w skład najmłodszego rodzaju sił zbrojnych. [https://media.terytorialsi.wp.mil.pl/informacje/454230/szkolenie-kryzysowe-terytorialsow, dostęp: 29.10.2019].

• Sprawdzianem dla WOT w 2019 roku były prowadzone od 21 do 28 maja przez tę formację działania przeciwpowodziowe i usuwania skutków trąby powietrznej. Podczas tych działań 1440 żołnierzy WOT wspierało lokalne społeczności, terenowe organy administracji państwowej i publicznej oraz służby ratownicze, w szczególności: Państwową i Ochotniczą Straż Pożarną. Zdecydowaną większość żołnierzy WOT stanowili żołnierze ochotnicy, których było 1179. Działania prowadzono na Lubelszczyźnie, gdzie usuwano skutki trąby powietrznej. Jednocześnie na skutek długotrwałych i intensywnych opadów na południu kraju zaczęły wylewać rzeki. Z wnioskami do Ministra Obrony Narodowej o wsparcie wojska w usuwaniu skutków powodzi wystąpili wojewodowie: podkarpacki, małopolski, śląski oraz świętokrzyski. Formacje WOT użyły do niesienia pomocy: 66 ciężarówek, 14 samochodów osobowo-terenowych, dwóch quadów, dwóch samochodów sanitarnych, łodzi z silnikiem zaburtowym, 21 agregatów prądotwórczych, 12 zestawów oświetleniowych oraz dodatkowego, drobnego sprzętu inżynieryjno-saperskiego, takiego jak: piły spalinowe i kombinezony do długotrwałej pracy w wodzie[4].

Prezentowane przykłady ilustrują pewne ukierunkowywanie WOT w stronę działań z zakresu zarządzania kryzysowego. Przywiązanie do terenu[5] powoduje, że np. działająca w powiecie kompania lekkiej piechoty (ok. stu żołnierzy) nie będzie

[4] Rzecznik WOT, ppłk Pietrzak, wyjaśnił, że udział WOT w działaniach przeciwpowodziowych i usuwania skutków trąby powietrznej był pierwszym praktycznym sprawdzianem dla tej formacji. Do głównych zadań żołnierzy WOT należało: wsparcie służb ratowniczych w zapewnieniu przejezdności dróg, usuwanie powalonych drzew na terenach posesji, zabezpieczenie dostaw energii elektrycznej gospodarstw i instytucji oraz oświetlenie rejonu prowadzenia działań ratowniczych. A także wzmacnianie wałów przeciwpowodziowych, zabezpieczanie osunięć, przygotowanie i transport materiałów przeciwpowodziowych, wypompowywanie wody i oświetlanie rejonów działań [https://www.infosecurity24.pl/kryzysowa-pomoc-1440-zolnierzy-wot, dostęp: 29.10.2019].

[5] Potwierdzeniem jest odpowiedź sekretarza stanu w Ministerstwie Obrony Narodowej, Wojciecha Skurkiewicza, na interpelację poselską nr 15446 – „Jeśli chodzi o udział żołnierzy Wojsk Obrony Terytorialnej (WOT) w omawianych działaniach, to pragnę wyjaśnić, że zadania Wojsk Obrony Terytorialnej są określone w ustawie z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej [Dz. U. z 2017 r., poz. 1430 ze zm.]. Art. 11c tej ustawy wskazuje m.in., że do zadań WOT należy zwalczanie klęsk żywiołowych i likwidacji ich skutków, ochrona mienia, udział w akcjach poszukiwawczych i ratowniczych, ochrona zdrowia i życia ludzkiego oraz udział w realizacji zadań z zakresu zarządzania kryzysowego. Misją WOT jest obrona i wspieranie lokalnych społeczności, co – zgodnie z ww. artykułem – w czasie pokoju będzie realizowane właśnie w formie przeciwdziałania czy też ograniczania skutków kataklizmów i katastrof. Jednakże, należy mieć na uwadze podstawową zasadę, jaka przyświeca tworzeniu WOT. Jest to zasada terytorialności, w myśl której żołnierze WOT będą realizować swoje zadania w tzw. Stałych Rejonach Odpowiedzialności (SRO), które dla brygad będą odpowiadały obszarom województw (brygada OT – województwo, batalion – 3-5 powiatów, kompania – powiat) [http://www.sejm.gov.pl/sejm8.nsf/InterpelacjaTresc.xsp?key=19E3D401, dostęp: 27.10.2019].

znaczącą siłą w dużych akcjach (przeciwpowodziowe, śnieżyce), ale na ograniczonym terenie (katastrofy, awarie) oraz w akcjach poszukiwawczo-ratowniczych (atut znajomość ludzi i terenu) jej znaczenie wzrasta. Dotyczy to szczególnie rejonów, gdzie nie stacjonują jednostki operacyjne SZ RP. Masowe użycie wojsk w sytuacjach kryzysowych następuje przy zagrożeniach na dużą skalę, natomiast dla zarządzających Systemem Zarządzania Kryzysowego istotne są elementy wysoko specjalistyczne, jak:

- Jednostki Inżynieryjne;
- Zespoły Rozpoznania Biologicznego;
- Chemiczno-Radiacyjne Zespoły Awaryjne;
- Grupy Ratownictwa Lotniczego;
- Grup Naziemnego Poszukiwania;
- Patrole Rozminowania.

Planowanie i udział Sił Zbrojnych RP w przedsięwzięciach z zakresu zarządzania kryzysowego

Podstawą udziału Sił Zbrojnych RP w przedsięwzięciach z zakresu zarządzania kryzysowego jest Ustawa o zarządzaniu kryzysowym, która w Art.7.1 określa, że na terenie Rzeczypospolitej Polskiej zarządzanie kryzysowe sprawuje Rada Ministrów, natomiast przy niej tworzy się Rządowy Zespół Zarządzania Kryzysowego (Art. 8.1), jako organ opiniodawczo-doradczy właściwy w sprawach inicjowania i koordynowania działań podejmowanych w zakresie zarządzania kryzysowego. Prezes Rady Ministrów jest przewodniczącym, natomiast Minister Obrony Narodowej i minister właściwy do spraw wewnętrznych – zastępcami przewodniczącego. Na potrzeby zarządzania kryzysowego w Resorcie Obrony Narodowej (RON) stworzony jest Zespół Zarządzania Kryzysowego Ministra Obrony Narodowej, zwany dalej „Zespołem". Zespół jest organem opiniodawczo-doradczym Ministra Obrony Narodowej w sprawach realizacji zadań z zakresu zarządzania kryzysowego.

W skład Zespołu wchodzą:

1. przewodniczący – Minister Obrony Narodowej;

2. zastępcy przewodniczącego – Sekretarz Stanu w Ministerstwie Obrony Narodowej, upoważniony przez przewodniczącego Zespołu oraz Szef Sztabu Generalnego WP;

3. sekretarz – Szef Sztabu Dowództwa Operacyjnego Rodzajów Sił Zbrojnych;
4. członkowie:
   a) sekretarze i podsekretarze stanu w Ministerstwie Obrony Narodowej,
   b) Dyrektor Generalny Ministerstwa Obrony Narodowej,
   c) Dowódca Operacyjny Rodzajów Sił Zbrojnych,
   d) Dowódca Wojsk Obrony Terytorialnej,
   e) Komendant Główny Żandarmerii Wojskowej,
   f) Szef Służby Kontrwywiadu Wojskowego,
   g) Szef Służby Wywiadu Wojskowego,
   h) Szef Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego Ministra Obrony Narodowej (CSIRT MON),
   i) Dowódca Garnizonu Warszawa,
   j) Dyrektor Centrum Operacyjnego Ministra Obrony Narodowej [Zarządzenie Nr 7/MON Ministra Obrony Narodowej z dnia 21 marca 2019 r. w sprawie organizacji, składu oraz miejsca i trybu pracy Zespołu Zarządzania Kryzysowego Ministra Obrony Narodowej, Dz. Urz. MON z dnia 25 marca 2019 r. Poz. 51].

Organem wykonawczym Ministra Obrony Narodowej w zakresie zarządzania kryzysowego w rozumieniu ustawy o ZK jest Dowództwo Operacyjne Rodzajów Sił Zbrojnych (zgodnie z Ustawą o zarządzaniu kryzysowym nie ma konieczności powoływania odrębnej instytucji). Do końca 2013 r. funkcjonowało Centrum Zarządzania Kryzysowego Ministerstwa Obrony Narodowej. Powołane decyzją nr 245/MON Ministra Obrony Narodowej z 7 lipca 2010 r. Centrum realizowało w resorcie obrony narodowej zadania określone w art. 13 ust. 2 Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, a ponadto do jego właściwości należały:

1. obsługa prac Zespołu Zarządzania Kryzysowego w Ministerstwie Obrony Narodowej pod względem merytorycznym, techniczno-organizacyjnym oraz ochrony informacji niejawnych i obsługi kancelaryjnej;
2. planowanie i koordynowanie użycia Sił Zbrojnych Rzeczypospolitej Polskiej w sytuacjach kryzysowych;
3. opracowywanie projektów dokumentów normatywnych Ministra Obrony Narodowej oraz monitorowanie realizacji zadań z zakresu zarządzania kryzysowego przez jednostki i komórki organizacyjne resortu obrony narodowej;
4. monitorowanie działalności szkoleniowo-operacyjnej wojsk, uczestniczenie w systemie meldowania o wypadkach i rażących naruszeniach dyscypliny wojskowej oraz uruchamianie procedur w zakresie aktywowania sił i środków wydzielanych z Sił Zbrojnych Rzeczypospolitej Polskiej w sytuacjach kryzysowych;

5. zapewnienie wymiany informacji z wojskowymi strukturami dowodzenia oraz zarządzania kryzysowego Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej [Decyzja Nr 245/MON Ministra Obrony Narodowej z dnia 7 lipca 2010 r. w sprawie utworzenia Centrum Zarządzania Kryzysowego Ministerstwa Obrony Narodowej, Dz. Urz. MON z 2010 r. Nr 14, Poz. 183].

Zasadniczym dokumentem planistycznym, sporządzanym na szczeblu strategicznym, regulującym kwestie użycia oddziałów i pododdziałów Sił Zbrojnych RP w sytuacjach kryzysowych jest *Plan zarządzania kryzysowego Ministerstwa Obrony Narodowej,* w którym określa się gotowość sił i środków, procedury aktywacji, organizację systemu dowodzenia i łączności, zasady koordynacji oraz organizację zabezpieczenia logistycznego i medycznego. Ujęto w nim także zasoby, które mogą zostać wykorzystane na potrzeby zarządzania kryzysowego. Na potrzeby konkretyzacji realizowanych przedsięwzięć w planie zawarto załączniki, które w zasadzie stanowią odrębne plany wsparcia władz cywilnych i społeczeństwa. Wykaz załączników do *Planu zarządzania kryzysowego MON* przedstawia się następująco:

- Załącznik nr 1 – Użycie Sił Zbrojnych RP w działaniach antyterrorystycznych i utrzymania porządku publicznego;
- Załącznik nr 2 – Użycie Sił Zbrojnych RP w izolacji obszaru zagrożenia oraz działaniach zabezpieczenia, ratowania życia i zdrowia oraz ewakuacji przy zagrożonych obiektach budowlanych i zabytkach;
- Załącznik nr 3 – Użycie Sił Zbrojnych RP w akcjach o charakterze poszukiwawczo- ratowniczym;
- Załącznik nr 4 – Użycie Sił Zbrojnych RP w sytuacjach wymagających użycia specjalistycznego sprzętu, a także oczyszczania terenu z przedmiotów wybuchowych i niebezpiecznych pochodzenia wojskowego oraz ich unieszkodliwianie;
- Załącznik nr 5 – Użycie Sił Zbrojnych RP w monitorowaniu i ocenie skutków zagrożeń niemilitarnych;
- Załącznik nr 6 – Użycie Sił Zbrojnych RP w likwidacji skażeń chemicznych i promieniotwórczych;
- Załącznik nr 7 – Użycie Sił Zbrojnych RP odbudowie oraz naprawach zniszczonej infrastruktury technicznej oraz zapewnieniu drożności szlaków komunikacyjnych;
- Załącznik nr 8 – Użycie Sił Zbrojnych RP w działaniach przeciwepidemicznych, sanitarno-higienicznych, udzielaniu pomocy medycznej oraz likwidowaniu skażeń i zakażeń biologicznych.
- Załącznik nr 9 – Użycie Sił Zbrojnych RP w ewakuacji ludności i mienia oraz ochronie terenu podczas zagrożeń niemilitarnych.

• Załącznik nr 10 – Ochrona i zabezpieczenie obiektów infrastruktury krytycznej użytkowanych przez MON [Użycie Sił Zbrojnych RP do wsparcia administracji publicznej w sytuacjach kryzysowych, https://docplayer.pl/7411486-Uzycie-sil-zbrojnych-rp-do-wsparcia-administracji-publicznej-w-sytuacjach-kryzysowych.html, dostęp: 27.10.2019].

W planach szczegółowych w pierwszej kolejności wzięto pod uwagę kwestie uregulowań prawnych w zakresie możliwości udziału wojska w poszczególnych sytuacjach kryzysowych, a następnie zawarto szczegółową charakterystykę zagrożenia, wykaz realizowanych zadań, procedury aktywizacji dostępnych sił i środków oraz zasady współdziałania wojska z innymi podmiotami. Oddziały Sił Zbrojnych mogą być przekazane do dyspozycji wojewody w składzie etatowym albo jako tworzone doraźnie zgrupowania zadaniowe. Zadania dla oddziałów wojskowych kierujący akcją przekazują wyłącznie ich dowódcom, którzy wydają podwładnym rozkazy określające sposób ich realizacji. Dowodzenie oddziałami Sił Zbrojnych odbywa się na zasadach określonych w regulaminach wojskowych i według procedur obowiązujących w Siłach Zbrojnych Rzeczypospolitej Polskiej [Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad pododdziałów i oddziałów SZ RP w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu, Dz. U. z 2003 r. Nr 41 poz. 347, art. 4, 5, 6]. Koordynatorem działań w terenie (województwie) są Wojewódzkie Sztaby Wojskowe (WSzW), do których w tym zakresie należą:

• współdziałanie z wojewodą w zakresie planowania użycia wojska w sytuacjach kryzysowych, a także koordynowanie użycia wydzielonych sił i środków SZ RP do realizacji zadań wsparcia układu niemilitarnego w sytuacji wystąpienia klęsk i katastrof, w tym uzgadnianie przedsięwzięć związanych z ich przemieszczeniem w rejon działań i zabezpieczeniem logistycznym;
• udział w posiedzeniach WZZK i przedstawianie wojewodzie propozycji rozwiązań, adekwatnie do istniejącej sytuacji kryzysowej;
• współdziałanie w zakresie udziału sił i środków resortu obrony narodowej w ćwiczeniach z zakresu zarządzania kryzysowego organizowanych na terenie województwa;
• współpraca z organami administracji publicznej szczebla wojewódzkiego, służbami, jednostkami i instytucjami wojskowymi na administrowanym terenie w zakresie monitorowania, oceny i przekazywania informacji o zagrożeniach;
• informowanie DO RSZ o zgłoszonych przez wojewodę potrzebach w zakresie użycia sił i środków do realizacji zadań zarządzania kryzysowego na terenie województwa;

- udział w rekonesansach zagrożonych rejonów oraz prowadzenie bazy danych i przekazywanie informacji o sytuacji kryzysowej [Rozporządzenie Ministra Obrony Narodowej z dnia 24 lutego 2017 r. w sprawie wojewódzkich sztabów wojskowych i wojskowych komend uzupełnień, Dz. U. z 2017 r. poz. 626].

Zaangażowanie SZ RP w realizację zadań przewidzianych dla wojska w obszarze zarządzania kryzysowego w znacznej mierze wynika z:

- wielkiej przydatności organizacji wojskowej (dyspozycyjność, zdyscyplinowanie, mobilność przestrzennej lokalizacji);
- wciąż wzrastającej skali zagrożeń niemilitarnych (współcześnie tego typu zagrożenia są równie groźne, jak wojny i ich skutki);
- niewydolności organizacyjnej i wykonawczej, zwłaszcza w sytuacjach szczególnych zagrożeń, stałych służb cywilnych, a także niedostatecznego przygotowania do sprostania nagłemu wzrostowi potrzeb ratowniczych, ochronnych, logistycznych, inżynieryjnych i innych w trybie natychmiastowym. Oznacza to, że w sytuacjach szczególnych zagrożeń i potrzeb zachodzi wręcz konieczność wsparcia wojskowego [Sobolewski 2013, s. 112].

Działania SZ w sytuacjach kryzysowych, wymagających użycia siły

Zarządzanie kryzysowe zajmuje się nie tylko problematyką zagrożeń naturalnych, klęsk żywiołowych i katastrof, ale również specyficznymi sytuacjami, które zagrażają nie tylko bezpieczeństwo obywateli – zagrażają bezpieczeństwu państwa. Do ich neutralizacji ustawodawca przewidział policję, a w wyjątkowych sytuacjach także siły zbrojne.

W przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego zagrożenia terrorystycznego, jeżeli użycie oddziałów i pododdziałów Policji okaże się niewystarczające lub może okazać się niewystarczające, do pomocy mogą być użyte oddziały i pododdziały Sił Zbrojnych Rzeczypospolitej Polskiej, stosownie do ich przygotowania specjalistycznego, posiadanego sprzętu i uzbrojenia oraz zaistniałych potrzeb. Przygotowanie do użycia Sił Zbrojnych Rzeczypospolitej Polskiej, w szczególności rozpoczęcie planowania, pozyskiwania informacji i współpracy z organami administracji publicznej, może nastąpić po wprowadzeniu trzeciego lub czwartego stopnia alarmowego i przed wydaniem decyzji o ich użyciu. Decyzję o użyciu Sił Zbrojnych Rzeczypospolitej Polskiej, niepodlegającą ogłoszeniu, wydaje Minister Obrony Narodowej, na wniosek ministra właściwego do spraw wewnętrznych, określając:

1. skład oddziałów i pododdziałów, które mają być użyte do pomocy, oraz ich zadania i liczebność;
2. obszar, na jakim oddziały i pododdziały, które mają być użyte do pomocy, będą wykonywały zadania oraz czas ich wykonywania;
3. ewentualne ograniczenia, dotyczące użycia posiadanych środków własnych będących w wyposażeniu oddziałów i pododdziałów, które mają być użyte do pomocy.

Minister Obrony Narodowej informuje niezwłocznie Prezydenta Rzeczypospolitej Polskiej i Prezesa Rady Ministrów o wydaniu decyzji. Prezydent Rzeczypospolitej Polskiej może wydać postanowienie o zmianie lub uchyleniu decyzji, o której mowa w ust. 3. Oddziały i pododdziały Sił Zbrojnych Rzeczypospolitej Polskiej, użyte do pomocy oddziałom lub pododdziałom Policji, mogą użyć i wykorzystać środki przymusu bezpośredniego i broń palną na zasadach przewidzianych dla żołnierzy Żandarmerii Wojskowej [Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz. U. z 2019 r. poz. 796, t. j., art. 22]. Oddziały i pododdziały Wojsk Specjalnych, użyte do pomocy oddziałom lub pododdziałom Policji mogą użyć i wykorzystać w działaniach kontrterrorystycznych środki przymusu bezpośredniego i broń palną w sposób przewidziany w art. 3 ust. 2a Ustawy z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, z zastrzeżeniem dopuszczalności użycia broni palnej w przypadkach określonych w art. 23 ust. 1 [Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych, Dz. U. z 2019 r. poz. 796, t. j., art. 22.7]. Oddziały lub pododdziały Sił Zbrojnych Rzeczypospolitej Polskiej użyte do pomocy oddziałom lub pododdziałom Policji pozostają w systemie dowodzenia Sił Zbrojnych Rzeczypospolitej Polskiej. Szczegóły współdziałania reguluje Rozporządzenie Rady Ministrów z dnia 21 lipca 2016 r. w sprawie szczegółowych warunków i sposobu organizacji współdziałania oddziałów i pododdziałów Policji z oddziałami i pododdziałami Sił Zbrojnych Rzeczypospolitej Polskiej w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego. Oddziały Sił Zbrojnych, wydzielone do pomocy oddziałom Policji, mogą być użyte do prowadzenia działań antyterrorystycznych na miejscu zdarzenia o charakterze terrorystycznym, w tym działań kontrterrorystycznych, osłony lub izolacji określonych obiektów, dróg, wydzielonych ulic lub części miast, ochrony obiektów oraz działań przywracających bezpieczeństwo i porządek publiczny. Użycie oddziałów Policji współdziałających z oddziałami Sił Zbrojnych utrwala się za pomocą urządzeń rejestrujących obraz i dźwięk [Rozporządzenie Rady Ministrów z dnia 21 lipca 2016 r. w sprawie szczegółowych warunków i sposobu organizacji współdziałania oddziałów

i pododdziałów Policji z oddziałami i pododdziałami Sił Zbrojnych Rzeczypospolitej Polskiej w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego, Dz. U. z 2016 r. poz. 1087].

Innym rodzajem współdziałania tych formacji są przedsięwzięcia z zakresu utrzymania (przywrócenia) porządku publicznego w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego, zwłaszcza poprzez sprowadzenie:

1. niebezpieczeństwa powszechnego dla życia, zdrowia lub wolności obywateli;
2. bezpośredniego zagrożenia dla mienia w znacznych rozmiarach;
3. bezpośredniego zagrożenia obiektów lub urządzeń ważnych dla bezpieczeństwa lub obronności państwa, siedzib centralnych organów państwowych albo wymiaru sprawiedliwości, obiektów gospodarki lub kultury narodowej oraz przedstawicielstw dyplomatycznych i urzędów konsularnych państw obcych albo organizacji międzynarodowych, a także obiektów dozorowanych przez uzbrojoną formację ochronną utworzoną na podstawie odrębnych przepisów;
4. zagrożenia przestępstwem o charakterze terrorystycznym, mogącym skutkować niebezpieczeństwem dla życia lub zdrowia uczestników wydarzeń o charakterze kulturalnym, sportowym lub religijnym, w tym zgromadzeń lub imprez masowych – jeżeli użycie oddziałów lub pododdziałów Policji okaże się lub może okazać się niewystarczające, do pomocy oddziałom i pododdziałom Policji mogą być użyte oddziały i pododdziały Sił Zbrojnych [Ustawa o Policji, Dz. U. z 2020 r. poz. 360, t.j.]. Użycie Sił Zbrojnych, w przypadkach, o których mowa w ust. 1, następuje na podstawie postanowienia Prezydenta Rzeczypospolitej Polskiej wydanego na wniosek Prezesa Rady Ministrów. Pomoc w takiej sytuacji może być udzielona również w formie prowadzonego samodzielnie przez oddziały i pododdziały Sił Zbrojnych przeciwdziałania zagrożeniu, w przypadku gdy oddziały i pododdziały Policji nie dysponują odpowiednimi możliwościami. Organ koordynujący wyznacza oddziałom Sił Zbrojnych Rzeczypospolitej Polskiej obszary wykonywania zadań, określa szczegółowe zadania do wykonania oraz kieruje działaniami za pośrednictwem funkcjonariuszy Policji. Właściwy dowódca oddziału Sił Zbrojnych współdziała z właściwym dowódcą oddziału Policji albo z organem koordynującym. Wsparcie logistyczne działań Policji prowadzonych z pomocą oddziałów wojska realizuje się z uwzględnieniem konieczności zachowania potencjału obronnego i gotowości bojowej Sił Zbrojnych i może obejmować w szczególności transport, wyżywienie, usługi medyczne, sprzęt specjalistyczny oraz zakwaterowanie [Rozporządzenie Rady Ministrów z dnia 22 lipca 2016 r. w sprawie użycia oddziałów i pododdziałów

Policji oraz Sił Zbrojnych Rzeczypospolitej Polskiej w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego, Dz. U. z 2016 r. poz. 1090].

Zakończenie

Skala współczesnych zagrożeń wskazuje na konieczność ciągłego podnoszenia i doskonalenia zdolności wojska do realizacji zadań związanych z ochroną społeczeństwa w przypadku klęsk żywiołowych i innych sytuacji nadzwyczajnych. W uzasadnionych przypadkach dochodzi do użycia wojska w sytuacji, gdy inne siły nie są w stanie sprostać oczekującym je zadaniom, a czasami nawet nie są w stanie ich wykonać. Specyficzna, zhierarchizowana struktura wojska, oparta na wysokim morale i dyscyplinie oraz wysokiej klasy sprzęt oraz wysoka zdolność szybkiego przystąpienia do działań powoduje, że Siły Zbrojne będą ciągle ważnym elementem w systemie zarządzania (reagowania) kryzysowego. Budowany konsekwentnie od lat system zarządzania kryzysowego i profesjonalne jego elementy, np. system ratowniczo-gaśniczy, powodują, że służby cywilne doskonale radzą sobie w trudnych sytuacjach. Wojsko jest przewidziane do udziału w przedsięwzięciach specyficznych lub w razie wystąpienia kataklizmów na skalę masową. Siły Zbrojne są przede wszystkim wyspecjalizowanym organem państwa, przeznaczonym do ochrony i obrony jego interesów, niezawisłości i integralności terytorialnej, stąd też w Krajowym Planie Zarządzania Kryzysowego odgrywają we wszystkich przewidzianych dla siebie zadaniach rolę „wspomagającego", nie „wiodącego" [Rządowe Centrum Bezpieczeństwa 2018].

Bibliografia

Decyzja Nr 245/MON Ministra Obrony Narodowej z dnia 7 lipca 2010 r. w sprawie utworzenia Centrum Zarządzania Kryzysowego Ministerstwa Obrony Narodowej, Dz. Urz. MON.2010.14.183.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 roku, Art.26.1., Dz. U. z 1997 r. Nr 78, poz. 483, z 2001 r. Nr 28, poz. 319, z 2006 r. Nr 200, poz. 1471, z 2009 r., Nr 114, poz. 946.

Kryzysowa pomoc 1440 żołnierzy WOT, https://www.infosecurity24.pl/kryzysowa-pomoc-1440-zolnierzy-wot, dostęp: 29.10.2019.

Kuśmierek Z. (2014), *Udział wojska w sytuacjach kryzysowych*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy", nr 10(1).

Ministerstwo Obrony Narodowej (2017), *Zadania WOT*, https://www.gov.pl/web/obrona-narodowa/zadania-wot, dostęp: 26.10.2019.

Ministerstwo Obrony Narodowej (2018), *Wojska Obrony Terytorialnej w operacji – DD-3.40*, Warszawa.

Odpowiedź na interpelację nr 15446 w sprawie udziału Wojsk OT w walce ze skutkami nawałnic, http://www.sejm.gov.pl/sejm8.nsf/InterpelacjaTresc.xsp?key=19E3D401, dostęp: 27.10.2019.

Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad pododdziałów i oddziałów SZ RP w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu (Dz. U. z 2003 r. Nr 41 poz. 347).

Rozporządzenie Ministra Obrony Narodowej z dnia 4 marca 2010 r. w sprawie wojewódzkich sztabów wojskowych i wojskowych komend uzupełnień (Dz. U. Nr 41, poz. 242).

Rozporządzenie Rady Ministrów z dnia 22 lipca 2016 r. w sprawie użycia oddziałów i pododdziałów Policji oraz Sił Zbrojnych Rzeczypospolitej Polskiej w razie zagrożenia bezpieczeństwa publicznego lub zakłócenia porządku publicznego (Dz. U. z 2016 r. poz. 1090).

Rozporządzenie Rady Ministrów z dnia 21 lipca 2016 r. w sprawie szczegółowych warunków i sposobu organizacji współdziałania oddziałów i pododdziałów Policji z oddziałami i pododdziałami Sił Zbrojnych Rzeczypospolitej Polskiej w przypadku wprowadzenia trzeciego lub czwartego stopnia alarmowego (Dz. U. z 2016 r. poz. 1087).

Rządowe Centrum Bezpieczeństwa (2018), *Zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa*, https://rcb.gov.pl/krajowy-plan-zarzadzania-kryzysowego-gotowy-zestaw-dzialan-na-wypadek-wystapienia-sytuacji-kryzysowej/, dostęp: 25.10.2019.

Szkolenie kryzysowe terytorialsów, https://media.terytorialsi.wp.mil.pl/informacje/454230/szkolenie-kryzysowe-terytorialsow, dostęp: 29.10.2019.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2019 r. poz. 1398).

Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (t.j. Dz. U. z 2019 r. poz. 1541, 2020).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (t.j. Dz. U. z 2017 r., poz. 1897).

Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (t.j. Dz. U. z 2017 r. poz. 1928).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2020 r. poz. 360, t.j.).

Ustawa z dnia 16 listopada 2016 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz. U. z 2016 r., poz. 2138, Art. 11c).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz. U. z 2019 r. poz. 796, Art. 22).

Użycie Sił Zbrojnych RP do wsparcia administracji publicznej w sytuacjach kryzysowych, https://docplayer.pl/7411486-Uzycie-sil-zbrojnych-rp-do-wsparcia-administracji-publicznej-w-sytuacjach-kryzysowych.html, dostęp: 27.10.2019.

Zapałowski A. (2018), *Siły Zbrojne. Teoria i praktyka funkcjonowania*, Warszawa, s. 257. *Zarządzanie kryzysowe tematem stoiska WOT na targach obronnych*, https://www.infosecurity24.pl/mspo-2019-zarzadzanie-kryzysowe-tematem-stoiska-wot-na-targach-obronnych, dostęp: 29.10.2019.

Zarządzanie kryzysowe tematem stoiska WOT na targach obronnych, https://www.se.pl/rzeszow/katastrofa-lotnicza-powiat-przeworski-2019-cwiczenia-sluzb-na-wypadek-sytuacji-kryzysowej-zdjecia-aa-8gG8-yaLX-87Q3.html, dostęp: 29.10.2019.

Monika Ostrowska
m.ostrowska@onet.pl
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego,
Wydział Nauk o Bezpieczeństwie

Cezary Podlasiński
czarekpo@wp.pl
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego,
Wydział Nauk o Bezpieczeństwie

Patrole rozminowania w systemie zarządzania kryzysowego

Wstęp

Patrol rozminowania – zwany też minerskim patrolem oczyszczania – jest specjalistycznym pododdziałem wojsk inżynieryjnych przeznaczonym do rozpoznania, usuwania i niszczenia przedmiotów wybuchowych i niebezpiecznych pochodzenia wojskowego w czasie pokoju i wojny. Pomimo czasu, który upłynął od zakończenia II wojny światowej, saperzy z patroli rozminowania wciąż otrzymują w ciągu roku tysiące zgłoszeń o znalezieniu niewybuchów i porzuconej amunicji. Czasowy spadek liczby zgłoszeń nastąpił w latach 90., obecnie jednak, w związku z licznymi inwestycjami budowlanymi (dróg, autostrad i budownictwa mieszkalnego), ponownie

zwiększyła się i utrzymuje na wysokim poziomie liczba zgłoszeń o znalezieniu niewybuchów[1] i niewypałów.

W 2017 roku patrole rozminowania interweniowały 7129 razy, co daje średnią około 20 razy dziennie. Należy przy tym dodać, że późna jesień, zima i wczesna wiosna to okresy zmniejszonej aktywności patroli rozminowania, a w okresach największej aktywności każdy z nich interweniuje nawet do kilku razy dziennie. Często są to zgłoszenia pilne, które należy realizować bezzwłocznie – saperzy pracują wtedy od świtu do zmierzchu.

Powyższe ukazuje, jak istotną rolę w zapewnieniu bezpieczeństwa społeczeństwu spełniają etatowe partole rozminowania, grupy nurków, saperskich pododdziałów rozpoznania (EOR – *Explosive Ordnance Reconnaissance*), pododdziały rozminowania (EOD – *Explosive Ordnance Disposal* / IEDD – *Improvised Explosive Device Disposal*) oraz inne wyspecjalizowane pododdziały inżynieryjne dedykowane do tych zadań.

Niniejszy rozdział ma na celu przedstawienie roli, zadań oraz struktury patroli rozminowania oraz statystyki zrealizowanych zadań na przestrzeni ostatnich lat, ze szczególnym uwzględnieniem lat 2017–2018.

W niniejszym rozdziale przyjęto następującą hipotezę badawczą: patrole rozminowania realizujące zadania w ramach zapewnienia bezpieczeństwa wewnętrznego nałożone na Siły Zbrojne RP, dedykowane do neutralizacji materiałów wybuchowych i niebezpiecznych w czasie pokoju i wojny, są zasadniczym ogniwem całościowego systemu zapewnienia bezpieczeństwa obywatelom oraz infrastrukturze państwa. Szczególnie istotna rola realizowana jest przez patrole w czasie pokoju. Obecny boom budowlano-inwestycyjny realizowany w kompleksach miejskich oraz rozbudowa sieci drogowej ukazuje, jak ważna rola w zapewnieniu bezpieczeństwa społeczeństwu, jak i prowadzonym inwestycjom, przypisywana jest właśnie patrolom rozminowania.

Zakłada się, że ogromna liczba powojennych materiałów niebezpiecznych i niewybuchów oraz ukrytych pod ziemią składów amunicji z czasu II wojny światowej będzie wymagała funkcjonowania patroli rozminowania jeszcze przez długie lata, a być może nawet zwiększenia ich liczebności. Jednocześnie ocenia się, że z przybrzeżnych wód Bałtyku będzie wyłaniać się coraz więcej materiałów niebezpiecznych, które mogą być szczególnie niebezpieczne dla osób wypoczywających nad polskim morzem.

[1] Niewybuch to przedmiot wypełniony materiałem wybuchowym, w którym mimo stworzonych warunków do wybuchu nie nastąpiła przemiana potencjalnej energii chemicznej materiału kruszącego w energię chemiczną.

Nie można jednocześnie wykluczyć, że upływ czasu może mieć negatywny wpływ na pozostałości nierozpoznanych jeszcze miejsc składowania broni i pocisków lub pojemników ze środkami chemicznymi, co może sugerować konieczność utrzymywania stałego i ścisłego kontaktu patroli rozminowania z jednostkami chemicznymi mającymi zdolność likwidacji zagrożeń chemicznych.

Miejsce patroli rozminowania w zarządzaniu kryzysowym. Podstawy prawne

Zapewnienie obywatelom bezpieczeństwa w obszarze likwidacji materiałów wybuchowych i niebezpiecznych wynika z podstawowych obowiązków państwa w ramach reagowania kryzysowego w aspekcie usuwania przedmiotów wybuchowych i niebezpiecznych (PWiN). Zostało to określone w zadaniach dedykowanych Siłom Zbrojnym RP zawartych w Konstytucji RP, w Strategii Bezpieczeństwa Narodowego oraz w szeregu ustaw, rozporządzeń, wytycznych i rozkazach.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym definiuje je jako działalność organów administracji publicznej będącą elementem kierowania bezpieczeństwem narodowym. Polega to na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej [Dz. U. z 2019 r., poz. 1398].

Zasadniczą podstawą realizacji zadań dla patroli rozminowania są akty prawne, rozporządzenia, plany reagowania kryzysowego, rozkazy przełożonych oraz dokumenty doktrynalne i instrukcje, m.in.:

1. Ustawa o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, nakładająca na Siły Zbrojne RP (SZ RP) zadanie udziału w zwalczaniu klęsk żywiołowych i likwidacji ich skutków, w działaniach antyterrorystycznych, akcjach poszukiwawczych oraz ratowania życia ludzkiego, a także w oczyszczaniu terenów z materiałów wybuchowych i niebezpiecznych pochodzenia wojskowego oraz ich unieszkodliwianiu [Dz. U. z 1967 r. Nr 44, poz. 220, art. 3, ust. 2];
2. Ustawa o stanie klęski żywiołowej, nakładająca na SZ RP obowiązek utrzymywania w gotowości sił i środków do wykonywania zadań związanych z zapobieganiem skutkom klęsk żywiołowych oraz ich usuwaniem [Dz. U. z 2007 r. Nr 62, poz. 558, art. 18];

3. Ustawa o zarządzaniu kryzysowym, określająca między innymi zakres zadań zarządzania kryzysowego, w których mogą uczestniczyć oddziały i pododdziały SZ RP stosownie do ich specjalistycznego przygotowania [Dz. U. z 2002 r. Nr 82, poz. 590, art. 25, ust. 3];
4. Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad udziału pododdziałów i oddziałów SZ RP w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu [Dz. U. z 2003 r. Nr 41, poz. 347];
5. Plan Zarządzania Kryzysowego Resortu Obrony Narodowej [Plan Zarządzania…];
6. Instrukcja Oczyszczanie terenów z przedmiotów wybuchowych i niebezpiecznych [Instrukcja…];
7. Zatwierdzony przez Szefa Sztabu Generalnego WP w dniu 11 października 2012 r. Protokół z przebiegu eksploatacji próbnej informatycznego systemu sprawozdawczości i monitoringu patroli rozminowania – SI PATROL [Protokół z przebiegu…];
8. Polecenie Szefa Inspektoratu Wsparcia Sił Zbrojnych nr 64 z dnia 2 października 2014 r. w sprawie wprowadzenia do Sił Zbrojnych RP Oprogramowania informatycznego Systemu Sprawozdawczości i Monitorowania Minerskich Patroli Rozminowania – SI PATROL [Polecenie Szefa…];
9. DD (dokument doktrynalny) 4.22 - Zabezpieczenie techniczne Sił Zbrojnych Rzeczypospolitej Polskiej. Zasady funkcjonowania [DD 4.22];
10. DD 4.22.13 - Instrukcja zarządzania eksploatacją uzbrojenia i sprzętu wojskowego w Siłach Zbrojnych Rzeczypospolitej Polskiej. Zasady ogólne [DD 4.22.13].

Zadania, struktura i rozmieszczenie patroli rozminowania

Patrole rozminowania realizują zadania w ramach interwencyjnego oczyszczania kraju z przedmiotów wybuchowych i niebezpiecznych, określonego w Krajowym Planie Zarządzania Kryzysowego z uwzględnieniem Rozporządzenia Rady Ministrów z dnia 20 lutego 2003 r., w sprawie szczegółowych zasad udziału pododdziałów i oddziałów SZ RP w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu [Dz. U. z 2003 r., poz. 347] oraz Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym [Dz. U. z 2013 r., poz. 1166 z późn. zm.].

Zasadniczym zadaniem patroli rozminowania jest działalność interwencyjna oparta na podejmowaniu i niszczeniu PWiN pochodzenia wojskowego, zgłoszonych przez uprawnione instytucje państwowe lub samorządowe.

Działania interwencyjne

Każdy niewypał lub niewybuch powinien być usunięty w czasie 72 godzin (interwencja zwykła). Usuwanie przedmiotów niebezpiecznych w miejscach publicznych (szkoły, drogi, budowy) uważane jest za interwencję pilną, która powinna być zrealizowana do 24 godzin. Za ochronę miejsca znalezionego niewybuchu do czasu przyjazdu patrolu rozminowania odpowiada Policja. Niewypał przewożony jest do miejsca jego zniszczenia, którym zazwyczaj jest poligon wojskowy [http://archiwum2013.mon.gov.pl/pl/strona/371/PG_273.html].

Procedury działania patroli rozminowania

W Siłach Zbrojnych RP obowiązują następujące procedury działania patroli rozminowania:

- znalazca niewybuchu lub niewypału zgłasza miejsce i termin jego wykrycia oraz informację o osobie, która może wskazać miejsce znajdowania się przedmiotów wybuchowych i niebezpiecznych jednemu z uprawnionych do przyjęcia zgłoszenia organów:
  - administracji państwowej lub samorządowej,
  - Policji,
  - Państwowej Straży Pożarnej,
  - Straży Granicznej,
  - Lasom Państwowym,
  - Straży Miejskiej (Gminnej),
- uprawnione organy przekazują zgłoszenie oficerowi dyżurnemu jednostki wojskowej, w której znajduje się właściwy terytorialnie patrol rozminowania (dane teleadresowe patroli rozminowania),
- po otrzymaniu zgłoszenia oficer dyżurny jednostki wojskowej ewidencjonuje je i powiadamia o nim dowódcę patrolu rozminowania, który realizuje zgłoszenie bezzwłocznie, zgodnie z przyjętym priorytetem (w trybie pilnym lub zwykłym) [http://archiwum2013.mon.gov.pl/pl/strona/371/PG_273.html].

Siły Zbrojne RP, w ramach systemu reagowania na zagrożenia niewybuchami i niewypałami, utrzymują w swoich strukturach 39 etatowych patroli rozminowania oraz 2 grupy nurków minerów, które rocznie realizują średnio ok. 8 tysięcy interwencji. Każdego roku neutralizują one kilkaset tysięcy przedmiotów wybuchowych i niebezpiecznych. Patrole rozminowania posiadają rejony odpowiedzialności, które pokrywają swoim zasięgiem obszar całego kraju. Wielkość przydzielonego obszaru dla patrolu rozminowania zależy od częstotliwości zgłoszeń na danym terenie. Na obszarze województwa działa średnio od 1 do

4 patroli [https://archiwum2019-bip.mon.gov.pl/przydatne-informacje/artykul/partole-rozminowania/ilosc-oraz-struktura-patroli-rozminowania-i-grup-nurkow-minerow-1032477/].

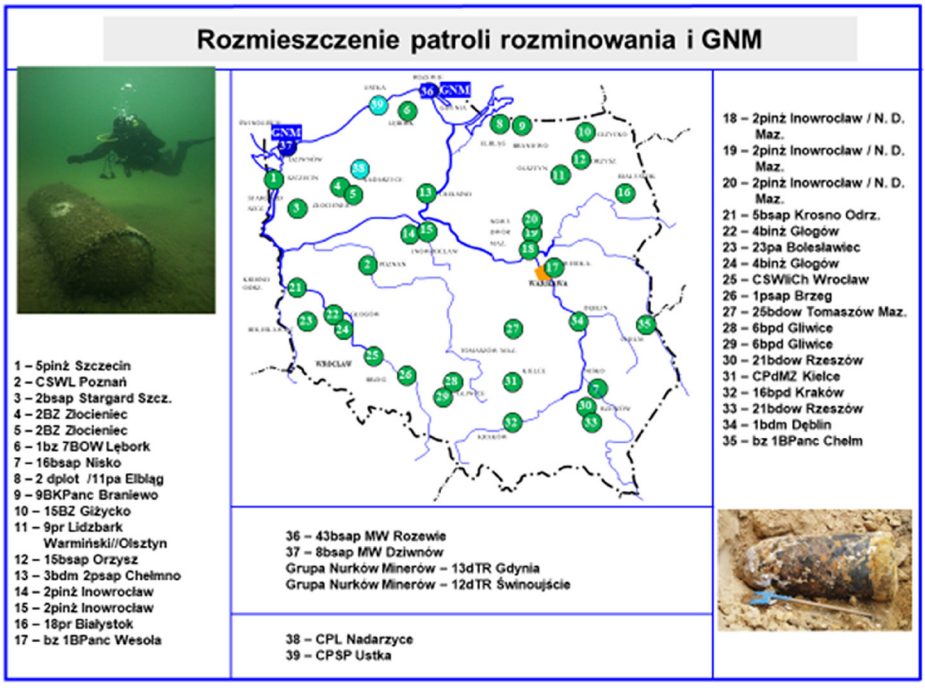
Grupy nurków minerów odpowiadają za obszary morskie wód przybrzeżnych oraz wspierają lądowe patrole rozminowania w podejmowaniu przedmiotów wybuchowych i niebezpiecznych w wodach śródlądowych.

Tabela 1. Skład przykładowego patrolu rozminowania

Lp.	Nazwa stanowiska	Stopień etatowy
1	Dowódca patrolu rozminowania	1 x pdf st.
2	Zastępca dowódcy patrolu rozminowania	1 x pdf
3	Starszy magazynier – saper	1 x pdf mł.
4	Starszy kierowca – saper	1 x pdf mł.
5	Saper	1 x szer./st. szer.
6	Saper	1 x szer./st. szer.
7	Kierowca – ratownik	1 x szer./st. szer.
8	Kierowca – ratownik	1 x szer./st. szer.

Źródło: opracowanie własne.

Rysunek 1. Rozmieszczenie patroli rozminowania i grup nurków minerów



Źródło: opracowanie własne na podstawie analizy zbiorczych zestawień wyników działań patroli rozminowania udostępnionych przez Dowództwo Generalne Rodzajów Sił Zbrojnych (DG RSZ).

Zestawienie prac (efekty patroli rozminowania) w 2017 i 2018 roku

W 2017 roku, podczas interwencyjnego oczyszczania terenu kraju, patrole rozminowania i żołnierze wojsk inżynieryjnych, sprawdzający pod względem występowania niewybuchów i niewypałów duże powierzchnie, znajdowali często znaczne ilości PWiN, w tym przedmioty o dużym wagomiarze. Najczęściej wykrywano je w rejonach zurbanizowanych, gęsto zaludnionych, na terenach prowadzonych prac rolnych, prac budowlanych oraz w kompleksach leśnych.

Tabela 2. Zestawienie wyników oraz zaangażowanych sił i środków w ramach interwencyjnego oczyszczania terenu z PWiN przez patrole rozminowania oraz grupy nurków minerów Polskiej Marynarki Wojennej w 2017 roku

Lp.	Wyszczególnienie		J.m.	RAZEM
1.	Liczba pracujących	Patroli	szt.	41
		Żołnierzy	liczba	358
2.	Przyjęto zgłoszeń		szt.	7 129
3.	Wykonano zgłoszeń		szt.	7 129
4.	Niszczenie PWiN z MCPPA (Miejsce Czasowego Przechowywania Porzuconej Amunicji.		szt.	2 610
5.	Całkowite rozminowanie		szt.	171
6.	Zabezpieczenie zajęć		szt.	89
7.	Nadzór saperski		szt.	40
8.	Profilaktyka		szt.	324
9.	Przepracowano		rd	52 864
10.	Przejechano		km	1 375 266
11.	**Wykryto i zniszczono:**			
	bomba lotnicza		szt.	1 810
	granat moździerzowy		szt.	4 720
	granat ręczny		szt.	1 452
	mina		szt.	738
	pocisk artyleryjski		szt.	16 530
	pocisk rakietowy		szt.	269
	torpeda		szt.	2
	bomba głębinowa		szt.	0
	amunicja strzelecka		szt.	456 304
	pocisk do granatnika		szt.	783
	inne (np. zapalniki)		szt.	45 705
	Razem		szt.	**528 313**
	materiał wybuchowy		kg	407,467
	proch		kg	41,928
	Razem		kg	**449,395**
12.	**Zużyto:**			
	materiału wybuchowego		kg	885,3
	lontu prochowego		m	805
	lontu detonującego		m	50
	spłonek		szt.	403
	zapalników elektrycznych		szt.	22 932
	innych (zapalniki różnego typu)		szt./pud.	39
13.	**Koszty**		zł	34 822 452

Lp.	Wyszczególnienie	J.m.	RAZEM
14.	**Nieszczęśliwe wypadki:**		
	zabici	0	0
	ranni	0	0

Źródło: opracowanie własne na podstawie analizy zbiorczych zestawień wyników działań patroli rozminowania udostępnionych przez Dowództwo Generalne Rodzajów Sił Zbrojnych (DG RSZ).

Do ważniejszych interwencji w zakresie likwidacji przedmiotów wybuchowych i niebezpiecznych w 2017 r. należy zaliczyć:

1. 6 marca w Zabłoci, w powiecie żarskim, z brzegu rzeki Nysa Łużycka, Patrol Rozminowania nr 21 podjął i zniszczył pocisk artyleryjski kal. 150 mm, 10 szt. pocisków artyleryjskich kal. 105 mm, 4 pociski artyleryjskie odłamkowo-burzące kal. 88 mm oraz 86 szt. przeciwpancernych pocisków artyleryjskich kal. 88 mm.

2. 28 marca w Szczytnie, ok. 500 m od płotu lotniska Szymany, podczas prac leśnych natrafiono na bombę lotniczą o masie 80 kg oraz 4 bomby lotnicze SD-4 HL o masie 5 kg. Podjęte przedmioty zostały zniszczone przez Patrol Rozminowania nr 11.

3. 23 maja na terenie budowy hali magazynowej w Ośle, w powiecie bolesławieckim, województwie dolnośląskim, podczas prac ziemnych wykopano bombę lotniczą o masie 100 kg bez zapalnika (typu FAB-100) produkcji radzieckiej, 3 bomby lotnicze o masie 4 kg (SD-4) produkcji niemieckiej oraz pocisk amunicji strzeleckiej kal. 20 mm z okresu II wojny światowej. Wykopane PWiN Patrol Rozminowania nr 23 zdetonował na poligonie Świętoszów.

4. 25 maja na terenie strefy ekonomicznej, w rejonie budowy hali magazynowej w Ośle, w powiecie bolesławieckim, w województwie dolnośląskim, znaleziono 36 bomb lotniczych kasetowych (1 szt. SD-1, 24 szt. SD-4, 11 szt. SD-10), 6 pocisków artyleryjskich kal. 30 mm i 2 zapalniki bomb lotniczych typu EL produkcji niemieckiej z okresu II wojny światowej. Znalezione PWiN zostały zdetonowane w Składowisku Materiałów Niebezpiecznych (SMN) na poligonie Świętoszów przez Patrol Rozminowania nr 23.

5. 26 maja na terenie budowy ronda w Kołbaskowie znaleziono bombę lotniczą o masie 20 kg, pochodzącą z okresu II wojny światowej. Ewakuowano pracowników budowy oraz wstrzymano ruch na drodze relacji Berlin – Szczecin. Bombę podjął i zabezpieczył Patrol Rozminowania nr 1.

6. 5 i 6 czerwca Patrol Rozminowania nr 23 zrealizował zgłoszenie w Świętoszkowie, w powiecie bolesławieckim, w województwie dolnośląskim, na terenie

budowy nowego mostu przez rzekę Kwisę. W jego środkowej części, podczas wykopywania koparką żelbetonowej postawy pod filar mostu i starych pali mostu, wykopano bombę lotniczą burzącą o masie 250 kg (typu SC-250), produkcji niemieckiej z okresu II wojny światowej. Zdetonowano ją w SMN na poligonie Świętoszów.

7. 16 czerwca w Dobrej, w powiecie bolesławieckim, w województwie dolnośląskim, w lesie przy autostradzie A-4, podczas zbierania grzybów, w rozkopanym dole, znaleziono 3 przeciwpancerne pociski artyleryjskie kal. 88 mm. Po minerskim sprawdzeniu terenu (rejon byłych artyleryjskich stanowisk ogniowych, gdzie wciąż widoczne są okopy) Patrol Rozminowania nr 23 dodatkowo wykrył 68 szt. przeciwpancernych pocisków artyleryjskich kal. 88 mm (typu 8,8 cm Pzgr.) i 2 czerepy pocisków art. kal. 105 mm produkcji niemieckiej z okresu II wojny światowej. Przedmioty niebezpieczne podjęto i zabezpieczono do czasu ich zniszczenia w odpowiednio przygotowanym i dedykowanym do tego celu miejscu (Miejsce Czasowego Przetrzymywania/Przechowywania Podjętej Amunicji – MCPPA). W czasie akcji podjęcia i załadunku PWiN niezbędne było zamknięcie ruchu drogowego na czas dwóch godzin.

8. 22 czerwca przy drodze powiatowej Iłowo-Osada – Pruski, podczas czyszczenia i kopania przydrożnego rowu natrafiono na 6 granatów moździerzowych. Podczas sprawdzania terenu przez Patrol Rozminowania nr 11 znaleziono jeszcze 157 granatów moździerzowych (większość bez zapalnika) oraz 10 korpusów granatów moździerzowych z widocznym materiałem wybuchowym. Miejsce znaleziska zabezpieczyła Policja z Działdowa. Ruch samochodowy i pieszy na tym odcinku drogi był wstrzymany przez cztery godziny.

9. 27 czerwca w Łęczycy, na terenie stanowiska archeologicznego w centrum miasta, wykryto podczas prac 9 min przeciwpancernych produkcji jugosłowiańskiej (mina uniwersalna nr 5 bez zapalników). Miny zabezpieczono przez Patrol Rozminowania nr 27 w MCCPA do czasu zniszczenia.

10. 29 czerwca w Kołbaskowie, podczas prowadzenia prac ziemnych, znaleziono bombę lotniczą produkcji rosyjskiej o masie 100 kg, pochodzącą z okresu II wojny światowej. Wstrzymano prace oraz ewakuowano pracowników budowy, a bombę podjął i zabezpieczył Patrol Rozminowania nr 1.

11. 28 sierpnia Patrol Rozminowania nr 23 realizował zgłoszenie w Pieszkowie, w powiecie lwóweckim, w województwie dolnośląskim, gdzie podczas wykopu pod kanalizację, nieopodal budynku mieszkalnego, znaleziono bombę lotniczą produkcji rosyjskiej o masie 100 kg (typu FAB-100) z okresu II wojny światowej. Bombę podjęto i zdetonowano na poligonie w Świętoszowie.

12. 22 września w Gryfinie, podczas przebudowy skrzyżowania dróg, znaleziono minę przeciwpancerną TM-53. Wszystkie prace zostały wstrzymane, zamknięto drogi dojazdowe do skrzyżowania oraz ewakuowano mieszkańców, a z pobliskiego przedszkola personel wraz z dziećmi.
13. 25 września w Szczecinie, w czasie przeszukiwania przez Policję piwnicy budynku poczty głównej, znaleziono 207 szt. PWiN, tj.: miny przeciwpancerne, przeciwpiechotne, pociski artyleryjskie, granaty ręczne, zapalniki oraz amunicję strzelecką. Ewakuowano personel poczty, zamknięto wszystkie drogi dojazdowe wraz z chodnikami dla pieszych oraz ewakuowano mieszkańców pobliskich budynków.
14. 31 października w Jarosławiu, w powiecie jarosławskim, w województwie podkarpackim, na boisku szkolnym podczas prac ziemnych firma budowlana natknęła się na niewybuchy z czasów II wojny światowej. Zarządzono zamknięcie szkoły oraz ewakuację 521 osób. Zgłoszenie realizował Patrol Rozminowania nr 33. Znaleziono ok 138 szt. przedmiotów wybuchowych i niebezpiecznych, tj.: 98 szt. granatów moździerzowych (kal. 120 mm i kal. 81mm), 7 szt. pocisków artyleryjskich kal. 75 mm i ponad 31 szt. łusek od pocisku art. kal. 75 mm.
15. 8 listopada w Dzierżoniowie, w powiecie dzierżoniowskim, podczas remontu mostu na ul. Sienkiewicza podjęto 200 kg materiału wybuchowego z czasów II wojny światowej. Policja i straż pożarna wyznaczyły strefę bezpieczeństwa. Ewakuowano wszystkie osoby w promieniu 500 m od miejsca znalezienia niewybuchów. Wśród ewakuowanych były dzieci z pobliskich dwóch szkół i przedszkola. Zgłoszenie realizował Patrol Rozminowania nr 26.
16. 14 listopada w Gołdapi przy ul. Podgórnej, w województwie warmińsko-mazurskim, podczas prac ziemnych znaleziono bombę o dużej sile rażenia (100 kg). Z pobliskich budynków mieszkalnych i Urzędu Miejskiego ewakuowano ok. 300 osób. Zgłoszenie realizował Patrol Rozminowania nr 10. Bomba lotnicza z czasów II wojny światowej została zdetonowana na poligonie.
17. 23 listopada w Kołobrzegu, w trakcie prac remontowych na terenie Szkoły Podstawowej nr 4 robotnicy odkopali pocisk moździerzowy z czasów II wojny światowej. Policja ewakuowała dzieci i pracowników placówki oraz mieszkańców sąsiadującego ze szkołą budynku. Pocisk podjęli saperzy Patrolu Rozminowania nr 37, który zdetonowali go na poligonie w Drawsku Pomorskim.
18. 6 grudnia podczas budowy na terenie kompleksu Centrum Doktryn i Szkolenia SZ w Bydgoszczy wykryto 7 bomb lotniczych o masie 80 kg, które podjął i zniszczył Patrol Rozminowania nr 13.

Analogicznie w roku 2018, podczas interwencyjnego oczyszczania terenu, patrole rozminowania podejmowały często znaczne ilości PWiN, w tym przedmioty o dużym wagomiarze. Najczęściej wykrywano je, jak w latach ubiegłych, w rejonach zurbanizowanych, na terenach prowadzonych prac rolnych, budowlanych, a także przy budowach autostrad i tras szybkiego ruchu oraz w kompleksach leśnych.

Tabela 3. Zestawienie wyników oraz zaangażowanych sił i środków w ramach interwencyjnego oczyszczania terenu z PWiN przez patrole rozminowania oraz grupy nurków minerów Polskiej Marynarki Wojennej w 2018 roku.

Lp.	Wyszczególnienie		J.m.	RAZEM
1.	Liczba pracujących	Patroli	szt.	41
		Żołnierzy	liczba	327
2.	Przyjęto zgłoszeń		szt.	6 218
3.	Wykonano zgłoszeń		szt.	6 218
4.	**Wykryto i zniszczono:**			
	bomba lotnicza		szt.	1 394
	granat moździerzowy		szt.	3 979
	granat ręczny		szt.	1 332
	mina		szt.	960
	pocisk artyleryjski		szt.	18 593
	pocisk rakietowy		szt.	683
	torpeda		szt.	12
	bomba głębinowa		szt.	–
	pocisk do granatnika		szt.	1 587
	Razem		szt.	**28 540**
5	**Wykryto i zlikwidowano (materiały)**			
	amunicja strzelecka (magazynowa)		szt.	51 687
	amunicja strzelecka (wojenna)		szt.	160 036
	inny		szt.	41 994
	materiał wybuchowy		g	335 062
	zapalniki		szt.	8 416
6.	**Nieszczęśliwe wypadki:**			
	zabici		o	o
	ranni		o	o

Źródło: [Meldunki i sprawozdania…].

Natomiast do ważniejszych interwencji w zakresie likwidacji przedmiotów wybuchowych i niebezpiecznych w 2018 r. należy zaliczyć:

1. 13 lutego, w miejscowości Dzierżoniów, przy moście w ciągu drogi powiatowej, ok. 500 m od centrum miasta, Patrol Rozminowania nr 26 z 1 psap Brzeg

podjął ładunki z II wojny światowej (ok. 120 kg materiału wybuchowego). Powiatowy zespół kryzysowy, celem zapewnienia bezpieczeństwa, określił strefę bezpieczeństwa na 500 m. Zamknięto ruch drogowy i ewakuowano ponad dwa tysiące osób (okolicznych mieszkańców oraz dzieci z pobliskich przedszkoli i szkół).

2. 16 lutego w Kędzierzynie Koźlu Patrol Rozminowania nr 28 z 6 bpd Gliwice podjął bombę lotniczą produkcji amerykańskiej z okresu II wojny światowej o oznaczeniu AN-M59 i wadze 450 kg (sama masa materiału wybuchowego to prawie 150 kg).

3. 16 marca w lesie w okolicach Mielca Patrol Rozminowania nr 30 z 21 bdow (21 BSP) Rzeszów podjął bombę lotniczą o wadze około 500 kg.

4. 23 marca w 1. Regionalnej Bazie Logistycznej w Dębogórzu koło Gdyni Patrol Rozminowania nr 36 z 43 bsap MW (3 FO) Rozewie podjął 160 bomb lotniczych i pociski artyleryjskie o różnym wagomiarze i kalibrze. Największa z nich ważyła około 250 kg.

5. 23 marca w Kojęcinach, w województwie dolnośląskim, Patrol Rozminowania nr 26 z 1 psap Brzeg, podjął ponad 160 pocisków do dział przeciwpancernych. Znajdowały się w 41 skrzyniach, około 400 m od terenów zamieszkanych. Saperzy ustalili, że zostały tam umieszczone prawdopodobnie na początku XX wieku.

6. 23 marca w miejscu prac ziemnych przy budowie centrum handlowego w Tarnowie Patrol Rozminowania nr 30 z 21 bdow (21 BSP) Rzeszów podjął 106 min przeciwpiechotnych produkcji niemieckiej typu SMI-35. W czasie operacji ich usuwania ewakuowano około 30 pracowników budowy w promieniu 500 m od znaleziska.

7. 28 marca w okolicy Kraszowic, w gminie Bolesławiec, w województwie dolnośląskim, w korycie rzeki Bóbr, Grupa Nurków Minerów z 12 dTR (8 FOW) Świnoujście, wydobyła kilkanaście pocisków rakietowych typu M-13, kal. 132 mm (tzw. Katiusza) oraz silniki do rakiet produkcji radzieckiej pochodzące z okresu II wojny światowej.

8. 27 kwietnia na terenie prac drogowych w Brzegu Patrol Rozminowania nr 26 z 1 psap Brzeg podjął granatnik przeciwpancerny typu Panzerfaust oraz bombę lotniczą z okresu II wojny światowej o masie 10 kg. Ze względów bezpieczeństwa ewakuacji poddano około 1200 osób.

9. 29 kwietnia w Sadkowie, w gminie Kąty Wrocławskie, Patrol Rozminowania nr 25 z Centrum Szkolenia Wojsk Inżynieryjnych i Chemicznych (CSWIiCh) Wrocław, podjął 5 kg kasetową bombę lotniczą z uszkodzonym zapalnikiem.

10. 3 maja w Wujskiem, w gminie Sanok, Patrol Rozminowania nr 33 z 21 bdow (21 BSP) Rzeszów podjął 5 szt. pocisków artyleryjskich kal. 100 mm.
11. 4 maja na terenie Lasu Osobowickiego – Stare Grodzisko Patrol Rozminowania nr 25 z CSWIiCh Wrocław podjął pocisk artyleryjski z uszkodzonym zapalnikiem produkcji rosyjskiej kal. 85 mm.
12. 4 maja w rejonie redy Portu Gdynia Grupa Nurków Minerów z 13 dTR (3 FO) Gdynia podjęła niemiecką minę morską typu GC z okresu wojennego oraz niemiecką torpedę ćwiczebną G-7.
13. 10 maja na terenie prac ziemnych w Toruniu Patrol Rozminowania nr 14 z 2 pinż Inowrocław podjął pięć 100 kg radzieckich bomb lotniczych FAB-100. Ewakuacji poddano około 900 osób.
14. 22 maja na terenie Basenu III Portu Gdynia Grupa Nurków Minerów z 13 dTR (3 FO) Gdynia podjęła niemiecką bombę lotniczą SC 500 z okresu II wojny światowej.
15. 14 czerwca na terenie Muzeum Westerplatte i Wojny 1939 roku w Gdańsku Patrol Rozminowania nr 8 z 2 dplot (15 pplot, 16 DZ) Elbląg podjął 2 pociski artyleryjskie kal. ok. 355 mm i wadze 400 kg, każdy o długości 162 cm.
16. Od 2 do 17 lipca w Turzy i Żabnie, pow. tarnowski, Patrol Rozminowania nr 33 z 21 bdow (21 BSP) Rzeszów podjął 75 sztuk amunicji strzeleckiej z okresu II wojny światowej.
17. 9 sierpnia w Głogowie w rzece Odrze Patrol Rozminowania nr 24 z 4 binż (2 pinż) Głogów oraz Grupa Nurków Minerów z 12 dTR (8 FOW) Świnoujście podjęli bombę lotniczą o wagomiarze 200 kg. Ze względów bezpieczeństwa ewakuacji poddano około 600 osób.
18. 13 sierpnia na plaży, przy kąpielisku miejskim w Podczelu (Kołobrzeg), Grupa Nurków Minerów z 12 dTR (8 FOW) Świnoujście i z 13 dTR (3 FO) Gdynia oraz Patrol Rozminowania nr 37 z 8 bsap (8 FOW) Dziwnów, podjęli 3 bomby lotnicze. Ze względów bezpieczeństwa ewakuacji poddano około kilku tysięcy osób.
19. 21 sierpnia w Klaudynie, w powiecie warszawskim, Patrol Rozminowania nr 19 z Sekcji Przechowywania (2 pinż) Nowy Dwór Mazowiecki, podjął granat moździerzowy kal. 82 mm. Ze względów bezpieczeństwa ewakuowano miejscową ludność.
20. 31 sierpnia w Morgownikach, w powiecie łomżyńskim, Patrol Rozminowania nr 12 z 15 bsap (16 DZ) Orzysz podjął bombę lotniczą. Ze względów bezpieczeństwa ewakuowano miejscową ludność.

21. 13 września na terenie leśnym w okolicy poradzieckiej miejscowości Pstrąże Patrol Rozminowania nr 23 z 23 pa (11 DKPanc) Bolesławiec podjął pocisk czołgowy przeciwpancerny kumulacyjny kal. 125 mm.

22. 14 września w pobliżu drogi krajowej nr 81 w Mikołowie Patrol Rozminowania nr 28 z 6 bpd (6 BPD) Gliwice, podjął pociski kalibru 210 mm, naboje działonowe, granaty ręczne, amunicję karabinową i tzw. pięści pancerne (potoczna nazwa niemieckiego granatnika przeciwpancernego Panzerfaust). Ze względów bezpieczeństwa ewakuowano miejscową ludność.

23. 9 października w pobliżu drogi krajowej nr 16 w Kolnie, Patrol Rozminowania nr 12 z 15 bsap (16 DZ) Orzysz podjął 2 pociski artyleryjskie 150 mm z czasów II wojny światowej. Ze względów bezpieczeństwa ewakuowano miejscową ludność.

24. 14 listopada, na terenie prac remontowych w centrum Głogowa, Patrol Rozminowania nr 24 z 4 binż (2 pinż) Głogów podjął 250-kilogramową bombę lotniczą z czasów II wojny światowej. Ze względów bezpieczeństwa ewakuowano około 3000 osób.

25. W dniu 10 grudnia, na terenie prace ziemnych w Policach, Patrol Rozminowania nr 1 z 5 pinż Szczecin podjął 250-kilogramową bombę lotniczą z czasów II wojny światowej. Ze względów bezpieczeństwa ewakuacji poddano około 25 000 osób.

26. 17 grudnia na terenie jednostki wojskowej w Morągu Patrol Rozminowania nr 11 z 9 pr Lidzbark Warmiński podjął 15 pocisków artyleryjskich o kalibrze 210 mm i masie 120 kg z czasów II wojny światowej. Ze względów bezpieczeństwa ewakuowano około 6000 osób.

Jednocześnie, w wyniku analizy sprawozdań za lata 2004–2018, autorzy niniejszego rozdziału dokonali zbiorczego zestawienia liczby zgłoszeń i zniszczonych PWiN. Poniższe zestawienie pozwala zaobserwować pewne tendencje w odnajdywaniu i neutralizacji PWiN.

Tabela 4. Zestawienie efektów działania patroli rozminowania w latach 2004–2018

Rok	Liczba zgłoszeń telefonicznych	Liczba szt. zniszczonych PWiN
2004	8547	1 453 438
2005	7698	1 008 314
2006	7818	1 299 842
2007	10051	604 550
2008	8380	538 972
2009	7264	346 739
2010	6693	345 496
2011	8142	713 586
2012	8016	1 798 658
2013	7793	735 739
2014	8791	498 275
2015	8764	618 439
2016	7609	675 472
2017	7129	528 313
2018	7195	316 544

Źródło: opracowanie własne na podstawie analizy zbiorczych zestawień wyników działań patroli rozminowania udostępnionych przez Dowództwo Generalne Rodzajów Sił Zbrojnych (DG RSZ).

W innym ujęciu statystycznym tzw. rejonów odpowiedzialności, poniższe zestawienie statystyczne pokazuje jak w poszczególnych latach od 2008 roku patrole rozminowania realizowały swoje zadania na obszarach poszczególnych województw, w ujęciu liczby zgłoszeń.

Tabela 5. Przykładowe roczne obciążenie działań patroli rozminowania z podziałem na województwa

Województwo	2008	2009	2010	2010	2011	(...)	2016	2017	Średnio
dolnośląskie	717	671	630	950	834		824	730	765
kujawsko-pomorskie	417	389	319	538	511		426	406	430
lubelskie	349	325	299	408	380		336	319	345
lubuskie	256	240	225	276	348		275	253	268
łódzkie	186	133	161	166	203		144	145	163
małopolskie	240	239	228	266	255		188	149	224
mazowieckie	1299	1089	1067	1098	1111		1233	1182	1154
opolskie	297	287	315	354	396		337	302	327
podkarpackie	432	453	465	500	598		467	430	478
podlaskie	316	326	246	281	279		339	276	295

Województwo	2008	2009	2010	2010	2011	(...)	2016	2017	Średnio
pomorskie	891	674	781	934	866		729	687	795
śląskie	385	301	308	322	371		244	237	310
świętokrzyskie	326	324	269	317	331		277	269	302
warmińsko-mazurskie	755	570	456	523	624		681	601	601
wielkopolskie	459	438	353	535	466		439	470	451
zachodniopomorskie	668	584	570	789	841		669	673	685
RAZEM	7993	7043	6692	8257	8414		7608	7129	

Źródło: opracowanie własne na podstawie analizy zbiorczych zestawień wyników działań patroli rozminowania udostępnionych przez Dowództwo Generalne Rodzajów Sił Zbrojnych (DG RSZ).

W analizowanych okresach, a w szczególności w latach 2017–2018, realizację zadań utrudnia m.in. przedłużający się okres procedowania projektu rozporządzenia Rady Ministrów realizowanego zgodnie z delegacją ustawową przez Ministerstwo Spraw Wewnętrznych i Administracji w sprawie oczyszczania terenów z materiałów wybuchowych i niebezpiecznych, mimo że Dowództwo Generalne Rodzajów Sił Zbrojnych uzgodniło pozytywnie jego projekt 22 lipca 2014 r. Brak regulacji prawnej w tym zakresie powodował i dalej powoduje, że tę lukę prawną wykorzystują firmy cywilne prowadzące działalność komercyjną w zakresie oczyszczania terenów z przedmiotów wybuchowych i niebezpiecznych. Sytuacja ta powoduje angażowanie patroli rozminowania do interwencyjnego podejmowania PWiN odnajdowanych w czasie działalności komercyjnej firm. Ponadto brakuje podstawy prawnej do wyznaczania przez wojewodów w porozumieniu z Szefem Inspektoratu Wsparcia Sił Zbrojnych nowych miejsc przeznaczonych do niszczenia podjętych PWiN. Wymusza to transportowanie ich drogami publicznymi na duże odległości, co wpływa znacząco na bezpieczeństwo społeczeństwa i zwiększenie kosztów funkcjonowania podsystemu oczyszczania terenu kraju z PWiN.

Według opinii żołnierzy ze składu patroli, jak i poszczególnych przełożonych, istnieje konieczność intensyfikacji działań związanych z pozyskaniem dla patroli rozminowania pojazdów typu Jelcz 442 przystosowanych do ciągnięcia przyczepy z pojemnikiem przeciwodłamkowym, co pozwoliłoby na usprawnienie przewozu przedmiotów wybuchowych i niebezpiecznych oraz podniesienie poziomu bezpieczeństwa ludności cywilnej i realizujących zadania żołnierzy. Jednocześnie, celem podniesienia sprawności oraz efektywności działania, konieczna jest wymiana mocno wyeksploatowanego sprzętu patroli rozminowania i grup nurków minerów. Działania te pozwoliłyby na efektywniejsze oczyszczanie terenu i obszarów morskich z PWiN oraz zapewniłoby większe bezpieczeństwo podczas realizacji powyższych zadań.

Tabela 6. Zasadniczy sprzęt występujący na wyposażeniu patroli rozminowania

	**Star 266 M2** to seryjna wersja zmodernizowanego polskiego terenowego samochodu ciężarowego. Modernizacja objęła remont kapitalny wszystkich układów podwozia (ramy, mostów napędowych i skrzyni rozdzielczej) oraz montaż nowego silnika, skrzyni biegów i przebudowanej kabiny kierowcy.
	**Żuraw Maxilift M50. 2H PLH** z wysięgnikiem teleskopowym przeznaczonym do załadunku wielogabarytowych przedmiotów wybuchowych i niebezpiecznych.
	**Samochód specjalny Honker-Saper** przeznaczony jest do transportu przedmiotów wybuchowych i niebezpiecznych oraz środków i sprzętu do ich wykrywania, wydobywania i niszczenia, a także holowania przyczepy o dopuszczalnej masie całkowitej 1500 kg z hamulcem i do 750 kg bez hamulca.
 	**Kontenerowy magazyn materiałów wybuchowych (KMMW)** służy do bezpiecznego przechowywania materiałów wybuchowych kruszących, środków inicjujących oraz podjętych PWiN, a także jako magazyn na środki przewidziane do prowadzenia szkolenia (amunicja strzelecka bojowa i ćwiczebna oraz środki pozoracji pola walki). Może być stosowany poza granicami kraju w misjach wojskowych i operacjach pokojowych. **Dane taktyczno-techniczne:** • strefa niebezpieczna związana z oddziaływaniem fali uderzeniowej o nadciśnieniu większym niż 10 kPa – 15 m, • łączny ekwiwalent trotylu (TNT) przechowywanych niewypałów i niewybuchów – 25 kg, • maksymalny ekwiwalent TNT pojedynczego niewypału lub niewybuchu – 1,5 kg, • maksymalna ilość przechowywanych materiałów wybuchowych (w przeliczeniu na TNT) – 25 kg, • maksymalna ilość TNT przechowywana w jednym gnieździe magazynowym – 1,3 kg, • odporność na temperaturę otoczenia od -30°C do +55°C .
	Przyczepa z pojemnikiem przeciwodłamkowym jest dwuosiowym pojazdem specjalnym przeznaczonym do przewożenia średniej wielkości niewybuchów i niewypałów o równoważniku do 10 kg czystego TNT oraz użytkowania w różnych warunkach atmosferycznych i klimatycznych, zdolnym do poruszania się po drogach gruntowych.

	Pojazd saperski Iveco Daily 55S18 „Topola - S" przeznaczony jest do przewożenia 6 żołnierzy patrolu rozminowywania. Posiada zamontowaną w tylnej części skrzynię ładunkową, wewnątrz której zamontowany jest pojemnik przeciwodłamkowy, przystosowany do przewożenia materiałów niebezpiecznych, których moc w wypadku detonacji nie jest większa od mocy wybuchu nieopakowanego (luzem) 3,5 kg TNT.
	Kombinezon przeciwwybuchowy EOD-9A z hełmem EOD-9A i wysięgnikiem jest przeznaczony do ochrony użytkownika przed czterotypowym zagrożeniom związanym z wybuchem, polegającym na oddziaływaniu: nadciśnienia, odłamków, fali uderzeniowej i promieniowania cieplnego. Kombinezon zapewnia użytkownikowi maksymalną ruchliwość i pole widzenia. Jest kompatybilny z wieloma akcesoriami, w tym z systemem chłodzenia ciała BCS-4, systemem łączności przewodowej i systemem łączności bezprzewodowej.
	Wykrywacz min MINEX 2FD 4.530 umożliwia bardzo dokładne umiejscowienie obiektu metalowego, również w przypadku małych części metalowych, a także pozwala na odróżnienie obiektów o różnej wielkości leżących obok siebie (szczególnie przydatne przy poszukiwaniu w pobliżu płotów i przewodów elektrycznych itp.). Wykrywacz posiada dodatkową możliwość kompensacyjną zakłóceń wielkoobszarowych, np. mineralizowanej gleby, różnych rodzajów skał albo słonej wody.
	Wykrywacz Groundshark ma wysoką wydajność wykrywania zakopanych obiektów (m.in. metalowych z niską zawartością metalu z dyskryminacją i niemetalowych, w tym tworzyw sztucznych i drewna), a także wizualizacji pod powierzchnią ziemi, asfaltu i warstw cementowych.
	Zestaw hakowo-linowy HAL Mk4 jest udoskonalonym jednolinowym zestawem haczyk i lina, który został zoptymalizowany do uzyskania dostępu i postępowania z podejrzanymi ładunkami i obiektami. Zestaw zawiera wybór elementów do mocowania lin do obiektów i kotwienia bloczków linowych do ścian, podłóg, okien i framug drzwi. Manewrowanie obiektami wzdłuż kompletnych tras jest realizowane poprzez zblocza samoczynnie otwierane.

Źródło: opracowanie własne na podstawie analizy zbiorczych zestawień wyników działania patroli rozminowania udostępnionych przez DG RSZ.

Istotną kwestią, związaną z poprawą koordynacji wykorzystania potencjału patroli rozminowania, jest potrzeba kontynuacji rozpoczętych prac związanych z utworzeniem Centralnego Ośrodka Zarządzania Zgłoszeniami Przedmiotów Wybuchowych i Niebezpiecznych (COZZPWiN) co pozwoli na osiągnięcie pełnej zdolności operacyjnej w zakresie przyjmowania i dystrybucji zgłoszeń dotyczących przedmiotów wybuchowych i niebezpiecznych z terenu RP oraz na optymalizację przedsięwzięć związanych z funkcjonowaniem i zarządzaniem patrolami rozminowania, grupami nurków minerów oraz grupami EOD.

Niezwykle istotną sprawą jest także prowadzenie systematycznej działalności profilaktycznej wśród ludności cywilnej i młodzieży na różnych poziomach edukacji na temat zagrożeń stwarzanych przez wybuchowe pozostałości wojenne oraz zasad postępowania w przypadku znalezienia PWiN (zwracając uwagę na obowiązujące akty prawne oraz przestrzeganie przepisów bezpieczeństwa), co pozwoli na zmniejszenie liczby wypadków z nimi związanych.

System Informatyczny PATROL (SI Patrol)

System Informatyczny PATROL pracuje operacyjnie od początku 2008 roku i jest systemem wieloszczeblowym, pracującym w oparciu o model rozproszonej bazy danych, w którym poszczególne stanowiska mogą pracować autonomicznie, bez konieczności stałego dostępu do centralnego serwera.

Rysunek 2. System Informatyczny PATROL

Źródło: http://rczpi.wp.mil.pl/pl/36_61.html.

System PATROL stał się, po wielu latach próbnej eksploatacji, nieodzownym narzędziem wspomagającym bieżącą pracę patroli rozminowania oraz osób funkcyjnych sprawujących nad nimi codzienny nadzór.

System Informatyczny PATROL (SI Patrol) jest używany w 39 patrolach rozminowania, 2 grupach nurków minerów oraz 6 grupach EOD, a także w pomieszczeniach służbowych służb dyżurnych 33 jednostek wojskowych podległych Dowódcy Generalnemu Rodzajów Sił Zbrojnych.

Zasadniczymi funkcjami SI Patrol są:

- przekazywanie informacji o zarejestrowanych zgłoszeniach dotyczących PWiN z poziomu służby dyżurnej do patroli rozminowania oraz o podjętych interwencjach z poziomu patroli rozminowania na szczebel służby dyżurnej swojej jednostki i jej przełożonych na szczeblu centralnym;
- przekazywanie na bieżąco aktualizowanych danych teleadresowych jednostek i osób funkcyjnych uczestniczących w systemie;
- okresowe przekazywanie informacji o efektach oraz kosztach funkcjonowania patroli rozminowania;
- wspieranie osób funkcyjnych w zakresie poprawnego przydziału zgłoszeń w zależności od rejonu odpowiedzialności patroli rozminowania;
- wspieranie patroli rozminowania w zakresie wytwarzania niezbędnej, określonej instrukcją dokumentacji bieżącej i sprawozdawczej;
- umożliwianie skutecznego, bieżącego monitorowania przez przełożonych stanu wykonywanych zadań przez patrole rozminowania oraz miejsc ich wykonywania (system meldunkowy, bieżące raportowanie położenia na mapach cyfrowych w PGO (Pakiet Grafiki Operacyjnej) oraz rodzaj wykonywanego zadania i jego stanu);
- realizowanie automatycznego, wielokanałowego i szybkiego powiadamiania o odnalezieniu PWiN osób funkcyjnych środkami łączności (SMS-y na służbowe telefony komórkowe, sformalizowane szyfrowanie informacji na terminale spełniające wymogi bezpieczeństwa).

System SI PATROL znacząco upraszcza i przyspiesza informację sprawozdawczą docierającą na szczebel przełożonego. Informacje zbierane w omawianym systemie prezentowane są w nim zarówno w postaci tabelarycznej, jak i wizualnej na mapach cyfrowych (PGO) i docierają ze szczebla najniższego jednocześnie do przełożonych różnych szczebli.

Zakończenie

Patrole rozminowania w systemie zarządzania kryzysowego państwa były, są i będą bardzo ważnym elementem zapewniania bezpieczeństwa zarówno społeczeństwu, jak i powstającym inwestycjom. Pomimo upływu kilkudziesięciu lat od zakończenia II wojny światowej oraz opuszczenia przez wojska radzieckie terytorium RP, w ziemi i wodzie nadal pozostaje ogromna liczba PWiN. Posiadane umiejętności oraz wyposażenie partoli rozminowania sprawia, że w zasadzie jako jedyne są one do przeciwdziałania omawianym zagrożeniom. Jednocześnie, z upływem lat, zagrożenie nie będzie malało, a w ocenie autorów wręcz będzie wzrastać lub pozostanie na podobnym poziomie. Wynika to ze znaczącego rozwoju inwestycji podejmowanych zarówno w miastach, jak i przy budowach i rozbudowach sieci drogowej. Ponadto z Bałtyku coraz częściej wyłaniają się pozostałości walk na morzu, jak i bombardowań infrastruktury nadmorskiej oraz uciekających wojsk niemieckich w okresie walk w 1944 i 1945 roku.

Bibliografia

DD 4.22 - Zabezpieczenie techniczne Sił Zbrojnych Rzeczypospolitej Polskiej. Zasady funkcjonowania, Inspektorat Wsparcia Sił Zbrojnych RP, Bydgoszcz 2012.

DD 4.22.13 - Instrukcja zarządzania eksploatacją uzbrojenia i sprzętu wojskowego w Siłach Zbrojnych Rzeczypospolitej Polskiej. Zasady ogólne, Inspektorat Wsparcia Sił Zbrojnych RP, Bydgoszcz 2013.

Instrukcja „Oczyszczanie terenów z przedmiotów wybuchowych i niebezpiecznych", DG RSZ, sygn. Inż. 598/2014, Warszawa, 2014.

Meldunki i sprawozdania z interwencyjnego oczyszczania terenu z PWiN przez patrole rozminowania oraz grupy nurków minerów Marynarki Wojennej w 2018.

Rozporządzenie Rady Ministrów z dnia 20 lutego 2003 r. w sprawie szczegółowych zasad udziału pododdziałów i oddziałów SZ RP w zapobieganiu skutkom klęski żywiołowej lub ich usuwaniu (Dz. U. z 2003 r. Nr 41, poz. 347).

Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (Dz. U. z 1967 r. Nr 44, poz. 220).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2019 r., poz. 1398).

Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (Dz. U. z 2007 r. Nr 62, poz. 558, art. 18).

Ustawa o zarządzaniu kryzysowym (Dz. U. z 2002 r. Nr 82, poz. 590, art. 25, ust. 3).

http://archiwum2013.mon.gov.pl/pl/strona/371/PG_273.html, dostęp: 25.04.2020.

https://archiwum2019-bip.mon.gov.pl/przydatne-informacje/artykul/partole-rozminowania/ilosc-oraz-struktura-patroli-rozminowania-i-grup-nurkow-minerow-1032477/, dostęp: 25.04.2020.

http://rczpi.wp.mil.pl/pl/36_61.html, dostęp: 25.04.2020.

Zbiorcze zestawienia wyników działań patroli rozminowania udostępnionych przez Dowództwo Generalne Rodzajów Sił Zbrojnych (DG RSZ) – materiały niepublikowane.

Barbara Standarska
barbara.standarska@gmail.com
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Nowe zastosowania bezzałogowych statków powietrznych podczas realizacji zadań militarnych

Wstęp

Rynek bezzałogowych statków powietrznych (BSP) to prężnie rozwijająca się gałąź gospodarki. Wykorzystanie ich to szerokie spektrum codziennego życia, platformy, które są dostępne na rynku, zaczynają się od micro do super heavy. Chińska firma zaprezentowała w Las Vegas Ehang 184 – drona taksówkę. Pierwsze testy na rynku komercyjnym odbędą się w USA. Z taksówki może skorzystać jedna osoba, która na tablecie wskazuje, dokąd chce lecieć. Dron jest w pełni zautomatyzowany i nie potrzebuje ingerencji pasażera do wykonania lotu (sam startuje, ląduje i określa trasę przelotu).

Drony również chętnie są wykorzystywane w rolnictwie czy w trakcie akcji poszukiwawczych. Nowoczesne kamery multispektralne czy programy rozpoznawania sylwetek na podstawie zdjęcia wprowadzają platformy w niekonwencjonalny i innowacyjny poziom na rynku światowym.

W Siłach Zbrojnych zastosowanie BSP w czasie pokoju, jak i wojny, to ogromny wachlarz zastosowań. Każde zadanie, misja, jest inna, w związku z czym wyposażenie oraz doposażenie drona na potrzeby wojskowe jest bardzo zróżnicowane. Coraz większe znaczenie ma liczebność i inwazja małych nano-dronów, które w ogromnych ilościach ciężko jest zneutralizować. Terroryści podczas ataków wykorzystują

nie tylko sprzęt wojskowy, ale również łatwo dostępne cywilne konstrukcje. Na rynku również powstają systemy tzw. antydrony, które mają skutecznie walczyć z wszystkimi platformami dostępnymi na rynku.

Istotnym problemem są uregulowania prawne dotyczące wykonywania lotów w zasięgu i poza zasięgiem wzroku. Pomimo nowelizacji Ustawy o prawie lotniczym [Dz. U. z 2019 r. poz. 1580 t.j.] oraz niektórych innych ustaw w 2019 r., uszczegółowienie zapisów, kto i w jakim zakresie może wykonywać loty BSP oraz jakie czynności powinien podjąć operator przed wykonaniem lotu, pozwalają na szybką i ewentualną interwencję służb mundurowych.

Celem rozdziału jest nakreślenie nowych zastosowań bezzałogowych statków powietrznych oraz możliwości ich wykorzystania z wkraczającą w Polskie Siły Zbrojne technologią. Nie zapominając o zagrożeniach oraz komercjalizacji tej gałęzi gospodarki.

Obecne wyposażenie Sił Zbrojnych

Polskie wojsko jest wyposażone w zestawy należące do grupy „Class I", takie jak zwiadowcze Orbitery, FlyEye, Scan Eagle, RQ-21A Black Jack oraz płatowiec uderzeniowy Warmate [„Polska Zbrojna" 2019, nr 6, s. 7].

Bezzałogowe statki powietrzne dzielimy na różne grypy, biorąc pod uwagę dane techniczne, takie jak masa startowa, długość lotu czy maksymalną wysokość lotu. Siły Zbrojne RP używają podziału NATO-wskiego bezzałogowych statków powietrznych, czyli:

„Class I" obejmuje platformy o masie startowej max 150 kg i o maksymalnym zasięgu 50 km oraz zastosowaniu wsparcia operacji na poziomie taktycznym na szczeblu sekcji, drużyny, plutonu, kompanii. Plus trzy podgrupy: small (konstrukcja ważąca od 20 do 50 kg i zasięgu ok. 50 km), mini (masa startowa od 2 do 20 kg i zasięg do 25 km), micro (drony mniejsze niż 2 kg i zasięgu maksymalnym 5 km).

„Class II" obejmuje konstrukcje o masie startowej od 150 do 600 kg i o maksymalnym zasięgu 200 km, wykorzystywane we wsparciu operacji na szczeblu batalionu, brygady.

„Class III" obejmuje bezzałogowe statki powietrzne o masie startowej od 600 kg i zasięgu powyżej 200 km, przeznaczone do wsparcia na poziomie operacyjnym i strategicznym do 3000 m nad poziomem gruntu. Class III dzieli się na podgrupy: Strike/Combat, Hale, Male; [Arjomandi 2012, Aeronautical Engineering, online].

Wojska Obrony Terytorialnej (WOT) wyposażone są w Fly Eye (grupa „Class I"). Według koncepcji rozwoju WOT docelowo w każdym województwie w Polsce będą się znajdowały bezzałogowe statki powietrzne, który mają zasięg działania 50 km, posiadają ładunek uderzeniowy 4 kg z maksymalnym czasem lotu do 3 h. Brygady Obrony Terytorialnej mają określone rejony działania, czyli tzw. stałe rejony odpowiedzialności, gdzie żołnierze zawodowi oraz żołnierze OT wykonują zadnia w czasie pokoju, kryzysu oraz wojny. Płatowiec żołnierzy WOT można doposażyć w optoelektronikę np. w kamerę dzienną, na podczerwień, dalmierz laserowy czy radar szczelinowy i następnie prowadzić działania rozpoznawcze. Co pozwoli na efektywniejsze wykonanie rozkazu i dostarczenie wiarygodnych informacji. Brygady I etapu formownia WOT są wyposażone w bezzałogowe statki powietrzne, a co za tym idzie grupy rozpoznania obrazowego realizują powierzone im zadania.

Jednostki specjalne mają dysponować dronami Black Hornet Nano Class-y I (mikro) inaczej zwanymi czarny szerszeń, których waga wynosi 16 g, czas lotu 30 min, maksymalna prędkość 18 km/h, maksymalna wysokość 50 m. [„Polska Zbrojna" 2019, nr 6, s. 6]. Mikrodron będzie standardowym indywidualnym wyposażeniem dowódcy drużyny. „Czarny szerszeń" jest wyposażony w trzy kamery z możliwością obrotu o 45 stopni i ma za zadanie przeprowadzić rekonesans w obszarze do 1 km oraz dostarczyć niezbędnych informacji o przeciwniku operatorowi. Zebrany materiał rozpoznawczy (np. w tunelach, jaskiniach, przesmykach) ma wesprzeć w dokonaniu analizy sytuacji taktycznej i podjęciu decyzji o ewentualnym szturmie, wycofaniu lub określeniu siły wsparcia potrzebnej do przeprowadzenia ataku na przeciwnika. Bardzo dobrze będzie się sprawdzał także w terenie zurbanizowanym. Ciężka do dostrzeżenia gołym okiem platforma jest dobrym dodatkowym uzbrojeniem żołnierza. Ewentualna utrata sprzętu jest znikoma w stosunku do życia żołnierza.

Strategicznym miejscem jest 12 Baza Bezzałogowych Statków Powietrznych w Mirosławcu, gdzie przy współpracy z 52 Grupą Ekspedycyjną US Air Force (52nd Expeditionary Operations Group Detachment 2) prowadzone są misje rozpoznawcze oraz patrolowe nad wschodnią flanką NATO, jest to jedyna taka baza w Polsce. 12 BBSP dysponuje dornami Clasay-I Orbiter o zasięgu działania do 15 km i maksymalnym czasie lotu 1,5 h. Wojska Amerykańskie dysponują MQ-9 Reaper o zasięgu działania do 5900 km i maksymalnym czasie lotu 28 h. Flota statków powietrznych w 12 Bazie ma być zwiększona, czego skutkiem będzie lepsze wykorzystanie miejsca stacjonowania do wykonywania zadań.

Automatyczność bezzałogowych statków powietrznych

Bezzałogowe statki powietrzne od dawna towarzyszą żołnierzom podczas realizacji zadań militarnych. Zostały docenione szczególnie podczas konfliktu zbrojnego w Afganistanie, gdy dostępne systemy uzbrojenie były niewystarczające do skutecznej walki z terrorystami. Trudność wykrycia przeciwnika działała systematycznie na szkodę wojsk koalicyjnych. Dlatego podjęto decyzje, aby wykorzystać na wielką skalę BSP do działań rozpoznawczych w tym konflikcie.

Zasadniczy wpływ na konflikt na Ukrainie i w Syrii miały małe drony, ogólnodostępne na rynku cywilnym. Zostały one tylko nieznacznie dostosowane do potrzeb i zadań, które miały wykonać. Głównym ich zadaniem było rozpoznanie oraz wsparcie pododdziałów lądowych. Nie są wykorzystywane do atakowania dużych celów, baz czy elementów infrastruktury krytycznej, lecz są ogromnym zagrożeniem oraz wsparciem przy działaniach militarnych. Materiały prasowe oraz miesięczniki wojskowe wspominają, że na lotniku w Syrii zniszczono rosyjskie statki powietrzne przy skoordynowanym ataku roju małych dronów. Podobnych metod użyto na Ukrainie, gdzie zniszczono składy amunicji armii ukraińskiej. Pod cywilne małe drony przymocowano granaty zapalające i skierowano je w celu spustoszenia danego rejonu [„Polska Zbrojna" 2019, nr 6, s. 6].

Prowadzone są prace nad zacieśnieniem korelacji pomiędzy lotnictwem załogowym i bezzałogowym. BSP będą realizować nowe zadania tak, aby zmniejszyć zagrożenie dla pilotów. Cel tych zastosowań jest taki, aby maszyny się uzupełniały, a także, aby móc wykorzystać oraz zmodernizować BSP tak, by mogły wykonywać zadania najbardziej zagrażające życiu załóg samolotu np. podczas pokonywania obrony przeciwnika, czyli wszędzie tam, gdzie jest nagromadzona liczba środków ogniowych oraz gdzie misje są monotonne czy długotrwałe.

W pierwszym kwartale 2019 r. podczas eventu International Airshow w Avalon 2019 r. w Australii został ogłoszony przez firmę Boeing nowy projekt drona, który ma latać obok tradycyjnego samolotu podczas realizacji zadań. Dron Loyal Wingman (Lojalny Skrzydłowy) łączy bezzałogowy autonomiczny system z samolotami załogowymi. Boeing zwraca uwagę, iż dron będzie swoistą „ochroną sił powietrznych" oraz dodatkiem dla szwadronów do realizowania najniebezpieczniejszych manewrów i misji. Projekt objął trzy wersje dronów, każdy z nich wygląda jak futurystyczny myśliwiec pozbawiony kokpitu. Mierzy 11,58 metrów długości i lata na odległość ok. 3700 km, reszta danych technicznych jest utajniona przez producenta. Wyposażony został w podstawowy zestaw misji wywiadowczych, rozpoznawczych i w każdym momencie można go przekonfigurować do potrzeb

danego zadania. Brak jest informacji, czy dron będzie wyposażony w środki bojowe, lecz będzie latał pół-automatycznie ,będąc kontrolowanym przez operatora lub pilota statku powietrznego [Łysoń 2019, online].

Wingmany docelowo będą działać wspólnie z samolotami piątej generacji czyli z multizadaniowym F35 lub F-22. F-35 jest trudny do wykrycia dla radarów. Zbiera wiele informacji i ma zdolność przetwarzania oraz przekazywania ich w czasie rzeczywistym do wszystkich, którzy są zaangażowani w wykonanie danego zadania. Jest to możliwe dzięki urządzeniu, które znajduje się na wyposażeniu nowoczesnego samolotu. System identyfikacji „swój obcy" dokładnie określa, kto jest z wojsk własnych, zaś kto z wojsk obcych. Dostarcza wszystkim dowódcom lepszy i dokładniejszy pogląd na aktualną sytuację na polu walki. Z tego typu samolotu będą mogły korzystać wszystkie rodzaje siły zbrojnych, co pozwoli na efektowniejsze wykorzystanie posiadanej floty lotniczej [„Polska Zbrojna" 2019, nr 8, s. 8].

W miesiącu sierpniu br. na terenie Federacji Rosyjskiej odbył się 32-minutowy oblot w pełni automatycznego BslAltius-U na wysokości do 800 m. Waży on ok. 6 ton i jest w stanie przenieść ładunek o masie do 2 ton. Dodatkowo został zastosowany satelitarny system nadzoru i łączności, co zwiększyło zasięg drona. Rezultatem oblotu jest zakończenie testów i etapu konfiguracji systemu, który ma wykonywać zadania rozpoznawcze [Przemysł lotniczy, Przemysł zbrojny 2019, online].

Przewaga w liczebności

Innym uwarunkowaniem zastosowania bezzałogowych statków powietrznych jest ich liczebność np. podczas prowadzonego ataku na polu walki. Gromada dronów wymaga spójnego systemu koordynowania misji, tak aby były zdolne do wykonania jednego zadania bez zakłócania się i dostarczenia niezbędnych informacji np. rozpoznawczych.

Pod tym kątem Amerykanie i Chińczycy prowadzą badania oraz znajdują nowe rozwiązania napotkanych problemów w czasie próbnych lotów. Skorzystano z tego rozwiązania podczas ceremonii otwarcia zimowych igrzysk olimpijskich w Pjoneczangu, gdzie wykorzystano około 1,2 tys. bezzałogowych statków powietrznych. Latające równocześnie w pełni zautomatyzowane zostały wykorzystane w celu efektywnych pokazów. Ten efekt również został zaimplementowany w bojowe gromady dronów [https://pl.sputniknews.com/swiat/201804127755634-Sputnik-Pentagon-drony-Gremliny-wideo, online].

Amerykański Program „LOCUST" (*Low – Cost UAV Swarming Technology*) tj. szarańcza, powstał w celu wsparcia technologii marynarki wojennej USA. Początkowo do startu Perdix's wykorzystywano wyrzutnię naziemną i wystrzeliwano je niczym pocisk. Otwierały skrzydła i dalej latały już automatycznie. Jesienią 2016 roku przeprowadzono test wyrzucenia szarańczy z samolotów. Wykorzystano do tego celu trzy samoloty F/A-18 Super Hornet i uwolniono niemal flotę 100 bezpilotowców. Szarańcza wypuszczona z łatwych do transportu skrzyń komunikuje się ze sobą i wykonuje lot automatyczny. Zbierają one dane równocześnie i wspólnie wykonują jedną misję. Gromadzą informację rozpoznawcze w wielu płaszczyznach, co pozwala na szczegółowy i rzetelny obraz sytuacji. Dodatkowo zwiększa to przewagę nad przeciwnikiem, który nie jest w stanie zareagować na czas i w tak dużej liczebności na statki powietrzne przeciwnika przed zebraniem materiałów.

Program „Gremlin" to kolejny projekt Amerykańskiej Agencji Zawansowanych Projektów Badawczych w Obszarze Obronności. Gremlin (nieco większy niż Perdix) przygotowany jest do wykonywania automatycznych lotów oraz wyposażony w różnorodne zestawy wyspecjalizowanego sprzętu do realizacji misji bojowych. Dodatkowo Gremlin może startować z platformy powietrznej, takiej jak samolot transportowy czy myśliwiec, np. zS-130 Hercules, który jest samolotem przystosowanym do przenoszenia bezzałogowca [Husseini 2018, online].

Gremlin, Perdix i Walkir to wytrzymały sprzęt z niedrogich i łatwo dostępnych surowców. Dzięki temu utrata sprzętu jest mało odczuwalna i ponosi się znikome straty finansowe w porównaniu do wartości nowoczesnego myśliwca. W oprogramowaniach bezzałogowych statków powietrznych wykorzystuje się automatyczność i sztuczną inteligencje. Chodzi o to, aby platformy wykonywały jak najwięcej zadań samodzielnie, bez ingerencji operatora (nie tylko start i lądowanie). Systemy kontroli pułapu lotu czy siły wiatru są wykorzystywane w chwili obecnej. Najnowsze projekty zakładają, że sztuczna inteligencja sama będzie rozpoznawać zbliżający się cel i decydować, czy zneutralizować go, reagować w nietypowych sytuacjach oraz dostosowywać się do panujących warunków na polu walki. Oczywiście jest to etap końcowy, zaś do tego momentu to człowiek (tzw. *kill-switcher*) będzie decydował o zniszczeniu celu.

Zagrożenia

Wykorzystywanie sztucznej inteligencji oraz bezzałogowych statków powietrznych na tak szeroką skalę niesie za sobą również pewne zagrożenia. Każdy system informatyczny, tak jak przesyłanie informacji między operatorem i platformą, musi być chroniony oraz zabezpieczony przed przejęciem łącza. Dane, które są zbierane podczas misji drona, również są narażone na działania przeciwnika. Operator musi mieć pewność, iż zebrany materiał jest wiarygodny i można go przekazać do dalszej obróbki i analizy.

W Stanach Zjednoczonych zarejestrowano przypadek, kiedy operator wojskowy utracił panowanie nad dronem i nie mógł wykonywać zaplanowanej misji. W tym przypadku atak hakerów powiódł się, co było przyczyną większego skupienia się na ulepszeniu oprogramowania zabezpieczającego.

W systemach komercyjnych wykrywania i neutralizacji dronów wykorzystano sensory m.in. radiowe, akustyczne, radarów oraz kamer wizyjnych, które wykrywają drony niezależnie od warunków atmosferycznych (mgły, deszczu, chmury, śniegu, wysokich i niskich temperatur, słońca) i pory dnia. System antydronowy Jastrząb jest wyposażony w software i wykrywa oraz unieszkodliwia niezliczoną liczbę platform w 100%. Wysłany sygnał zakłócający zrywa łączność pomiędzy dronem a operatorem oraz wymusza bezpieczne lądowanie BSP na ziemi w najgodniejszym miejscu z dala od obiektów szczególnych albo jego odesłanie z powrotem do operatora. System Jastrząb można wykorzystywać na platformach mobilnych, jak i stacjonarnie. Monitorowanie terenu przez radar w obrębie 360 stopni i 3 km pozwala na skuteczne wykrycie drona nieprzyjaciela i zestrzelenie.

System antydron może być wykorzystywany w działaniach militarnych i w środowisku cywilnym np. na imprezach masowych czy lotniskach. Ochrona wojskowego i cywilnego lotniska oraz obiektów szczególnych infrastruktury ma ogromny wpływ na zwiększenie bezpieczeństwa i ochronę przed przeciwnikiem.

Zakończenie

Istotnym przedstawionym elementem jest wykorzystanie BSP z nową technologią Sił Zbrojnych i w szerszym zakresie w działaniach militarnych. Zagrożenie, jakie płynie z rynku cywilnego i odstępczości różnego rodzaju platform, jest niepokojące.

Bezzałogowe Statki Powietrzne to nieodzowny i ciągle rozwijający się obszar technologiczny. Nowe zastosowania BSP w czasie realizacji zadań militarnych oraz współpraca platform z innymi statkami powietrznymi, które przekazują obraz na bieżąco, pokazują, iż efektowne rozpoznanie i płynny przekaz informacji jest nieodzownym elementem w trakcie konfliktu zbrojnego. Co za tym idzie, liczą się wykorzystanie nowoczesnej techniki do wykonywania najniebezpieczniejszych zadań i ograniczenie zagrożenia dla załóg statków powietrznych. Koszty ekonomiczne utraty sprzętu są znikome w stosunku do życia wyszkolonego żołnierza.

Gromady bezzałogowych statków powietrznych mają ogromną przewagę liczebną nad przeciwnikiem i zbierają informacje w jednym czasie z danego obszaru. Pozwala to na połączenie obrazu z wszystkich dronów, co daje jeden kompatybilny obraz, który jest przekazywany w czasie rzeczywistym do operatora lub samolotu. Statki powietrzne piątej generacji są wyposażone w system, który przetwarza obraz z wszystkich platform i przekazuje jeden pełny do operatora na ziemi.

Dynamicznie rozwijająca się gałąź uzbrojenia, jaką są bezzałogowe statki powietrzne, będzie wykorzystywana w całej strukturze siły zbrojnych. Docelowo każdy żołnierz na stanowisku dowódczym, rozpoczynając od dowódcy sekcji, będzie miał do dyspozycji bezzałogowe statki powietrzne. Pozwoli na wykorzystanie sprzętu w najbardziej niebezpiecznych działaniach oraz zmniejszenie narażenia żołnierza na ewentualny atak, a co za tym idzie, na ocalanie życia ludzkiego.

Wykorzystywane w dronach oprogramowanie jest połączone ze sztuczną inteligencją. Platformy podczas lotu w gromadach komunikują się ze sobą i określają najbezpieczniejszą trasę przelotu. Sztuczna inteligencja jest również wykorzystywana podczas określania, czy zbliżająca się platforma to swój czy nieprzyjaciel. Docelowo to system ma decydować, czy zniszczyć cel. Takie rozwiązanie niesie za sobą wiele zagrożeń np. podczas gdy przeciwnik przejmie panowanie nad dronem, w związku z czym system musi być bardzo dobrze szyfrowany i zabezpieczony na ewentualne ataki hakerów.

System antydronowy ma na celu zwiększyć i wzmocnić obronę przed przeciwnikiem. Walka z gromadami dronów jest bardzo trudna ze względu na ich liczebność. Szybkie wykrycie i neutralizacja platform pozwalają na skuteczną obronę przed atakiem nieprzyjaciela oraz zwiększenie bezpieczeństwa w najbardziej kluczowych miejscach.

Bibliografia

„Polska Zbrojna”, 2019, Czerwiec,cnr 6.

„Polska Zbrojna”, 2019, Sierpień, nr 8.

Ustawa z dnia 3 lipca 2002 r o Prawie lotniczym (Dz. U. z 2019 r., poz. 1580 t.j.).

Źródła internetowe

Arjomandi M. (2012), *Mech Eng 3016 Aeronautical Engineering* [online], http://web.archive.org/web/20121021021237/http://personal.mecheng.adelaide.edu.au/maziar.arjomandi/aeronautical%20engineering%20projects/2006/group9.pdf, dostęp: 26.08.2019.

Husseini T. (2018), *Gremlins are coming: DARPA enters Phase III of its UAV programme* [online], www.army-technology.com/features/gremlins-darpa-uav-programme, dostęp: 24.08.2019.

https://pl.sputniknews.com/swiat/201804127755634-Sputnik-Pentagon-drony-Gremliny-wideo, dostęp: 25.08.2019.

Łysoń M. (2019), *Dron Loyal Wingman od Boeing wspomoże myśliwce w walce*, https://whatnext.pl/dron-loyal-wingman-od-boeing-wspomoze-mysliwce-w-walce/, dostęp: 25.08.2019.

Przemysł lotniczy, Przemysł zbrojny (2019), „Altus-U oblot”, https://www.altair.com.pl/news/view?news_id=28745, dostęp: 25.08.2019.

www.whatnext.pl/dron-loyal-wingman-od-boeing-wspomoze-mysliwce-wwalce, dostęp: 24.08.2019.

Janusz Liber
januszliber@wp.pl
Fundacja Instytut Wywiadu Gospodarczego

Kontrwywiad biznesowy jako jeden z elementów bezpieczeństwa korporacyjnego na przykładzie międzynarodowych organizacji – wybrane elementy

Wstęp

Bezpieczeństwo korporacyjne odpowiada za koordynację działań z obszaru bezpieczeństwa w organizacji, w ścisłej współpracy z kierownictwem biznesowym oraz wszystkimi osobami funkcyjnymi zarządzającymi poszczególnymi elementami systemu bezpieczeństwa, np. zapewnienie ciągłości działania, zarządzanie zgodnością[1], ochrona fizyczna, BHP, itp., w celu ochrony interesów biznesowych organizacji, ludzi, zysków oraz reputacji, jak również minimalizacji ryzyka [Cabric 2015, s. 23].

Bezpieczeństwo korporacyjne jest również odpowiedzialne za przygotowanie wszystkich pracowników firmy do realizacji zadań w systemie bezpieczeństwa

[1] *Compliance* – zapewnienie zgodności to zapewnienie przestrzegania przepisów prawa, regulacji wewnętrznych oraz standardów rynkowych, odpowiednio poprzez funkcję kontroli oraz zarządzanie ryzykiem braku zgodności. Proces zarządzania ryzykiem braku zgodności realizowany jest poprzez identyfikację, ocenę, kontrolę i monitorowanie ryzyka braku zgodności działalności organizacji z przepisami prawa, regulacjami wewnętrznymi i standardami rynkowymi oraz raportowanie w tym zakresie [http://justcomply.pl/pl/compliance-2/, dostęp: 22.06.2019].

organizacji, realizowanych w ramach ich codziennych obowiązków. Oprócz tradycyjnych obszarów bezpieczeństwa, jak ochrona fizyczna i zabezpieczenia techniczne, bezpieczeństwo korporacyjne obejmuje bezpieczeństwo informacji, zarządzanie ciągłością działania, odtwarzanie awaryjne[2], poprzez cykl życia produktów i kluczowych procesów, aby zapewnić rzeczywiste wsparcie w osiąganiu celów biznesowych organizacji. Bezpieczeństwo korporacyjne odpowiada za analizę i kwantyfikację ryzyka; opracowanie, planowanie, wdrażanie i kontrolowanie środków bezpieczeństwa, jak również wskaźniki ich wydajności i efektów, w celu przewidywania trendów, zapobiegania incydentom oraz rozumienia ich korelacji w różnych częściach korporacji i na różnych etapach procesów biznesowych. Oprócz wiedzy i doświadczenia w zakresie bezpieczeństwa, kluczowymi kompetencjami dla zarządzania korporacyjnego w zakresie bezpieczeństwa, są: uczciwość, przedsiębiorczość, orientacja na ludzi, umiejętności zarządzania, jak również umiejętność skutecznego komunikowania się i przekonywania [Cabric 2015, s. 23].

Rola i zadania bezpieczeństwa korporacyjnego

Rolą bezpieczeństwa korporacyjnego jest ochrona organizacji, technologii, pracowników, zasobów technicznych oraz danych klientów przed zagrożeniami wewnętrznymi i zewnętrznymi. Jego ostatecznym celem jest zapewnienie prawidłowego funkcjonowania firmy i ograniczenie ryzyka. Dla realizacji przedmiotowych celów korporacja może zatrudniać odpowiednich pracowników, kupować oprogramowanie zabezpieczające, jak również przechodzić na bardziej zaawansowane technologie w celu ochrony materialnych i niematerialnych aktywów firmy [*What is Corporate Security?*, https://bizfluent.com/info-8057178-corporate-security.html]. Podstawowe elementy (zadania) bezpieczeństwa korporacyjnego w międzynarodowej organizacji to[3]:

[2] *Disaster recovery* – (z angielskiego: odzyskanie po awarii, odtwarzanie awaryjne) – proces związany z odtworzeniem utraconych danych. Jest to część *Business Countinuity* – czyli zapewniania ciągłości. Rozwiązania *Disaster Recovery* skupiają się na przywróceniu przetwarzania po awarii (katastrofie) uniemożliwiającej pracę w Ośrodku Podstawowym. Ośrodek Podstawowy rozumiany jest jako infrastruktura informatyczna (pomieszczenia, zasilanie, serwery, sieć, obsługa itp.), używana w czasie normalnej pracy przedsiębiorstwa lub instytucji [https://mfiles.pl/pl/index.php/Disaster_recovery, dostęp: 22.06.2019].

[3] Opracowanie własne na podstawie: Crump 2015; *What is Corporate Security?*, https://bizfluent.com/info-8057178-corporate-security.html, dostęp: 17.06.2019. Badania własne autora.

- fizyczna ochrona osób i mienia,
- zapewnienie bezpieczeństwa osobowego,
- zarządzanie ryzykiem,
- zarządzanie kryzysowe,
- zarządzanie ciągłością działania,
- odtwarzanie awaryjne,
- przeciwdziałanie cyberprzestępczości,
- zarządzanie bezpieczeństwem danych oraz informacji,
- zarządzanie informacjami o nieprawidłowościach,
- przeciwdziałanie nadużyciom,
- przeciwdziałanie korupcji,
- przeciwdziałanie praniu brudnych pieniędzy,
- przeciwdziałanie szpiegostwu gospodarczemu,
- przeciwdziałanie konfliktowi interesów,
- przeciwdziałanie nieuczciwej konkurencji,
- prowadzenie dochodzeń wewnętrznych,
- ochrona marki (znaku towarowego),
- zapewnienie jakości (produktów i usług),
- zarządzanie zgodnością,
- bezpieczeństwo i higiena pracy,
- inne elementy (zarządzanie konfliktami oraz elementy pochodne).

Aktualne trendy w zarządzaniu bezpieczeństwem korporacyjnym zmierzają do podkreślenia znaczenia odporności organizacji na gwałtowne zmiany oraz kryzysy, w związku z czym, dla scharakteryzowania cech firmy przygotowanej na wystąpienie przywołanych elementów ryzyka, coraz powszechniej stosuje się anglojęzyczne określenie *resilience*[4], w kolokacjach*: organisational resilience*[5] lub też *resilient organisation*[6]*.* Prof. David Denyer charakteryzuje odporność organizacyjną jako zdolność organizacji do przewidywania, przygotowywania, odpowiadania, jak również dostosowania do nagłych zmian i zakłóceń, w celu zapewnienia nieprzerwanego funkcjonowania (przetrwania) korporacji [Denyer 2017, s. 3].

W 2017 r. 29 osób, w tym menedżerowie znanych międzynarodowych sieci handlowych, stanęło przed sądem. Według prokuratury przyjmowali oni łapówki w zamian za wprowadzenie do sprzedaży i lepszą ekspozycję towarów, m.in. alkoholi,

[4] Ang. sprężystość.
[5] Ang. sprężystość (odporność) organizacyjna.
[6] Ang. sprężysta (odporna) organizacja.

wody mineralnej oraz napojów (łącznie 49 firm). Rekordzista, pracownik niemieckiej sieci handlowej, miał przyjąć 4,1 mln zł. Do przestępstw dochodzić miało w latach 2005–2010. Siedmiu przedstawicieli dostawców (producentów) miało tworzyć zorganizowaną grupę przestępczą, której celem było korumpowanie pracowników jednej z niemieckich i francuskich sieci handlowych[7].

Koszty, jakie banki ponoszą z tytułu strat wynikających z ryzyka operacyjnego, sięgają kilku, a nawet kilkunastu milionów złotych rocznie, ale są oczywiście znacznie niższe niż odpisy kredytowe wynoszące od kilkudziesięciu do kilkuset milionów w skali roku. Po ekspozycji na ryzyko widać, że to operacyjne nie jest problemem pomijalnym – na koniec 2017 r. kwota ekspozycji na ryzyko operacyjne w polskim sektorze bankowym szacowana była na 79 mld zł. Ryzyko operacyjne wyraźnie więc dokłada się do wymogów dotyczących wielkości kapitału, które banki muszą utrzymywać (co obniża jednak ich rentowność)[8].

Firma spedycyjna, działająca w Trójmieście, utratę pierwszych sześciu najważniejszych klientów i pół miliona złotych szybko skojarzyła z odejściem czterech pracowników, którzy zatrudnili się w przedstawicielstwie szwedzkiej konkurencji. Posługiwali się oni szczegółami dotyczącymi kontraktów, jakie ich były pracodawca zawarł z kontrahentami, tras przejazdów itd., mimo że podpisali wcześniej umowy o zakazie konkurencji i zachowaniu poufności informacji przez trzy lata od ustania stosunku pracy. Prokuratura odmówiła wszczęcia dochodzenia, gdyż firma nie mogła przedstawić „twardych dowodów". Jej pliki, znalezione przez policję w komputerach konkurencji, nie miały znaczenia, bo podejrzani po prostu zaprzeczyli, że je wykradli [https://mycompanypolska.pl/artykul/518/zarzadzanie-zlodzieje-firmowych-tajemnic].

Barings Bank to jeden z najstarszych i najbardziej poważanych banków handlowych w Wielkiej Brytanii. Za jego spektakularny upadek odpowiada wyłącznie jeden makler – Nick Leeson, zatrudniony w jego singapurskim oddziale [https://mfiles.pl/pl/index.php/Upadek_Barings_Bank]. W lutym 1995 roku Barings Bank upadł na skutek gigantycznych strat, które opiewały na 1,4 mld dolarów. Przyczyną upadku była działalność spekulacyjna Lessona, możliwa ze względu na fakt, iż był on odpowiedzialny za kontrolę transakcji zawieranych przez maklerów, w tym

[7] Kulisy afery korupcyjnej: 50–70 menadżerów sieci decyduje o zakupach Polaków [http://www.portalspozywczy.pl/handel/wiadomosci/kulisy-afery-korupcyjnej-50-70-menadzerow-sieci-decyduje-o-zakupach-polakow,124373.html, dostęp: 26.06.2019].

[8] Oczywiście dominuje ryzyko kredytowe wyceniane na 944 mld zł. Banki: ile tracą na oszustwach pracowników i wyłudzeniach? [https://www.parkiet.com/Parkiet-PLUS/306269958-Banki-ile-traca-na-oszustwach-pracownikow-i-wyludzeniach.html, dostęp: 1.07.2019].

samego siebie. Stworzyło mu to możliwość obejścia kontroli wewnętrznej [Dudziak, Szpakowska 2013].

Jak wskazano powyżej, niewłaściwe funkcjonowanie organizacji w obszarze bezpieczeństwa korporacyjnego może wywoływać różnorodne, negatywne skutki: od utraty reputacji, poprzez utratę zaufania interesariuszy oraz obniżenie wartości firmy, wymierne straty finansowe, do upadku organizacji włącznie.

Znaczenie ładu korporacyjnego dla bezpieczeństwa organizacji

Podstawą właściwego zarządzania organizacją międzynarodową, w tym w obszarach bezpieczeństwa korporacyjnego, jest *GRC* – termin ogólny, obejmujący podejście firmy do trzech obszarów (*governance, risk management and compliance)*, które pomagają zapewnić, że organizacja rzetelnie osiąga cele, rozwiązuje problemy niepewności i działa w sposób uczciwy [*OCEG Capability Model GRC Standards,* ss. 215–224]. Ład korporacyjny (*corporate governance*) to połączenie procesów ustanowionych i realizowanych przez dyrektorów/ zarząd, które znajdują odzwierciedlenie w strukturze organizacji oraz w sposobie, w jaki jest ona zarządzana i kierowana dla osiągania określonych celów. Zarządzanie ryzykiem *(risk management)* polega na przewidywaniu i zarządzaniu ryzykiem, które może utrudnić organizacji osiąganie założonych celów, w tym podczas funkcjonowania firmy w warunkach niepewności. Zgodność *(compliance)* odnosi się do przestrzegania wyznaczonych granic (przepisów prawa, polityk i procedur firmy) [Weidenmier, Ramamoorti 2006, ss. 205–219].

Krytycznym elementem *GRC* jest kultura organizacji, która w międzynarodowych korporacjach bardzo często określana jest terminem *tone at the top*[9]. Kluczowym czynnikiem kultury korporacyjnej jest zakres, w jakim firma i jej ludzie pojmują uczciwość i obowiązujące wartości etyczne. Jest to szczególnie istotne,

[9] *Tone at the top* – to pojęcie, które powstało i początkowo przyjęło się w środowisku rewidentów finansowych (audytu finansowego). Polskie środowiska, związane z audytem i rewizją finansową, tłumaczą to pojęcie jako „przykład z góry", co zawęża właściwe rozumienie tego pojęcia. Bowiem nie chodzi wyłącznie o sam przykład i ustanawiane szczegółowe uregulowania dotyczące funkcjonowania jakiejś społeczności, ale o klimat (kulturę społeczną), jaki tworzony jest i pielęgnowany przez kierownictwa i liderów firm oraz instytucji. [https://www.salon24.pl/u/starywrocek/508336,tone-at-the-top-w-polsce-wybor-nalezy-do-nas, dostęp: 3.07.2019.
Więcej: https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/tone-at-the-top-research.pdf.

ponieważ firmy działające na bazie uczciwości oraz zdefiniowanych i zaakceptowanych zasad etyki rzadko wpadają w tarapaty – dodatkowo traktują one przedmiotowe reguły jako podstawę swojego sukcesu. Takie firmy przyciągają do siebie najlepszych pracowników, jak również najbardziej wymagających klientów, dostawców, finansjerę oraz partnerów biznesowych [Steinberg 2011, s. 3].

Jednym z kluczowych elementów *GRC* oraz bezpieczeństwa korporacyjnego jest zarządzanie ryzykiem, jednakże ze względu na objętość oraz cel rozdziału, autor pominie ten element, definiując w dalszej części publikacji wybrane czynniki ryzyka, w celu lepszego przybliżenia tematyki opracowania [zob. szerzej: Neef 2003].

Wybrane determinanty wdrażania bezpieczeństwa korporacyjnego

Sposób organizacji i wdrażania systemu bezpieczeństwa korporacyjnego, w tym elementów kontrwywiadu biznesowego w przedsiębiorstwie, jest zdeterminowany wieloma czynnikami, m.in.:

- rodzajem działalności,
- miejscem prowadzenia działalności,
- strukturą organizacyjną,
- pozycją na rynku (konkurencja i konkurencyjność),
- świadomości interesariuszy oraz kierownictwa,
- lokalnych lub szczególnych przepisów prawa – np. prawny obowiązek wdrożenia określonych procedur[10] lub też ryzyko potencjalnej odpowiedzialności firmy lub jej pracowników za popełnienie określonych czynów zabronionych pod groźbą kary[11].

Przywołane powyżej czynniki sposobu organizowania i wdrażania systemu bezpieczeństwa korporacyjnego są bardzo często współzależne – rodzaj i miejsce działalności wymuszają przestrzeganie określonych wymogów prawa, itp.

W tym miejscu opracowania warto podkreślić, iż pochodną ww. determinantów bezpieczeństwa jest podatność organizacji na ataki, według której dzielimy je na „cele miękkie" – *soft targets* oraz „cele twarde" – *hard targets.* Przedmiotowe

[10] Np. regulacje (globalne, krajowe, branżowe) z obszaru przeciwdziałania praniu brudnych pieniędzy i finansowania terroryzmu lub też przepisy dotyczące ochrony danych osobowych *GDPR (General Data Protection Requirements)*, obowiązujące na terenie Unii Europejskiej od 25 maja 2018 r.

[11] Np. *UK bribery Act, Foreign Corrupt Practices Act.*

określenia mają charakter elastyczny i niekiedy (w zależności od towarzyszących okoliczności), ich rozróżnienie może sprawiać problemy [szerzej zob. Forest 2006]. Dla usystematyzowania tej części rozdziału warto wskazać, iż typowe „cele miękkie" to w większości miejsca ogólnodostępne – szpitale, szkoły, areny sportowe, hotele, domy kultury, kina, kawiarnie i restauracje, centra handlowe, dworce kolejowe, itp. [szerzej zob. Bennett 2007]. „Cele twarde" stanowią kontrast dla „celów miękkich", ponieważ zazwyczaj są dobrze chronione i z reguły ograniczają dostęp osób postronnych – budynki rządowe, instalacje wojskowe, misje dyplomatyczne, obiekty infrastruktury krytycznej.

Z punktu widzenia kontrwywiadu biznesowego, pojęcia *soft, hard target* mają dodatkowe zastosowanie. Są one wykorzystywane do określania poziomu wiedzy (świadomości) „kluczowych" osób (pracownicy, dostawcy towarów i usług, itp.) o zagrożeniach (z kontrwywiadowczego punktu widzenia) dla firmy oraz sposobie postępowania wskazanych osób, w przypadku ich zidentyfikowania, w celu zabezpieczenia interesów pracodawcy oraz interesariuszy, jak również realizacji ich celów biznesowych.

Na podkreślenie zasługuje fakt, iż sposób realizacji działań kontrwywiadowczych w organizacjach wolnorynkowych, szczególnie zaś, funkcjonowanie kontrwywiadu biznesowego może być uwarunkowane obszarem działalności firmy, która ze względu na rodzaj produkcji, np. zamówienia rządowe musi spełniać wymogi określone w przepisach dot. ochrony informacji niejawnych[12]. Kolejnym czynnikiem determinującym funkcjonowanie „służb" kontrwywiadu biznesowego w takich przedsiębiorstwach jest udział zamówień rządowych w ogólnym wolumenie zamówień.

Uwzględniając wyżej przytoczone okoliczności, z punktu widzenia bezpieczeństwa korporacyjnego organizacje wolnorynkowe można podzielić na dwie grupy[13]:

[12] Obowiązek wdrożenia rozwiązań określonych w regulacjach krajowych lub organizacji międzynarodowych np. NATO.

[13] Podział organizacji wolnorynkowych z uwzględnieniem przepisów regulujących ochronę informacji niejawnych jest kluczowy ze względu na fakt, iż jest to jedyny czynnik „wymuszający" zadania i obowiązki przedsiębiorstwa z zakresu bezpieczeństwa, ponieważ pozostałe regulacje ustawowe muszą być solidarnie stosowane przez wszystkich uczestników rynku.

- podmioty spełniające wymogi ochrony obiektów, informacji, osób, itp. ze względu na konieczność wdrożenia przepisów regulujących ochronę informacji niejawnych[14],
- przedsiębiorstwa organizujące przedsięwzięcia z zakresu kontrwywiadu biznesowego, z wyłączeniem przepisów regulujących ochronę informacji niejawnych.

Przedsięwzięcia kontrwywiadu biznesowego/ bezpieczeństwa korporacyjnego, opisane w niniejszym rozdziale, są działaniami, które w przypadku przedsiębiorstw pierwszej grupy powinny zostać przez nie wdrożone (niezależnie od działań wynikających z przepisów ochrony informacji niejawnych), dla zapewnienia realizacji podstawowych celów biznesowych firmy, jak również ochrony istotnych interesów korporacji[15].

Zagrożenia zewnętrzne i wewnętrzne dla organizacji

Celem każdej firmy jest uzyskanie przewagi konkurencyjnej, którą firma powinna utrzymywać – może to być m.in. wytworzenie większego zysku od średniego w branży czy posiadanie znaczącego udziału w rynku. Przewaga konkurencyjna jest to osiągnięcie przez przedsiębiorstwo nadrzędnej pozycji wobec większej liczby konkurentów. Jest ona relatywną miarą jej funkcjonowania na rynku – pozwala na zaoferowanie klientowi usług lub produktów odpowiadających jego oczekiwaniom, a lepszych niż oferty konkurencji. Wyraża się to w wyższej jakości produktu, niższej cenie i lepszej obsłudze lub bardziej kompleksowym zaspokojeniu potrzeb klienta [Encyklopedia zarządzania, https://mfiles.pl/pl/index.php/Przewaga_konkurencyjna].

Mając na uwadze tematykę rozdziału, stwierdzić należy, iż oprócz formalnych (zgodnych z zasadami prawa i regułami rynkowymi) sposobów osiągania przewagi konkurencyjnej [szerzej zob. Godlewska-Majkowska, Skrzypek, Płonka 2016], istnieje ryzyko osiągania takiej przewagi dzięki popełnieniu czynów nieetycznych lub zabronionych pod groźbą kary [*Jak szpieguje się w korporacjach. 10 największych skandali w historii biznesu*]. Zagrożenia dla organizacji biznesowych mogą pojawiać się w rezultacie procesów makroekonomicznych – niezależnych od

[14] Przykładem takiego przedsiębiorstwa jest PKP Energetyka, która w 2015 r. została kupiona przez Fundusz CVC za pomocą Sp. z o.o. Caryville Investments [*Zakończono Prywatyzację PKP Energetyka,* https://www.bankier.pl/wiadomosc/Zakonczono-prywatyzacje-PKP-Energetyka-3414252.html, dostęp: 10.07.2019 r.

[15] W kontaktach z uczciwą, a szczególnie nieuczciwą konkurencją rynkową.

przedsiębiorstwa, jednakże wiele z nich jest wynikiem zorganizowanych działań konkurencji, środowisk przestępczych, nieuczciwych dostawców i odbiorców, nielojalnego personelu oraz organów władzy krajowej[16].

M. Kwieciński oraz K. Pasella opracowali listę zagrożeń wewnętrznych i zewnętrznych dla organizacji biznesowej, które mogą stanowić podstawę do projektowania struktury i działań kontrwywiadu biznesowego w innowacyjnym, nowoczesnym przedsiębiorstwie [Pasella, Kwieciński 2015]:

- sprzeniewierzenie aktywów,
- celowe działanie na szkodę firmy, m.in. w kooperacji z konkurencją,
- szpiegostwo przemysłowe, w tym przy wykorzystaniu cyberprzestępczości,
- naruszenie (zabór) wartości intelektualnych,
- manipulacje i oszustwa księgowe na szkodę lub z zyskiem dla właścicieli czy grup interesu,
- oszustwa i nadużycia podatkowe,
- czyny nieuczciwej konkurencji,
- wspieranie działalności przestępczej, w szczególności prania brudnych pieniędzy i finansowanie terroryzmu,
- korupcja,
- handel informacjami poufnymi przedsiębiorstwa,
- kradzieże, wymuszenia, zastraszanie, porwania dla okupu, przekupstwo, szantaż,
- mobbing oraz molestowanie seksualne,
- nepotyzm.

Przedmiotowa lista jest zbiorem „uniwersalnych" zagrożeń, które mogą indywidualnie lub łącznie wystąpić w każdej organizacji biznesowej, a świadomość ryzyka ich wystąpienia, jak również sposobu przeciwdziałania, wykrywania i procedowania, uzależniona jest od „dojrzałości" firmy[17].

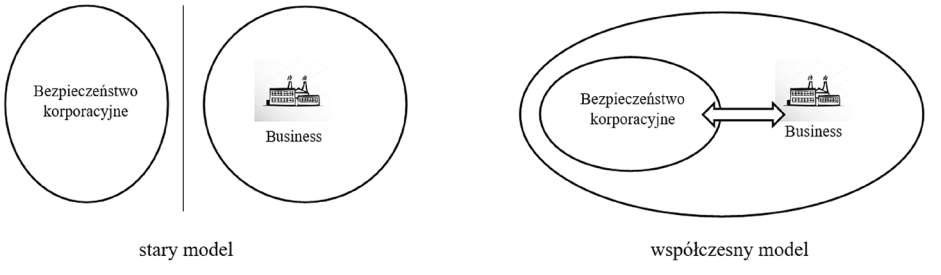
[16] Zob. wybrane opracowania i raporty: *Report to the nations on occupational fraud and abuse: 2014 global fraud study* 2014 oraz Nogacki, Ciecierski 2013.

[17] Szefowie krakowskiej firmy regularnie byli informowani przez księgową, że trzeba uiścić kolejne rachunki: na rzecz kontrahentów, wierzycieli czy kolejne podatki. W konsekwencji księgowa okradła pracodawców na kwotę 5 mln złotych [https://www.tvn24.pl/krakow,50/prokuratura-ksiegowa-wyprowadzila-ponad-piec-milionow,929774.html, dostęp: 1.072019].

Kontrwywiad biznesowy w korporacji

Problematyka osłony kontrwywiadowczej w biznesie nadal zajmuje mało miejsca w literaturze dotyczącej zarządzania organizacjami, która w większości traktuje o teoretycznym i praktycznym podejściu do budowania oraz utrzymywania przewagi konkurencyjnej. Autorzy poświęcają wiele miejsca opisowi metod i sposobów ekspansji na rynku, zapominając przy tym o podejmowaniu koniecznych działań w imię ochrony działań ekspansywnych. Tymczasem bezpieczeństwo prowadzonego biznesu stało się już częścią koncepcji biznesowej [Pasella, Kwieciński 2015, s. 1]. Zmianę współzależności bezpieczeństwa korporacyjnego oraz biznesu obrazuje rys 1.

Rysunek 1. Porównanie „starego" i „nowego" modelu bezpieczeństwa korporacyjnego



Źródło: opracowanie własne na podstawie: Crump 2015, s. 18.

Podstawą właściwego przygotowania programu ochrony kontrwywiadowczej przedsiębiorstwa jest świadomość możliwości wystąpienia określonych, negatywnych zdarzeń mających wpływ na funkcjonowanie organizacji, identyfikacja obszarów podwyższonego / największego ryzyka oraz wdrożenia przedsięwzięć mających na celu ochronę przedsiębiorstwa przed skutkami zdefiniowanych zagrożeń. Uwzględniając przedstawione w niniejszym rozdziale zadania bezpieczeństwa korporacyjnego, jak również listę zagrożeń wewnętrznych i zewnętrznych przedsiębiorstwa, stwierdzić należy, iż służby kontrwywiadu biznesowego w międzynarodowej organizacji skupiają swoje działania na kilku głównych obszarach, obejmujących „powiązane" zagadnienia[18]:

[18] Autor proponuje obszary odpowiedzialności służb kontrwywiadu biznesowego z punktu widzenia menedżera ds. bezpieczeństwa korporacyjnego oraz odporności organizacji – Corporate Security and Resilience Manager, usytuowanego w międzynarodowej korporacji.

- zapewnienie bezpieczeństwa informacji,
- przeciwdziałanie nadużyciom,
- przeciwdziałanie korupcji,
- przeciwdziałaniu nieuczciwej konkurencji,
- przeciwdziałanie zakłóceniom w funkcjonowaniu organizacji, jako rezultatu naruszenia przepisów prawa lub regulacji wewnętrznych,
- przeciwdziałanie zachowaniem nieetycznym,
- prowadzenie postępowań wyjaśniających (dochodzeń wewnętrznych).

Wewnątrzkorporacyjne regulacje z obszaru kontrwywiadu biznesowego

W celu wdrożenia wyżej opisanych działań, międzynarodowe podmioty gospodarcze określają zasady funkcjonowania firmy, jej pracowników oraz kontrahentów poprzez realizację następujące czynności:

- opracowanie odpowiednich regulacji wewnętrznych (polityki, procedury), np.:
  - polityka bezpieczeństwa informacji,
  - polityka przeciwdziałania nadużyciom,
  - polityka antykorupcyjna,
  - polityka konfliktu interesów,
  - polityka przeciwdziałania nieuczciwej konkurencji,
  - polityka *due dilligence,*
  - polityka prowadzenia czynności wyjaśniających,
  - polityka informowania o nieprawidłowościach,
- powołanie stosownych struktur organizacyjnych, np. działów:
  - bezpieczeństwa korporacyjnego,
  - zapobiegania stratom,
  - audytu,
  - prawnego,
  - zarządzania zasobami ludzkimi,
- określenie obowiązków, zadań oraz kompetencji poszczególnych jednostek organizacyjnych[19], jak również ich pracowników:

[19] Np. w jednej z największych sieci handlowych na świecie pion zapobiegania stratom oraz komórka bezpieczeństwa korporacyjnego raportowały do Dyrektora Bezpieczeństwa Korporacji, jednakże w ramach kompetencji określonych przez kierownictwo firmy, komórka zapobiegania stratom odpowiadała za przeciwdziałanie i wykrywanie przestępczości na poziomie sklepów (drobne sprawy), natomiast pion bezpieczeństwa korporacyjnego zajmował się globalnym zabezpieczeniem interesu firmy, gdy zidentyfikowane zagrożenie miało wpływ na ryzyko funkcjonowania organizacji.

– w ramach bieżącej działalności przedsiębiorstwa,
– w czasie kryzysu,
– w przypadku uruchomienia procesów zarządzania ciągłością działania oraz odtwarzania awaryjnego,

- zdefiniowanie zasad współpracy poszczególnych komórek organizacyjnych wewnątrz organizacji:
  – w ramach bieżącej działalności przedsiębiorstwa,
  – w przypadku wystąpienia sytuacji kryzysowej,
  – w przypadku uruchomienia procesów zarządzania ciągłością działania oraz odtwarzania awaryjnego,
- zdefiniowanie zasad współpracy organizacji z dostawcami towarów i usług oraz innych instytucji:
  – w ramach bieżącej działalności przedsiębiorstwa,
  – w przypadku wystąpienia sytuacji kryzysowej,
  – w przypadku uruchomienia procesów zarządzania ciągłością działania oraz odtwarzania awaryjnego,
- zapoznanie z opisanymi regulacjami wszystkich pracowników firmy, a w niektórych organizacjach także dostawców towarów i usług[20].

Cele i zadania służb kontrwywiadu biznesowego są składową celów i zadań bezpieczeństwa biznesowego, które stanowią część zadań i obowiązków wszystkich jednostek organizacyjnych firmy, realizowanych dla zapewnienia realizacji podstawowych celów biznesowych firmy [szerzej zob. Certo, Peter 1989].

Funkcje i zasady działania kontrwywiadu biznesowego

Mając na uwadze fakt, iż działania prewencyjne nie zapewniają pełnej ochrony organizacji przed przestępczością, zachwianiom nieetycznym oraz innym działaniom na jej szkodę, system osłony kontrwywiadowczej powinien spełniać następujące funkcje *(deterrence, detection, defence, defeat*) [*FM 3-19.30 Physical Security* 2001, ss. 16–17] co oznacza że:

- system osłony kontrwywiadowczej powinien być zorganizowany w taki sposób, aby „odstraszał" agresorów zewnętrznych i wewnętrznych od podejmowania działań na szkodę chronionej organizacji. Jeśli sprawca ma alternatywny wybór celu, najprawdopodobniej skieruje swoją aktywność przeciwko organizacji, którą postrzega jako łatwiejszy „kąsek",

[20] Więcej w dalszej części rozdziału.

- w przypadku podjęcia przez agresora działań przeciwko organizacji, w systemie ochrony kontrwywiadowczej biznesu powinny zostać uruchomione elementy odpowiedzialne za wykrywanie poczynań potencjalnego sprawcy, lub też, dostarczenie stosownym jednostkom organizacyjnym przedsiębiorstwa informacji o wystąpieniu czynników ryzyka (pozostających w ich zainteresowaniu), np. *red flags* [szerzej zob. Pasella, Kwieciński 2015, ss. 58–60],
- ochrona aktywów organizacji przed atakiem, realizowana w ramach systemu osłony kontrwywiadowczej – ich celem jest opóźnienie lub zapobieżenie działaniom agresora. Mogą to być elementy utrudniające fizyczny dostęp sprawców do obiektów organizacji (ogrodzenia, bariery, telewizja przemysłowa, kontrola dostępu) lub do jej zasobów informacyjnych zgromadzonych np. w sieciach komputerowych. Definiuje się je jako systemy zarządzania tożsamością i dostępem [szerzej zob. Bertino, Takathasi 2010],
- systemy bezpieczeństwa, w tym osłony kontrwywiadowczej biznesu, w dużej mierze zależą od działań dedykowanego personelu (operatorzy systemów, osoby prowadzące postępowania wyjaśniające, itp.), którego celem jest ,,pokonanie" potencjalnego agresora. W związku z tym, systemy detekcji oraz ochrony aktywów muszą być zaprojektowane w taki sposób, aby uwzględnić (nie utrudniać) działania pracowników realizujących zadania osłony kontrwywiadowczej.

Mając powyższe na uwadze, służby kontrwywiadu biznesowego międzynarodowych organizacji, podobnie jak ich rządowe, odpowiedniki organizują swoje działania w oparciu na tzw. cyklu wywiadowczym[21]:

- ukierunkowywaniu *(direction)*,
- gromadzeniu informacji *(collection)*,
- przetwarzaniu informacji *(processing)*,
- analizowaniu informacji *(analysis)*,
- raportowaniu *(dissemination)*,
- informacji zwrotnej *(feedback)*.

Ukierunkowanie aktywności jednostek organizacyjnych odpowiedzialnych za kontrwywiad biznesowy wynika z wielu przesłanek – do głównych przesłanek należą:

- konieczność zapewnienia realizacji strategicznych i doraźnych celów organizacji,
- strategiczne i doraźne potrzeby informacyjne kierownictwa biznesowego,
- doraźne potrzeby informacyjne właścicieli ryzyka,

[21] Więcej: *FM 34-3 Intelligence Analysis*, Headquarters, Department of the Army, Washington, DC, 15 March 1990 r. Ze względu na objętość opracowania autor rozdziału pokrótce przybliży zasady gromadzenia oraz raportowania informacji przez służby kontrwywiadu biznesowego.

- informacje uzyskane w wyniku uprzednio podjętych działań lub przekazane przez wewnętrzne struktury firmy lub organizacje zewnętrzne.

W celu realizacji zadań z zakresu osłony kontrwywiadu biznesowego, dedykowane jednostki organizacyjne przedsiębiorstwa realizują czynności długoplanowe oraz doraźne, które w większości przypadków są pochodną rezultatu analizy oraz oceny ryzyka w organizacji[22]. Warto nadmienić, iż w ramach globalnego rejestru ryzyka przygotowuje się indywidualne oceny ryzyka dla każdego z kluczowych zagrożeń, np. nadużyć, korupcji, we wszystkich jednostkach organizacyjnych firmy np. dział zakupów, sprzedaży, operacyjny, itp. W przedmiotowym dokumencie uwzględnia się[23]:

- przyczyny wystąpienia ryzyka,
- konsekwencje wystąpienia ryzyka,
- elementy bieżącej kontroli,
- bieżącą ocenę poziomu ryzyka,
- planowane działania mające na celu redukcję ryzyka (jeśli konieczne),
- określenie właściciela ryzyka.

Opisane powyżej działania są istotne z punktu widzenia strategicznego zarządzania ryzykiem oraz budowy systemu długoterminowej osłony kontrwywiadowczej, jednakże wykazują one ograniczoną przydatność w operacyjnym zarządzaniu bezpieczeństwem, w tym planowaniu bieżących działań osłony kontrwywiadowczej. Wynika to m.in. z faktu, iż w zależności od kultury organizacyjnej firmy, jej rejestr ryzyka[24] jest najczęściej aktualizowany w cyklu rocznym lub dwuletnim, natomiast zarządzanie operacyjne bezpieczeństwem wymaga permanentnego uzyskiwania informacji o zagrożeniach, ich ocenie oraz podejmowaniu odpowiednich działań dla zapewnienia realizacji podstawowych celów biznesowych firmy oraz ochrony istotnych interesów korporacji.

Kontrwywiad biznesowy – źródła i analiza informacji

Źródła informacji wykorzystywanych w ramach działalności kontrwywiadu biznesowego w międzynarodowych organizacjach można podzielić na[25]:

[22] W przedmiotowych działaniach stosuje się metodykę oceny oraz analizy ryzyka dedykowaną dla określonej organizacji, natomiast reszta działań odbywa się na bazie cyklu Deminga.

[23] W zależności od przyjętej metodologii oceny i prezentowania ryzyka.

[24] Ryzyka dla korporacji przeanalizowane oraz ocenione przez stosowne jednostki organizacyjne (dedykowane osoby), zgromadzone w jednym dokumencie.

[25] Autor celowo unika używania określeń źródeł informacji wykorzystywanych przez służby specjalne.

- osobowe:
  - pracownicy korporacji,
  - dostawcy towarów i usług,
  - odbiorcy instytucjonalni,
  - klienci indywidualni,
  - osoby trzecie,
- techniczne:
  - firmowa sieć komputerowa,
  - urządzenia IT,
  - telefony służbowe,
  - systemy GPS w samochodach służbowych,
  - telewizja przemysłowa,
  - kontrola dostępu,
  - pozostałe,
- dokumenty oraz bazy danych posiadane oraz pozyskane przez organizację,
- źródła ogólnodostępne:
  - Internet,
  - rejestry,
  - bazy danych,
  - media społecznościowe,
  - fora dyskusyjne,
- instytucjonalne:
  - administracja rządowa – organy ścigania, sądy, administracja rządowej, itp.
  - prywatne – firmy detektywistyczne, podmioty realizujące zadania z obszaru *due dilligence,* itp.
  - media – prasa, radio, telewizja, Internet.

Strukturę kontrwywiadowczej sieci informacyjnej (źródeł informacji) międzynarodowej organizacji ukazuje rys. 2. Analizując przedmiotową strukturę informacyjną, warto zauważyć, iż kluczowym czynnikiem jej funkcjonalności jest dostępność zasobów informacyjnych poszczególnych źródeł informacji dla służb kontrwywiadu biznesowego organizacji. Uwzględniając wskazany czynnik, źródła informacji kontrwywiadu biznesowego dzielimy na:

- wewnętrzne – całkowicie dostępne *(źródła i zasoby korporacyjne)*,
- zewnętrzne – dostępność regulowana wzajemnymi umowami oraz regulacjami *(źródła i zasoby dostawców towarów i usług, odbiorców instytucjonalnych oraz indywidualnych),*

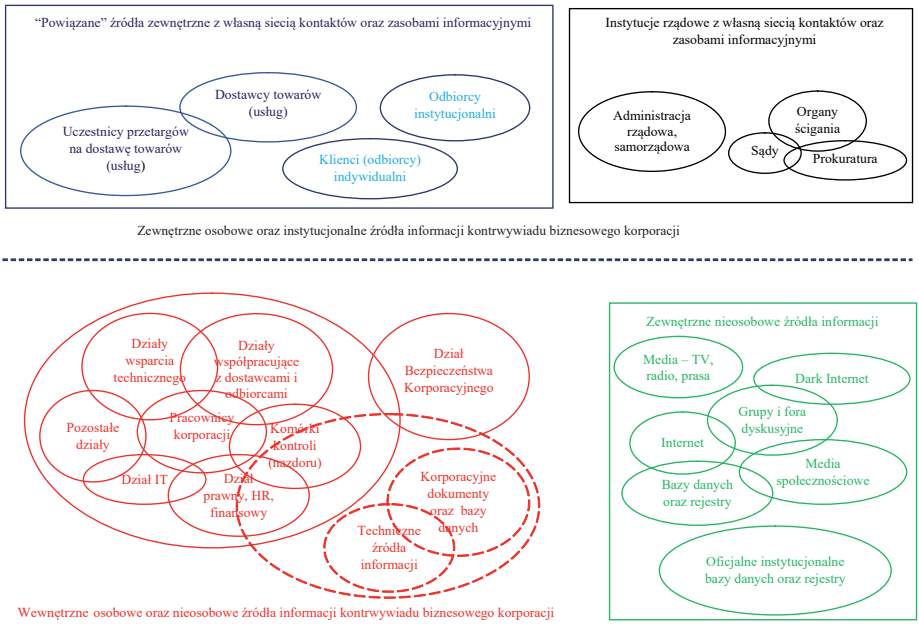
- zewnętrzne – dostępność limitowana regulacjami ustawowymi *(sądy, organa ścigania, prokuratury, administracja),*
- zewnętrzne ogólnodostępne *(media – prasa, telewizja, radio, itp.),*
- zewnętrzne – dostępność limitowana wiedzą, narzędziami oraz umiejętnościami pracowników kontrwywiadu biznesowego *(Internet, dark Internet, ogólnodostępne rejestry i bazy danych, media społecznościowe, fora dyskusyjne, itp.).*

Korporacyjne metody pozyskiwania informacji o zjawiskach, mogących stanowić zagrożenie dla realizacji podstawowych celów biznesowych firmy, jak również ochrony istotnych interesów organizacji, to:

- dedykowane kanały dla przekazywania informacji o potencjalnych nieprawidłowościach przez:
  - pracowników organizacji[26],
  - dostawców towarów i usług,
  - klientów instytucjonalnych oraz indywidualnych,
- dedykowane kanały informacyjne komórek kontrwywiadu biznesowego,
- doraźna i planowa wymiana informacji pomiędzy jednostkami organizacyjnymi korporacji, w tym z departamentami odpowiedzialnymi za rozpoznanie rynku, konkurencji, itp.

[26] Polityka informowania o nieprawidłowościach. W niektórych państwach istnieje ustawowy obowiązek zapewnienia możliwości raportowania nieprawidłowości w firmie, jak również obowiązek ochrony sygnalistów.

Rysunek 2. Struktura kontrwywiadowczej sieci informacyjnej (źródeł informacji) międzynarodowej organizacji



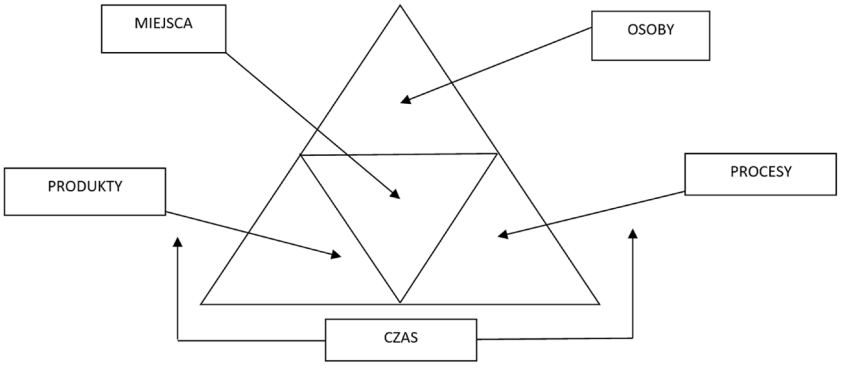
Źródło: opracowanie własne.

- specjalistyczne oprogramowania monitorujące sieci firmowe, oprogramowanie analizujące dane gromadzone w komputerach firmowych, analiza połączeń telefonicznych oraz danych z systemów zabezpieczeń,
- analiza dokumentów oraz baz danych znajdujących się w zasobach organizacji,
- eksploatacja i analiza ogólnodostępnych źródeł informacji,
- analiza informacji lub zapytań otrzymanych z sądów, organów ścigania oraz administracji rządowej,
- analiza raportów od podmiotów świadczących specjalistyczne usługi dostarczania informacji na rzecz korporacji,
- awarie, wypadki i zdarzenia nadzwyczajne,
- czynności kontrolne,
- dochodzenia wewnętrzne.

Narzędziem, wykorzystywanym przez służby kontrwywiadu biznesowego podczas planowania, procesowania oraz analiz przedsięwzięć na poziomie zarządzania operacyjnego (codzienne rutyny), jest tzw. *the hot koncept* [Beck, Chapman 2003, s. 16]. Stosując przedmiotowe rozwiązanie, zakłada się, iż jego niektóre elementy

organizacji (miejsca, produkty, procesy oraz osoby, itp.) są bardziej podatne na wystąpienie czynników ryzyka (zagrożeń) niż inne. Przedmiotowe podejście pozwala na komplementarną ochronę biznesu, ponieważ w przypadku zidentyfikowania jednego elementu, np. rutyny[27], której naruszenie może wywołać negatywne skutki dla organizacji, automatycznie wiążemy ją z konkretnymi osobami, miejscem oraz czasem realizacji czynności. W podobny sposób analizujemy inne elementy wysokiego ryzyka – czas[28], produkty[29], osoby[30] oraz miejsca[31]. Uzyskane dane objęte są dalszą analizą, m.in. dla ustalenia potencjalnych przyczyn *(modus operandi)* oraz możliwości wystąpienia powiązanych czynników ryzyka. Działanie takie daje podstawę do zaplanowania i wdrożenia najskuteczniejszych środków osłony kontrwywiadowczej organizacji. Założenia *the hot concept* przedstawia rys. 3.

Rysunek 3. „The Hot Concept"



Źródło: opracowanie własne na podstawie Beck, Chapman 2003, s. 16.

[27] W przypadku sieci handlowych może to być np. proces kontroli sprzedaży alkoholu. Jeśli nieuczciwa konkurencja spowoduje i udokumentuje sprzedaż alkoholu nieletniemu, to w teorii rezultatem takiego działania może być odebranie wszystkim placówkom tej sieci koncesji na sprzedaż alkoholu, co w przypadku branży handlowej może skutkować upadkiem firmy.

[28] Np. jakie procesy i przez kogo są realizowane w czasie najwyższego ryzyka – w godzinach nocnych, w dni wolne od pracy, itp.

[29] Np. w przypadku firmy produkcyjnej mogą to być produkty (informacje o produktach) znajdujące się w sferze badań naukowych – nowy model samochodu, lek przełomowy w leczeniu HIV, itp., co umożliwi nieuczciwej konkurencji uzyskanie przewagi rynkowej oraz oszczędzenie budżetu na podobne badania naukowe.

[30] Np. jakie osoby mają dostęp do kluczowych informacji o organizacji lub też, czy osoby pozostające w zainteresowaniu kontrwywiadu biznesowego podejmują działania w celu uzyskania dostępu do określonych miejsc, np. działu badań w organizacji,

[31] Np. czy miejsca kluczowe dla firmy (istotne procesy, produkty, itp.) są odpowiednio zabezpieczone i jakie osoby mają, chcą mieć do nich dostęp.

Wykorzystanie informacji kontrwywiadowczych w organizacji

Końcowymi stadiami cyklu informacyjnego są rozpowszechnianie informacji (raportów, analiz) oraz informacja zwrotna od adresatów. We wszystkich stadiach zarządzania informacją, a w szczególności podczas rozpowszechniania dokumentów mających istotne znaczenie dla korporacji, należy przestrzegać zasady niezbędnej wiedzy *(need to know principle)*[32]. W organizacjach międzynarodowych o dużej i zhierarchizowanej strukturze organizacyjnej, wiele osób, w tym zajmujących wysokie stanowiska w korporacji, bardzo często występuje do komórki odpowiedzialnej za kontrwywiadowczą ochronę organizacji o dostarczenie określonych informacji. W związku z tym, iż duża część opisanych zapytań spowodowana jest wyłącznie chęcią zdobycia informacji – bez szczególnego powodu (*nice know principle*), obowiązkiem administratora informacji (osoby odpowiedzialnej za dystrybucję) jest powiadomić o takim zapotrzebowaniu określone osoby funkcyjne w korporacji. Ze względu na częstotliwość rozpowszechniania, informacje możemy podzielić na nw. grupy:

- informacje rozpowszechniane doraźnie, ze względu na potrzebę natychmiastowego zabezpieczenia interesu firmy – w celu podjęcia pilnych działań prewencyjnych,
- informacje rozpowszechniane doraźnie, ze względu na ich strategiczne znaczenie (skutki, osoby zaangażowane, ryzyko reputacyjne firmy, itp.) raportowanego zdarzenia,
- informacje (raporty) rozpowszechniane doraźnie, po zakończeniu dochodzeń wewnętrznych – w celu podjęcia decyzji personalnych oraz organizacyjnych, mających istotne znaczenie dla bieżącego funkcjonowania korporacji,
- informacje (raporty) rozpowszechniane doraźnie, po zakończeniu czynności kontrolnych – w celu podjęcia decyzji personalnych oraz organizacyjnych mających istotne znaczenie dla bieżącego funkcjonowania korporacji,
- informacje zbierane doraźnie lub planowo ,,na żądanie" uprawnionych osób, organów firmy – dla podjęcia określonych decyzji związanych z ,,badaną" tematyką,
- informacje (analizy, raporty) przesyłane cyklicznie do kluczowych osób, struktur korporacji (komitety, grupy robocze) – dla podejmowania doraźnych i strategicznych decyzji personalnych i organizacyjnych na bazie dostarczonej wiedzy, raportów, statystyk oraz trendów, itp.

[32] Zasada niezbędnej wiedzy – informacje, raporty, analizy otrzymują wyłącznie osoby, wewnętrzne jednostki organizacyjne oraz podmioty zewnętrzne, które z uzasadnionych powodów (posiadają interes) powinny zapoznać się z ich treścią.

Struktury organizacyjne firmy oraz podmioty zewnętrzne otrzymujące informacje (raporty, analizy) służb kontrwywiadu biznesowego:

- struktury macierzystej organizacji:
  - zarząd, dyrektorzy departamentów, menedżerowie zajmujący kluczowe stanowiska,
  - istotne komórki organizacyjne,
  - komitety o charakterze stałym,
  - komitety o charakterze doraźnym
  - grupy robocze,
- instytucje zewnętrzne:
  - organy ścigania, prokuratura, sądy,
  - dostawcy towarów i usług,
  - odbiorcy instytucjonalni i indywidualni.

Jak wspomniano na początku niniejszego opracowania, czynnikami kluczowymi dla zapewnienia bezpieczeństwa korporacyjnego międzynarodowej organizacji są: *GRC governance, risk management, compliance)*. Mając powyższe na uwadze, zarządy (kluczowe osoby) korporacji chcą otrzymywać doraźną i cykliczną wiedzę z interesującej ich tematyki, w tym z obszaru przestrzegania regulacji wewnętrznych oraz przepisów ustawowych w organizacji. W tym celu organizuje się cykliczne (najczęściej kwartalne) zebrania tzw. komitetu zgodności *(compliance comittee)*, w skład którego wchodzą najważniejsze osoby w korporacji (*CEO, CFO, CIO, COO, CSO*[33], dyrektorzy departamentów oraz kierownicy najważniejszych komórek organizacyjnych). Pochodną działalności komitetu zgodności są operacyjne i strategiczne decyzje *(feedback)* dotyczące obszarów będących przedmiotem obrad członków komitetu.

Zakończenie

Rozważania zawarte w niniejszym rozdziale stanowią jedynie ogólny zarys funkcjonowania kontrwywiadu biznesowego w ramach bezpieczeństwa korporacyjnego w międzynarodowych organizacjach. Głównym zadaniem służb kontrwywiadu jest identyfikowanie informacji o istotnych zagrożeniach dla firmy, jak również ich

[33] Chief Executive Officer, Chief Financial Officer, Chief Security Officer, Chief Information Officer, Chief Operations Officer.

dystrybucja do odpowiednich komórek organizacyjnych/ osób dla wsparcia podejmowania kluczowych decyzji menedżerskich w korporacji. Organizując osłonę kontrwywiadowczą przedsiębiorstwa, należy mieć na uwadze nie tylko relacje wewnątrz organizacji, lecz także współdziałanie z organizacjami zewnętrznymi, takimi jak dostawcy i odbiorcy oraz instytucje rządowe. Zgodnie z treścią opracowania, działania kontrwywiadowcze stanowią istotny wkład w realizację podstawowych celów biznesowych firmy, jak również ochronę istotnych interesów korporacji. Uzyskanie pełnego obrazu zadań, sposobu działania, jak również wymiernych skutków funkcjonowania kontrwywiadu biznesowego w międzynarodowej organizacji, jest możliwe, na przykładzie pojedynczej instytucji lub kilku organizacji funkcjonujących w podobnych obszarach rynku, m.in. ze względu na możliwość indywidualnej oceny poziomu ryzyka wynikającego ze specyfiki zagrożeń, na jakie przedmiotowe przedsiębiorstwa są narażone.

Bibliografia

Beck A., Chapman P. (2003), *Hot Spots in The Supply Chain: Developing and Understanding of What Makes Some Retail Stores Vulnerable to Shrinkage*, a White Paper for ECR Europe, Brussels.

Bennett B.T. (2007), Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel, John Wiley & Sons.

Bertino E., Takahasi K. (2010), *Identity Management: Concepts, Technologies, and Systems,* Artech House, December 31.

Carbic M. (2015), *Corporate Security Management Challenges, Risks and Strategies,* Butterworth -Heinemann.

Certo S., Peter J.P. (1989), *Strategic Management – A Focus on Process*, Mc Graw Hill International, New York.

Crump J. (2015), *Corporate Security Intelligence and Strategic Decision-Making,* CRC Press, Taylor & Francis Group.

Denyer D. (2017), *Organizational Resilience, A summary of academic evidence, business insights and new thinking* by BSI and Cranfield School of Management, Cranfield School of Management, Cranfield University.

Dudziak M., Szpakowska E. (2013), *Zarządzanie ryzykiem i niepewność w działalności gospodarczej. Podejmowanie decyzji biznesowych,* ,,Zarządzanie i finanse", vol. 1, nr 1.

FM 34-3 Intelligence Analysis (1990), Headquarters, Department of the Army, Washington, DC, 15 March.

FM 3-19.30 Physical Security (2001), Headquarters, Department of the Army, Washington DC, 8 January.

Forest J.F. (2006), Homeland Security: Protecting America's Targets, Greenwood.

Godlewska-Majkowska H., Skrzypek E., Płonka M. (2016), *Przewaga konkurencyjna w Przedsiębiorstwie, Sektor – Wiedza – Przestrzeń,* Texter, Warszawa.

Pasella K., Kwieciński M. (2015), *Kontrwywiad gospodarczy w przedsiębiorstwie – od strategii działania do pracy operacyjnej z personelem,* ,,Bezpieczeństwo teoria i praktyka", Zeszyty Naukowe Krakowskiej Akademii im Frycza, 4.

Neef D. (2003), *Managing Corporate Reputation and Risk, Developing a Strategic Approach to Corporate Integrity Using Knowledge Management,* Elsevier.

Nogacki R., Ciecierski M. (2013), *Oszustwa i nadużycia pracownicze plagą współczesnego biznesu*, Profesjonalny Wywiad Gospodarczy Skarbiec Sp. z o.o., Warszawa.

OCEG Capability Model GRC Standards (2011) Hoboken, NJ, USA: John Wiley & Sons, Inc., 20 December.

Report to the nations on occupational fraud and abuse: 2014 global fraud study (2014), Association of Certified Fraud Examiners, Austin.

Steinberg R. (2011) *Governance, Risk Management and Compliance It Can't Happen to Us – Avoiding Corporate Disaster While Driving Success,* John Wiley & Sons, Inc.

Weidenmier M., Ramamoorti S. (2006), *Research Opportunities in Information Technology and Internal Auditing*, ,,Journal of Information Systems'', 20(1).

Źródła internetowe

http://justcomply.pl/pl/compliance-2/, dostęp: 22.06.2019.

https://mfiles.pl/pl/index.php/Disaster_recovery, dostęp: 22.06.2019.

https://bizfluent.com/info-8057178-corporate-security.html, dostęp: 17.06.2019.

http://www.portalspozywczy.pl/handel/wiadomosci/kulisy-afery-korupcyjnej-50-70-menadzerow-sieci-decyduje-o-zakupach-polakow,124373.html, dostęp: 26.06.2019.

https://mycompanypolska.pl/artykul/518/zarzadzanie-zlodzieje-firmowych-tajemnic, dostęp: 26.06.2019.

https://mfiles.pl/pl/index.php/Upadek_Barings_Bank, dostęp: 26.06.2019.

https://www.salon24.pl/u/starywrocek/508336,tone-at-the-top-w-polsce-wybor-nalezy-do-nas, dostęp: 3.07.2019.

https://www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/tone-at-the-top-research.pdf, dostęp: 1.07.2019.

https://mfiles.pl/pl/index.php/Przewaga_konkurencyjna, dostęp: 1.07.2019.

https://www.money.pl/galerie/artykul/huawei-kaspersky-szpiegostwo-przemyslowe,38,5,2425638.html.

https://www.tvn24.pl/krakow,50/prokuratura-ksiegowa-wyprowadzila-ponad-piec-milionow,929774.html, dostęp: 1.07.2019.

https://www.bankier.pl/wiadomosc/Zakonczono-prywatyzacje-PKP-Energetyka-3414252.html, dostęp: 10.07.2019.

https://www.parkiet.com/Parkiet-PLUS/306269958-Banki-ile-traca-na-oszustwach-pracownikow-i-wyludzeniach.html, dostęp: 1.07.2019.

Jadwiga Mazur
jadwiga.e.mazur@gmail.com
Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie

Bariery i czynniki wspierające w realizacji wybranych programów profilaktycznych w ocenie ich beneficjentów na przykładzie miasta Łódź

Wprowadzenie

Programy profilaktyczne są częścią działań podejmowanych przez samorządy terytorialne w celu zapewnienia nie tylko bezpieczeństwa i porządku publicznego, ale również wsparcia i pomocniczości. Celem rozdziału jest przedstawienie procesu realizacji programów profilaktycznych w zakresie przeciwdziałania alkoholizmowi, narkomanii i przemocy w rodzinie na terenie miasta Łódź, zwłaszcza w odniesieniu do oceny realizacji tych programów przez ich beneficjentów. Kolejno zostaną zaprezentowane kwestie związane z miastem i z zagrożeniami, profilaktyką. Następnie podstawowe i zarazem ważne zadania z zakresu profilaktyki na szczeblu miasta, podjęte przez odpowiedzialne za ich realizacje podmioty oraz wybrane organizacje. Przedstawione zostaną ogólne wnioski z badania ewaluacyjnego oraz refleksje beneficjentów w zakresie barier i czynników wspierających realizację programów.

Miasto

Miasto jest terenem zainteresowania zarówno praktyków, jak i badaczy. Badacze dokonują poszukiwań naukowych, próbując odpowiedzieć na postawione pytania badawcze. Praktycy natomiast podejmują często trud wprowadzenia w życie wypracowanych rozwiązań. Korzystając z bogatego dorobku naukowego, dotyczącego badań nad miastem, warto wskazać dorobek szkoły chicagowskiej. Szczególnie dotyczy to czterech głównych jej nurtów: urbanizacyjno-ekologicznego, prezentowanego w połączeniu z jej liderami R. Parkiem i E.W. Burgessem, kryminologicznego z jej liderem C.R. Shawem, psychologii społecznej łączonej z E. Farisem w roli lidera oraz prognozowania społecznego, której liderem jest W.F. Ogburn. Prezentowane nurty mają swoje odzwierciedlenie w szeregu prac istotnych dla rozwoju socjologii [Czekaj 2007, s. 238].

Nurt ekologiczny skupia się na opisie różnych światów społecznych funkcjonujących w rzeczywistości społecznej, także na analizie różnych nieopisywanych kwestii społecznych, jak również formy organizacji i instytucji społecznej [Czekaj 2007, ss. 240–268].

Nurt kryminologiczny dotyczy głównie przestępczości i dezorganizacji społecznej z jednoczesnym sporządzaniem map jej przestrzennej dystrybucji. To z kolei skutkowało podejmowaniem aktywności w zakresie budowy programów przeciwdziałających przestępczości z uwzględnieniem wskaźników przestępczości i środków, które miały spowodować osiągniecie założonych celów (organizacja społeczności, badania diagnostyczne, wykorzystanie zasobów instytucji). Efektem były takie działania, jak systematyczne wdrażanie programów zapobiegania dezorganizacji społecznej, tworzenie nowych agend, jeśli zajdzie taka potrzeba, kontynuacje programów edukacyjnych. Nurt ten wskazywał również słabość systemu kontroli społecznej [Czekaj 2007, ss. 270–285].

W nurcie psychologii społecznej szkoły chicagowskiej wskazuje się głównie na korzenie w twórczości H. Meada oraz zainteresowanie psychiatrią [Czekaj 2007, s. 306]. Natomiast nurt prognozowania społecznego odnosi się przede wszystkim do działań związanych z raportowaniem o problemach społecznych i skupia wokół planowania społecznego [Czekaj 2007, ss. 308–309]. Zaproponowane w tym rozdziale rozważania, dotyczące programów profilaktycznych miasta Łodzi, koncentrują się głównie wokół problemów podejmowanych w nurcie kryminologicznym szkoły chicagowskiej.

Biorąc pod uwagę kwestie miejskie, można również wskazać samo miasto jako miejsce składające się z czterech sfer, mianowicie środowiska geograficznego

(przyrodniczego), środowiska technicznego, zespołu ludzi (zbiorowości) użytkujących to środowisko, systemu organizacji społeczności miejskiej [Pióro 1964, ss. 211–240, za: Rykiel 1999, s. 15]. Poszukiwać odniesienia do prowadzonych rozważań można wokół zespołu ludzi/ zbiorowości, który użytkuje to środowisko, jak i systemu organizacji społeczności miejskiej. Z kolei w rozważaniach innego badacza, W. Piotrowskiego, można wyłonić organizacje, w których jednostka może odgrywać rolę społecznego działacza. Wyróżnia on umownie organizacje lokalne i ponadlokalne, gdzie „wyznacznikiem tego podziału będzie przestrzenny zasięg bezpośredniej działalności danej organizacji" [Piotrowski 1965, ss. 5–6]. Taki rodzaj działalności terenowej można odnieść w tym wypadku do działań związanych z realizacją zadań z zakresu profilaktyki, prowadzonych przez organizacje, którym je zlecono.

Należy również w tym miejscu nadmienić, że miasto Łódź jest miejscem badań i refleksji naukowych od wielu dekad. W. Piotrowski, odnosząc się do szkoły chicagowskiej, prowadząc badania dotyczące społeczno-przestrzennej struktury miasta Łodzi, poruszał kwestie związane z integracją funkcjonalną dzielnic i zanikania podstaw społecznych związanych z wyróżnianiem obszarów naturalnych. Ponadto według jego opinii, nowa zabudowa na początku lat sześćdziesiątych i powstawanie nowych struktur osiedlowych miały też wpływ na kształtowanie ówczesnych stosunków społecznych [Piotrowski 1966]. Z kolei Z. Rykiel, w analizie dotyczącej przemiany struktury społeczno-przestrzennej miasta polskiego a świadomości terytorialnej jego mieszkańców, zwraca uwagę na „słabą świadomość terytorialną mieszkańców osiedli mieszkaniowych, w tym zwłaszcza blokowisk. Słabość ta wynikała z niedostatków związków swojskości w blokowiskach" [Rykiel 1999, s. 21]. Można przypuszczać, że poczucie anonimowości, obcości, brak związku z miejscem zamieszkania pośrednio wpływały na procesy dezorganizacji i pojawianie się sytuacji klasyfikowanych jako zagrożenia.

Zagrożenia

Zapobieganie negatywnym zjawiskom wymaga najpierw poznania ich przyczyn, nie tylko na poziomie ich powstawania, ale także poprzez szersze spojrzenie, obejmujące zachodzące procesy zmian i ich skutki na poziomie zarówno mikro-, jak i makrospołecznym. Takie spojrzenie jest konieczne zwłaszcza w projektowaniu działania profilaktycznego, gdzie celem powinno być skupianie się najpierw na

diagnozowaniu rzeczywistych źródeł zagrożeń. Dopiero dogłębna diagnoza pozwala konstruować takie strategie profilaktyczne, które dostosowane są do konkretnej lokalnej społeczności.

Termin zagrożenie rozumiane jest jako „prawdopodobieństwo utraty jakiejś cenionej przez jednostkę wartości: bytowania na określonym poziomie, zdobywania kwalifikacji i pozycji społeczno-zawodowej”[1], połączone często z poszukiwaniem pomocy w organizacjach do tego powołanych.

Proponowane przez różnych autorów katalogi zagrożeń generalnie odnoszą się do tych płynących z natury (kataklizmy), jak i takich, którymi sprawcami są ludzie. Przytaczanie tych katalogów dla potrzeb rozdziału nie jest konieczne, warto jednak zaznaczyć, że w obecnych czasach – i nie tylko – przeważające są dwa rodzaje zagrożeń. Pierwsze dotyczy zagrożenia bytu (ekonomiczne) oraz zagrożenia ego (czyli psychologiczne), przy czym pojęcie bytu, jak i ego, rozumiane są dość szeroko. Byt to życie i zdrowie, jakość tego życia, natomiast ego to potrzeba poczucia podmiotowości, zaspokajana w różnych kontekstach społecznych i różnych okolicznościach [zob. Ratajczak 1993, ss. 5–11]. Podejście do bytu w rozumieniu poziomu i jakości życia ulegało zmianie na przestrzeni ostatnich trzech dekad. Połączone z rozbudzonymi potrzebami konsumpcyjnymi, nie jest porównywalne z latami dziewięćdziesiątymi. Natomiast kwestia podmiotowości nie zmieniła się; potrzeba podmiotowego traktowania, z należytym szacunkiem, nie zmieniła się i jest ważna zwłaszcza w sytuacji korzystania z pomocy.

Powiązane z bytem i ego jest również psychologiczne pojęcie możliwości, które może mieć treść „poznawczą (co ludzie mogą przyjąć do wiadomości) oraz treść emocjonalną (co ludzie mogą wytrzymać)” [zob. Tomaszewski 1993, ss. 11–21]. Te spojrzenia na znaczenie możliwości są również ze sobą związane przez definiowanie rzeczywistości przez jednostki i grupy. Łączą się też z możliwością kontrolowania biegu zdarzeń w odniesieniu do wyznaczonych celów.

Pojawiające się zagrożenia wymagają przyjmowania strategii radzenia sobie z nimi. Podejmowane są głównie dwie strategie – pierwsza, bierna, polegająca na oczekiwaniu pomyślnego ich biegu lub próbie przeczekiwania biegu niepomyślnego. Druga strategia – czynna – polega na próbie kontrolowania przebiegu tych zdarzeń i wykorzystywania pojawiających się możliwości [zob. Tomaszewski 1993, ss. 11–21]. Strategie te są stosowane w zależności od posiadanych doświadczeń życiowych, wiedzy czy innowacyjności w działaniu. Każdej z nich towarzyszy jednak stres

[1] Wyniki badań opinii publicznej wskazują na zjawisko rosnącej bezradności ludzi w szybko zmieniającej się rzeczywistości ekonomicznej, społecznej i politycznej. Zob. *Przedmowa* [Ratajczak 1993, ss. 5–11].

i poczucie nieprzewidywalności zdarzeń. To również sygnał do próby korzystania z oferowanej przez innych pomocy, zarówno płynącej z naturalnej sieci wsparcia, jakim jest rodzina, przyjaciele czy znajomi, jak i sieci wsparcia zbudowanej przez organizacje do tego powołane. Organizacje z zakresu wsparcia i pomocniczości oferują obecnie spory zakres pomocy, zależny w dużej mierze od posiadanego budżetu, ale także od aktywności osób korzystających ze wsparcia.

Profilaktyka

Organizacje, które zapewniają wsparcie i pomoc z zakresu profilaktyki, ulegały transformacjom przez ostatnie trzy dekady. Ich sprawczość zależała nie tylko od stawianych im wyzwań, ale także od posiadanej wiedzy. Analizując je, można stwierdzić, że są organizacjami uczącymi się, odpowiadającymi na nowe wyzwania. Po roku 1989 nowa rzeczywistość społeczna przyniosła ze sobą wiele zagrożeń, które wymagały nowych rozwiązań. Próby zaradzenia zagrożeniom rozpoczęły się już w ostatniej dekadzie ubiegłego wieku, a proponowane rozwiązania prewencyjne i profilaktyczne nie zawsze spełniały oczekiwania społeczne. Wynikało to z jednej strony ze specyficznej postawy roszczeniowej wobec organizacji zajmujących się tymi problemami, trudności radzenia sobie z zachodzącymi zmianami czy ze stosowania starych strategii radzenia sobie, niemających już zastosowania w nowych sytuacjach. Z drugiej strony był to również czas wprowadzania rozwiązań z zakresu profilaktyki, zdobywania nowych doświadczeń, zarówno przez twórców, jak i realizatorów programów profilaktycznych.

W dotyczących profilaktyki rozważaniach często pojawia się kłopot z jej definiowaniem. W znaczeniu ogólnym to „użycie jakiegoś środka zapobiegawczego; (w znaczeniu ścisłym) użycie środków zapobiegających chorobie" [Reber 2000, s. 551]. Natomiast według A. Nowak i E. Wysockiej profilaktyka to „wiele przedsięwzięć zabezpieczających przed powstaniem negatywnych stanów rzeczy" [Nowak, Wysocka 2001, s. 229]. Można więc stwierdzić, że „profilaktyka różni się od innych sposobów przeciwdziałania tym, że jest czynnością uprzedzającą, że podejmowana jest, zanim takie groźne zjawiska się ujawnią lub rozprzestrzenią, a ich dolegliwość wymusi dopiero zastosowanie bezpośrednich środków zaradczych" [Szymańska, Zamecka 2002, s. 20]. Ogólnie można stwierdzić, że profilaktyka to takie oddziaływania, których celem jest utrwalenie akceptowanych społecznie zachowań i niedopuszczanie do powstania kolejnych zachowań czy zjawisk negatywnych.

Termin profilaktyka używany jest czasami wymiennie z terminem prewencja. Ta różnorodność wskazuje również potrzebę formułowania definicji ogólnych, wąskich, jak i szerokich, często odnoszących się do konkretnych oddziaływań. Jednocześnie należy stwierdzić, że wielość definicji profilaktyki i prewencji odnosi się do mnogości dziedzin, w których mają one zastosowanie. Stąd zoperacjonalizowanie tego terminu jest dość trudne i często wymaga odniesienia do konkretnych działań zapobiegających.

Termin prewencja, podobnie jak profilaktyka, odnosi się ogólnie do przeciwdziałania – ,,zapobiegania czemuś, zwłaszcza przestępstwom" [Słownik Języka Polskiego 1995, s. 880]. To również ,,zapobieganie, prawo – jeden z celów stosowania kar; prewencja ogólna (generalna), zapobieganie popełnianiu przestępstw i wykroczeń przez ogół społeczeństwa – przez stosowanie kar w stosunku do sprawców oraz przez samo zagrożenie karą; prewencja szczególna (specjalna) zapobieganie popełnianiu przestępstw i wykroczeń przez tego samego sprawcę – przez wykonanie kary za określony czyn wg prawa pol. Celami wymiaru kary są: społeczne oddziaływanie wymierzonej kary oraz zapobieganie popełnieniu przestępstwa przez sprawcę i wychowanie go" [Nowa encyklopedia powszechna PWN, t.5 (P–S) 1998, s. 328]. Ta definicja wskazuje powiązanie terminu prewencji z prawem i rozwiązaniami z zakresu prawa. Oznacza głównie zapobieganie czemuś, zwłaszcza naruszeniom norm prawnych [Sobol 2002, s. 896]. Natomiast w pedagogice specjalnej termin prewencja obejmuje ,,działania prozdrowotne, opiekuńcze i edukacyjne, a obszarem jej zainteresowania jest zapobieganie uszkodzeniom fizycznym, dysfunkcjom intelektualnym, obejmuje też działania zapobiegające trwałym uszkodzeniom funkcjonalnym lub trwałej niepełnosprawności (prewencja wtórna)" [Dykcik 2002, s. 88]. Pedagogika przyjmuje również trzy rodzaje prewencji, pierwszy obejmujący podstawowe przyczyny zagrożeń, w drugim celem jest zapobieganie wzrostowi problemów społecznych w grupach dużego zagrożenia, a trzeci dotyczy jednostek i grup, wobec których wcześniejsze przedsięwzięcia nie przyniosły spodziewanych efektów [Boczoń, Toczyńska, Zielińska 1995, ss. 362–363].

Bez względu na rozważania definicyjne dotyczące profilaktyki czy prewencji, można zgodzić się z J. Czapską, że działaniach praktycznych trudno jest ,,rozdzielić prewencję od represji, ponieważ reakcja na dokonane naruszenie dóbr prawnych może działać zapobiegawczo, a działania prewencyjne mogą przekształcić się w określonych warunkach w represję" [zob. Czapska 2004, s. 17]. Ponadto, oprócz rozważań teoretycznych, profilaktykę stosuje się też w praktycznych działaniach podejmowanych przez podmioty odpowiedzialne za bezpieczeństwo oraz wsparcie i pomocniczość. Przykładem rozwiązań w tym zakresie są lokalne społeczności, a zwłaszcza miasta.

Profilaktyka w mieście Łódź

Trudno jest w ramach jednego rozdziału zanalizować wszystkie podejmowane działania profilaktyczne w mieście. Dlatego wybrano tylko niektóre z nich, a w szczególności dotyczące uzależnień i przemocy w rodzinie, gdzie beneficjentami są głównie osoby dorosłe. Należy jednak nadmienić, że w sytuacji uzależnień czy przemocy w rodzinie oddziaływanie tych programów pośrednio odnosi się również do dzieci i młodzieży.

Jeśli chodzi o działania profilaktyczne Urzędu Miasta Łodzi w latach 2016–2018 w zakresie przeciwdziałania uzależnieniom i przemocy w rodzinie, opisane zostaną podejmowane wyzwania z tego zakresu w ramach:

1. Miejskiego Programu Profilaktyki i Rozwiązywania Problemów Alkoholowych,
2. Miejskiego Programu Przeciwdziałania Narkomanii, Gminnego Programu,
3. Przeciwdziałania Przemocy w Rodzinie oraz Ochrony Ofiar Przemocy w Rodzinie.

Wybrane programy są realizowane z powodzeniem przez ostatnią dekadę, natomiast opis odnosi się do trzech lat 2016–2018. Zdecydowano się na ich analizę, ponieważ zostały poddane ewaluacji, a ich opis wskazuje na główne kierunki działania organizacji realizujących zadania z zakresu profilaktyki i jej skuteczności.

Opis realizacji pozostałych programów nie jest możliwy ze względu na objętość rozdziału.

Opracowując tego typu programy, zazwyczaj przyjmuje się, że ich realizowanie umożliwić ma osiągnięcie zaplanowanych w nich celów, dotyczących najogólniej rzecz ujmując zaspokojenia oczekiwań beneficjentów, a przez to także podniesienia ich poziomu i jakości życia. Ponadto zapobieganie rozpoznanym przez diagnozy problemom ma również spełnić oczekiwania społeczności miejskiej w zakresie poczucia bezpieczeństwa.

Typy instytucji finansowanych ze środków UMŁ w ramach realizacji programów profilaktycznych w latach 2016–2018 to głównie: klub/ stowarzyszenie o profilu sportowym – 53, stowarzyszenie/ fundacja świadczące różne formy wsparcia – 29, publiczna placówka medyczna, świetlica – 8, instytucja kościelna – 5. Osoby kierujące realizacją tych programów łączyły często funkcję administracyjną z pracą w charakterze specjalisty, mającego bezpośrednią styczność z beneficjentami programów. Najczęściej byli to psycholodzy, trenerzy, terapeuci, wychowawcy, pielęgniarki. Posiadali też bardzo duże doświadczenie w pracy w danej organizacji – średni staż ich pracy w organizacji w badanej grupie wynosił ponad 13 lat.

Takie zadania są trudne zarówno w zakresie diagnozowania, opracowania programów pomocy oraz realizacji. Wymagają zarówno pracy profesjonalistów,

nakładów finansowych ze strony samorządu terytorialnego, jak i właściwej koordynacji podmiotów realizujących te zadania. Programy odnosiły się do takich obszarów działania, jak:

- wspieranie działań profilaktycznych promujących styl życia wolny od alkoholu, w tym także aktywności o charakterze sportowym i kulturalnym, kierowanych do ogółu dzieci i młodzieży w ramach organizacji czasu wolnego jako alternatywa dla podejmowania zachowań ryzykownych (profilaktyka uniwersalna realizowana przez organizacje pozarządowe),
- wspieranie działalności organizacji/ środowisk samopomocowych dla osób uzależnionych i współuzależnionych od alkoholu,
- wprowadzanie do podstawowej i specjalistycznej opieki zdrowotnej metod wczesnego diagnozowania zagrożeń związanych z nadużywaniem alkoholu – wykonywanie testów przesiewowych oraz interwencji motywujących do zmiany zachowania,
- wspieranie inicjatyw promujących zdrowy styl życia, wolny od narkotyków, w tym także prowadzenie działań profilaktycznych o charakterze sportowym i kulturalnym, kierowanych do ogółu dzieci i młodzieży w ramach organizacji czasu wolnego jako alternatywa dla podejmowania zachowań ryzykownych (profilaktyka uniwersalna),
- organizowanie i prowadzenie specjalistycznego poradnictwa (prawnego, psychospołecznego oraz medycznego, psychologicznego, pedagogicznego, rodzinnego, socjalnego), a także usług terapeutycznych oraz grup wsparcia dla rodzin osób uzależnionych od narkotyków i zagrożonych uzależnieniem,
- zwiększanie dostępności i skuteczności zróżnicowanych form profesjonalnej terapii uzależnień dla osób z problemem narkotykowym,
- organizowanie i prowadzenie zróżnicowanych form poradnictwa (m.in.: medycznego, psychologicznego, psychospołecznego, pedagogicznego, rodzinnego, prawnego, socjalnego), zajęć psychologa z rodziną w kryzysie oraz zapewnienie możliwości wykonania obdukcji lekarskich dla osób dotkniętych przemocą,
- organizowanie i prowadzenie warsztatów umiejętności radzenia sobie z agresją i rozwiązywania konfliktów w rodzinie bez stosowania jakichkolwiek form przemocy (profilaktyka uniwersalna),
- indywidualne i grupowe działania korekcyjno-edukacyjne dla sprawców przemocy (nieletnich, pełnoletnich) [Długosz, Dzięglewski, Mazur 2019, s. 9].

Poziom realizacji zaplanowanych celów, podział zadań dokonany w ramach poszczególnych programów, mają zapewniać osiąganie ich założeń. Jednym z nich jest oczekiwanie, że sposób realizacji tych zadań zapewni uzyskanie zakładanych

rezultatów dzięki wielu rodzajom podejmowanych działań, rekomendowanych przez ekspertów jako tych, które mają przeciwdziałać zagrożeniom. Nie bez znaczenia pozostaje pytanie o problemy i bariery ograniczające lub uniemożliwiające prawidłową realizację zadań przez podmioty do tego uprawnione czy powołane do ich realizacji.

W podejmowanych badaniach ewaluacyjnych realizowanych programów profilaktycznych zazwyczaj poddaje się analizie wybrany obszar, jak i podmioty odpowiedzialne za ich realizację. Wśród nich bierze się pod uwagę dostępne wskaźniki realizacji programów, podejmuje się analizę porównawczą ilościowych wskaźników, poziom zaspokojenia potrzeb beneficjentów instytucji prowadzących działania z zakresu wsparcia i pomocniczości, a także ilościowe analizy potrzeb (jeśli takie są dostępne lub możliwe do pozyskania jako wyniki badań). Zalecane, a nawet konieczne, są analizy sprawozdań z dotychczasowych realizacji programów. Źródłami danych są sprawozdania, bezpośredni wykonawcy oraz beneficjenci. Metodami i technikami stosowanymi w tych przedsięwzięciach są analizy danych zastanych, sondaże diagnostyczne, wywiady kwestionariuszowe i indywidualne wywiady pogłębione, pozwalające na poznanie odbioru programów przez beneficjentów. Narzędzia badawcze to zwykle formularze do zestawiania danych sprawozdawczych, kwestionariusze z pytaniami otwartymi, częściowo ustrukturyzowany scenariusz wywiadu czy kwestionariusze ankiety. Dobór przedstawicieli jest zazwyczaj celowy, a kryterium udziału w badaniach – status podmiotu rozumianego jako instytucja korzystająca ze wsparcia Urzędu Miasta w ramach realizacji programów.

W realizacji programów profilaktycznych w Łodzi bierze udział sporo podmiotów z zakresu wsparcia i pomocniczości, mających różny status. Budżet przeznaczony na te działanie wynosił około 16 milionów[2]. Kwota ta wydaje się wysoka, niemniej w odniesieniu do wielkości miasta i potrzeb w zakresie profilaktyki – jest zadawalająca. Należy przy tym wziąć pod uwagę zarówno dane liczbowe dotyczące np. liczby osób korzystających z profesjonalnej terapii, osób, wobec których podjęto interwencję kryzysową czy liczby osób z problemem alkoholowym czy narkotykowym (również z przemocą w rodzinie), korzystających z różnego rodzaju poradnictwa, a głównie porad psychologicznych, socjalnych i prawnych. Pomoc ta – w realizacji indywidualnych ścieżek życiowych osób z powyższymi problemami – jest jednak nieoceniona. Ponadto nieprzeliczalna w odniesieniu do pozytywnych zmian, obejmujących nie tylko osoby indywidualne, ale także ich rodziny.

[2] Budżet zrealizowany w poszczególnych Programach w latach 2016–2018. Źródło: Sprawozdania z realizacji MPPiRPA, MPPN, GPPwR za lata 2016–2018 UM Łódź.

Można też wskazać pozytywny trend w kierunku zwiększenia liczby uczestników w programach profilaktycznych oraz poszerzania obszaru oddziaływania przez zwiększającą się liczbę podmiotów podejmujących wyzwania w zakresie realizacji tych działań. Pozytywny trend utrzymuje się bez względu na wielkość budżetu przeznaczonego na te zadania.

W zakresie wyszczególnionych wyżej programów, dotyczących przeciwdziałania dysfunkcjom życia rodzinnego i społecznego, których przyczyną jest używanie narkotyków, można zaobserwować coraz wyższy poziom realizacji zadań. Z kolei dane, dotyczące specjalistycznego poradnictwa, usług terapeutycznych czy grup wsparcia, wskazują na niższą liczbę świadczonych porad, z jednoczesnym wzrostem liczby osób korzystających z terapii. Można przyjąć, że mniejsza skala problemów związanych z zażywaniem narkotyków niż napojów alkoholowych świadczy o tym, iż osoby korzystające z substancji psychoaktywnych są bardziej skłonne do uczestnictwa w długiej i wymagającej samodyscypliny terapii niż osoby uzależnione od alkoholu. Zwiększyła się również liczba specjalistycznych porad świadczonych przez organizacje pozarządowe. W tym poradnictwa udzielały też podmioty odpowiadające za porady prawne, rodzinne i psychologiczne, w dalszej kolejności socjalne.

Wzrosła też liczba osób korzystających z terapii uzależnienia od narkotyków, w przeciwieństwie do terapii uzależnień od alkoholu przy niezmienionej liczbie organizacji świadczących terapię oraz porównywalnym budżecie. Na szczególną uwagę zasługuje również zróżnicowana oferta terapeutyczna, w tym terapia indywidualna, terapia rodzinna, porady diagnostyczne i terapeutyczne, interwencje kryzysowe czy, ważne dla beneficjentów zwłaszcza z problemem uzależnienia od alkoholu, grupy wsparcia. Tym bardziej, że te ostanie mają już długą tradycję, są dobrze zorganizowane i korzystają ze wspólnych doświadczeń. Kluby AA są również miejscem skupienia osób uzależnionych (często także członków ich rodzin). Jako wspólnoty odejmują też nowe wyzwania w drodze dochodzenia do trzeźwości.

Podsumowanie i wnioski

W poszukiwaniu determinantów efektywności realizowanych zadań z zakresu wsparcia i pomocniczości Urzędu Miasta Łódź można wyróżnić kilka czynników.

Pierwszym z nich jest jakość usług z zakresu wsparcia i pomocniczości, która została oceniona przez beneficjentów dobrze i bardzo dobrze, ze zróżnicowaniem na poszczególne programy. Najlepiej został oceniony program z zakresu

przeciwdziałania narkomanii, gdzie wysoka ocena wynika zarówno z wysokiej jakości usług terapeutycznych, jak i długości jej trwania oraz możliwości wydłużenia korzystania z pomocy przez pobyt w hostelu. Dodatkowym i bardzo docenianym przez beneficjentów czynnikiem był także wysoki profesjonalizm tych usług, jak i wypracowane przez dekady programy wsparcia wraz z zapleczem materialnym.

Jako drugi można usytuować program zapobiegania alkoholizmowi, gdzie zarówno tradycja pomocy, jak i w miarę rozbudowana, chociaż niedoinwestowana baza materiałowa, zapewniają możliwość stałej pomocy grupom tworzącym wspólnoty i zdeterminowanym do powrotu do życia bez alkoholu. Wartością dodaną jest praca stowarzyszeń, będących jednocześnie grupami wsparcia dla osób uzależnionych i współuzależnionych.

Trzeci program, skierowany do ofiar przemocy, jest w dużej mierze niedoinwestowany, a oferowana pomoc mieści się w zadaniach programu zapobiegania alkoholizmowi. Widoczne to jest również w wykazach podmiotów pomocowych, które są wymieniane praktycznie we wszystkich programach.

Ważnymi, pozytywnie ocenianymi przez beneficjentów aspektami realizacji, są: proces komunikowania między nimi a pomagającymi i podmiotami, niezawodność i kompetencje kadry, rozumiane jako dysponowanie wiedzą i umiejętnościami zgodnymi z przedstawioną ofertą realizowanych programów, oraz wiarygodność i zaufanie do pracowników organizacji.

Ocena podmiotów i jakości prowadzonych usług z zakresu wsparcia i pomocniczości przez beneficjentów jest dobra i bardzo dobra. Niemniej wielość podmiotów pracujących w systemie wsparcia i pomocniczości może z czasem prowadzić do rozproszenia finansowania tych usług, warto więc przemyśleć możliwość stworzenia konsorcjów pomocowych, kumulujących te usługi z uwzględnieniem ich lokalizacji i dostępności dla beneficjentów.

Można też stwierdzić, że inwestycja miasta w programy i podmioty je realizujące jest ze wszech miar opłacalna, chociaż może nie bezpośrednio widoczna, bo trudno w jakikolwiek sposób przeliczyć na finanse odrodzenie wspólnoty, powrót do trzeźwości, spokój rodziny czy dążenie do zmniejszenie zakresu marginalizacji mieszkańców miasta.

Bibliografia

Czapska J. (2004), *Bezpieczeństwo obywateli. Studium z zakresu polityki prawa*, Wydawnictwo Pollpres, Kraków.

Czekaj K. (2007), *Socjologia Szkoły Chicagowskiej i jej recepcja w Polsce*, Górnośląska Wyższa szkoła Handlowa im. Wojciecha Korfantego, Katowice.

Długosz P., Dzięglewski M., Mazur J. (2019), *Stopień realizacji celów programów profilaktycznych Urzędu Miasta Łodzi w świetle danych sprawozdawczych, działań ich realizatorów i opinii beneficjentów*, Łódź.

Dykcik W. (2002), *Tendencje rozwojowe pedagogiki specjalnej w zakresie opieki, edukacji i rehabilitacji* [w:] *Pedagogika specjalna*, red. W. Dykcik, Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza w Poznaniu, Poznań.

Nowa encyklopedia powszechna PWN (1998), T. 5 (P – S), PWN, Warszawa.

Nowak A., Wysocka E. (2001), *Problemy i zagrożenia społeczne we współczesnym świecie. Elementy patologii społecznej i kryminologii*, ,,Śląsk" Wydawnictwo Naukowe, Katowice.

Piotrowski W. (1965), *Miasto Opole i jego struktura ekologiczna w wypowiedziach aktywistów terenowych*, Instytut Śląski, Opole.

Piotrowski W. (1966), *Społeczno-przestrzenna struktura miasta Łodzi. Studium ekologiczne*, Ossolineum, Wrocław.

Pióro Z. (1964), *Niektóre czynniki kształtujące struktury i procesy ekologiczne współczesnych miast polskich* [w:] *Socjologiczne problemy miasta polskiego*, red. S. Nowakowski, PWN, Warszawa.

Ratajczak Z. (1993), *Zmiany społeczne zagrożenia i wyzwania dla jednostki,* ,,Kolokwia psychologiczne. Pismo Komitetu Nauk Psychologicznych PAN", red Z. Ratajczak, Tom 2, Warszawa.

Reber A.S. (2000), *Słownik Psychologii*, red. I. Kurcz, K. Skarżyńska, Wydawnictwo Naukowe SCHOLAR, Warszawa.

Rykiel Z. (1999), *Przemiany struktury społeczno-przestrzennej miasta polskiego a świadomość terytorialna jego mieszkańców*, Wydawnictwo Continuo.

Słownik Języka Polskiego (1995), PWN, Warszawa.

Sobol E. (2002), *Słownik wyrazów obcych*, PWN, Warszawa.

Szymańska J., Zamecka J. (2002), *Przegląd koncepcji i poglądów na temat profilaktyki* [w:] *Profilaktyka w środowisku lokalnym*, red. G. Świątkiewicz, Krajowe Biuro ds. Przeciwdziałania Narkomanii, Warszawa.

Tomaszewski T. (1993), *O możliwościach jednostki w sytuacjach przemian społecznych* [w:] *Zmiany społeczne zagrożenia i wyzwania dla jednostki*, red. Z. Ratajczak, ,,Kolokwia psychologiczne. Pismo Komitetu Nauk Psychologicznych PAN", tom 2, Warszawa.

Sprawozdania z realizacji MPPiRPA, MPPN, GPPwR za lata 2016–2018 UM Łódź.

Piotr Niedzielski
piotr.niedzielski@usz.edu.pl
Uniwersytet Szczeciński, Instytut Zarządzania

Michał Antolak
antolakmichal@majkoltrans.pl
ZFSNT NOT w Szczecinie

Magdalena Zioło
magdalena.ziolo@usz.edu.pl
Uniwersytet Szczeciński, Instytut Ekonomii i Finansów

System Zarządzania Bezpieczeństwem w transporcie kolejowym – wybrane aspekty

Wprowadzenie

Bezpieczeństwo stanowi podstawową wartość w życiu ludzi i społeczeństw. Zapewnienie poczucia bezpieczeństwa jest wartością nie tylko dla użytkowników transportu, w tym transportu kolejowego, ale także dla otoczenia, w którym transport funkcjonuje. Tak więc bezpieczeństwo w transporcie kolejowym jest elementem systemu bezpieczeństwa technicznego i publicznego państwa. Transport kolejowy w Polsce podlega takim samym uregulowaniom, co cały system transportowy w Unii Europejskiej, gdzie jednym z narzędzi jest posiadanie przez podmioty świadczące usługi na

tym rynku Systemu Zarządzania Bezpieczeństwem (SMS), który to system podlega ocenie regulatorowi krajowemu, jakim w warunkach Polski jest Urząd Transportu Kolejowego (UTK). Systemy Zarządzania Bezpieczeństwem (SMS) są usystematyzowanym zbiorem zasad, procedur i reguł postępowania przy wykonywaniu działalności przedsiębiorstwa kolejowego, mającym zapewnić wysoki poziom bezpieczeństwa świadczonych usług. Polscy przewoźnicy kolejowi, zgodnie ze standardami Unii Europejskiej, byli zobowiązani wdrożyć do swojej działalności Systemy Zarządzania Bezpieczeństwem (SMS).

Celem rozdziału jest wskazanie, że wdrożenie i dalsze doskonalenie Systemów Zarządzania Bezpieczeństwem u polskich przewoźników kolejowych przynosi pozytywne efekty w obszarze bezpieczeństwa, co ma odzwierciedlenie we wskaźnikach analizowanych w niniejszym rozdziale. Jednocześnie przeprowadzone autorskie badania o charakterze pilotażowym, dokumentacji trzech przewoźników, w obszarze szacowania ryzyka, dla ograniczonego katalogu stałych zagrożeń występujących u wszystkich przewoźników kolejowych, wskazuje potencjalne obszary możliwości poprawy Systemu Zarządzania Bezpieczeństwem, przy wykorzystaniu roli Urzędu Transportu Kolejowego jako regulatora tego segmentu rynku w Polsce.

Bezpieczeństwo w transporcie kolejowym jako element systemu bezpieczeństwa publicznego

Historycznie pojęcie „bezpieczeństwo" wywodzi się wprost z czasów Imperium Rzymskiego, a etymologicznie z języka łacińskiego, gdzie słowo *se cura* znaczyło „wolny od troski", a *securitas* – polityczną stabilność. Bezpieczeństwo stanowi naczelną/ podstawową potrzebę człowieka i oznacza stan spokoju, pewności, stan, który jest wolny od zagrożeń [Leszczyński 2010, s. 33]. Współcześnie wskazuje się szereg obszarów bezpieczeństwa na różnych poziomach np. bezpieczeństwo militarne, bezpieczeństwo ekonomiczne, bezpieczeństwo finansowe [Flejterski, Zioło 2015, ss. 9–31], bezpieczeństwo techniczne itd. W tym kontekście pojęcie bezpieczeństwa jest pojęciem bardzo często występującym w różnych obszarach życia, w tym w życiu codziennym, zarówno jeśli chodzi o organizację, funkcjonowanie życia społecznego, państwowego, jak i naukę. Powszechność ta rodzi wieloznaczność tego terminu, dlatego współcześnie

dodaje się przymiotniki dookreślające obszar/dziedziny bezpieczeństwa. W literaturze przedmiotu można wskazać szereg rodzajów bezpieczeństwa, zaliczanych do szeroko definiowanego bezpieczeństwa publicznego tj. zabezpieczenie przed zamachami na życie, zdrowie i mienie obywateli, bezpieczeństwo imprez masowych i zgromadzeń, bezpieczeństwo sanitarno-epidemiologiczne, bezpieczeństwo prawne i obrotu prawnego, bezpieczeństwo pożarowe, bezpieczeństwo informacyjne, bezpieczeństwo informatyczne (cyberbezpieczeństwo), bezpieczeństwo budowlano-architektoniczne, bezpieczeństwo środowiskowe (ekologiczne), bezpieczeństwo techniczno-technologiczne, czy wreszcie bezpieczeństwo w transporcie i komunikacji [Fehler 2009]. Bezpieczeństwo dotyczy więc wielu obszarów, w konsekwencji zawiera tym samym w sobie szereg celów. Zagrożenie bezpieczeństwa, definiowane jako destrukcyjne oddziaływanie otoczenia, może być spowodowane wieloma czynnikami. Zagrożenia bezpieczeństwa mogą mieć rożny charakter, skalę zasięgu i siłę oddziaływania, zatem można wyróżnić: zagrożenia potencjalne i realne, zagrożenia subiektywne i obiektywne, zagrożenia wewnętrzne i zewnętrzne, zagrożenia militarne i pozamilitarne, zagrożenia instytucjonalne i przypadkowe [Gierszewski 2013]. Negatywne oddziaływanie otoczenia na obszar bezpieczeństwa, stwarzanie szeregu zagrożeń, w tym zagrożeń wynikających z działania sił przyrody (zagrożenie środowiskowe), techniki (zagrożenie techniczne) czy rozwoju cywilizacji (zagrożenie społeczne), jest praktycznie nieograniczone [Sienkiewicz-Małyjurek, Niczyporuk 2010]. Stan bezpieczeństwa odzwierciedla więc określoną konfigurację relacji między instytucjami państwa, odpowiedzialnymi za kształtowanie i monitorowanie stanu bezpieczeństwa w określonych, poszczególnych obszarach a podmiotami zbiorowymi i obywatelami (społeczeństwem), które są zarówno zainteresowane określonym poziomem bezpieczeństwa, jak i współuczestniczą w jego kreacji przez państwo (i jego organy), zobowiązane do tego w ramach swoich polityk [Lis 2015]. Bezpieczeństwo na poziomie indywidualnym jest jedną z podstawowych potrzeb człowieka, co ma odzwierciedlenie w powszechnie znanej hierarchizacji potrzeb w postaci tzw. piramidy potrzeb Maslowa [Encyklopedia Zarządzania]. Bezpieczeństwo można zaliczyć do jednych z najbardziej pożądanych wartości, stanowi ono niejako podstawę osiągania kolejnych wartości. Bezpieczeństwo jako wartość jest stopniowalne, co oznacza, że można być mniej lub bardziej bezpiecznym, lub przekładając to na system zarządzania bezpieczeństwem, można osiągać mniejszy lub większy poziom bezpieczeństwa. Minimalny poziom bezpieczeństwa jest niezbędny, aby przetrwać lub aby procesy społeczno-gospodarcze mogły w miarę prawidłowo

przebiegać, jednak występuje pewien paradoks, który można określić prawem zmniejszających się zysków z zaangażowania zasobów w poziom bezpieczeństwa, przejawiający się faktem, że im wyższy poziom bezpieczeństwa, osiągamy (co wymaga zaangażowania określonego wolumenu zasobów), tym mniejszą wartość dla nas ma ten fakt (mniej doceniamy wyższy poziom bezpieczeństwa). Tak więc sprawne zarządzanie bezpieczeństwem w różnych obszarach aktywności człowieka, w tym także w obszarze transportu, warunkuje/ jest jedną z determinant rozwoju społeczno-gospodarczego na różnych poziomach tj. lokalnym, regionalnym, narodowym i ponadnarodowym np. na poziomie Unii Europejskiej. W tym ujęciu bezpieczeństwo jest kategorią interdyscyplinarną i może być rozpatrywane na różnych poziomach tj: (i) bezpieczeństwo jednostki, w ujęciu subiektywnym, jak i obiektywnym, (ii)bezpieczeństwo struktur społecznych, w tym bezpieczeństwo wewnętrzne i zewnętrzne państwa, (iii) bezpieczeństwo międzynarodowe w ujęciu regionalnym, kontynentalnym, jak i globalnym.

Przedsiębiorstwa świadczące usługi transportowe są zobowiązane zrealizować je z uwzględnieniem szeregu zagrożeń wynikających z przestrzennego charakteru produkcji usług transportowych [Niedzielski 2013, ss. 143–157]. Bezpieczeństwo transportu określają następujące podstawowe determinanty – (1) czynnik ludzki, (2) środek transportu, (3) środowisko. Ogólny poziom bezpieczeństwa transportu jest składową tych trzech podsystemów. Każdy z nich wpływa na nie w sposób pozytywny lub negatywny. Poprawa (wzrost) poziomu bezpieczeństwa jest więc możliwa dzięki podnoszeniu jakości wszystkich trzech składników, z jednoczesną optymalizacją wzajemnych powiązań między nimi, co prezentuje poniższy rysunek:

Rysunek 1. Wzajemne relacje człowiek–technika–środowisko w kształtowaniu bezpieczeństwa

Źródło: opracowanie własne.

Przejawem negatywnych zdarzeń nadzwyczajnych w transporcie jest błąd człowieka, naruszenie funkcjonowania środków transportu, systemów transportu, uszkodzenie lub zniszczenie dróg transportu i budowli transportowych. W wyniku tego dochodzi do zagrożenia dla życia i zdrowia ludzi, zagrożenia dla wartości materialnych lub środowiska naturalnego. Bezpieczeństwo i ryzyko mają charakter prawdopodobieństwa. Ich wartości mieszczą się w przedziale od 0 do 1, przy czym ich suma jest zawsze równa 1. Bezpieczeństwa absolutnego, którego wartość wynosi 1, w praktyce nie można zapewnić. Tak więc bezpieczeństwo można określić jako stan, w którym możliwość wystąpienia szkody wśród osób lub mienia jest zminimalizowana i utrzymuje się w ramach ciągłego procesu identyfikacji zagrożeń i zarządzania ryzykiem bezpieczeństwa na dopuszczalnym poziomie lub poniżej tego dopuszczalnego poziomu [Podręcznik Zarządzania Bezpieczeństwem ULC 2009]. Tak więc **bezpieczeństwo transportu i systemów transportowych wyraża stan, w którym ryzyko uszkodzenia zdrowia osób lub powstania szkód materialnych zostało zminimalizowane do akceptowalnego poziomu**. Transport, w tym także transport kolejowy, ze względu na przestrzenny charakter i złożoność produkcji usług transportowych, należy do dziedzin o największej częstotliwości występowania zdarzeń nadzwyczajnych.

Zapewnienie poczucia bezpieczeństwa jest wartością nie tylko dla użytkowników transportu, w tym transportu kolejowego, ale także dla otoczenia, w którym transport funkcjonuje. Tak więc istotnymi aspektami, związanymi ze sprawnym systemem zarządzania bezpieczeństwem, są: poczucie braku zagrożenia

i poczucie bezpieczeństwa, zarówno dla klientów transportu, w tym transportu kolejowego, jak i jego otoczenia.

System Zarządzania Bezpieczeństwem w transporcie kolejowym jako element zasad Unii Europejskiej

System zarządzania bezpieczeństwem (*Safety Management System*, potocznie SMS) według dyrektywy 2004/49/WE Parlamentu Europejskiego i Rady z 29.04.2004 roku oznacza: „organizację i środki przyjęte przez zarządcę infrastruktury lub przedsiębiorstwo kolejowe w celu zapewnienia bezpiecznego zarządzania jego działaniem" [Dyrektywa 2004/49/UE].

Z powyższej definicji oraz treści dyrektywy 2004/49/WE wynika, że systemy zarządzania bezpieczeństwem są usystematyzowanym zbiorem zasad, procedur i reguł postępowania przy wykonywaniu działalności przedsiębiorstwa kolejowego, mającym zapewnić wysoki poziom bezpieczeństwa świadczonych usług. Tak więc, uogólniając, na system bezpieczeństwa w transporcie kolejowym składają się: geneza zagrożeń, diagnoza stanu i systemu bezpieczeństwa, programowanie działań zapobiegawczych, środki poprawy, monitoring podejmowanych działań oraz ocena ich efektywności.

System zarządzania bezpieczeństwem ma być zgodny z wymaganiami krajowych przepisów bezpieczeństwa, wymaganiami bezpieczeństwa ustanowionymi w technicznych specyfikacjach interoperacyjności (TSI) przy stosowaniu wspólnych metod oceny bezpieczeństwa (CSM). Na podstawie rozporządzenia Ministra Transportu z dnia 19 marca 2007 roku, Prezes Urzędu Transportu Kolejowego (UTK), wydając certyfikat lub autoryzację bezpieczeństwa, dokonuje akceptacji systemu zarządzania bezpieczeństwem, czym potwierdza spełnienie przez niego wymagań prawnych [Dz. U. z 2007 r. nr 60, poz. 407].

W ogólnym ujęciu system zarządzania bezpieczeństwem powinien składać się z elementów takich, jak [Dz.U. z 2007 r. nr 60, poz. 407, Rozporządzenie Komisji UE 1158/2010, Rozporządzenie Komisji UE 1169/2010]:

a) programy poprawy bezpieczeństwa,

b) opisy procedur dla osiągniecia celów z programów bezpieczeństwa,

c) opisy procedur dla utrzymania infrastruktury, urządzeń do prowadzenia ruchu kolejowego oraz pojazdów kolejowych,

d) opisy procedur i metod oceny ryzyka powstałego w wyniku prowadzonej działalności,
e) sposób sprawowania nadzoru nad oceną ryzyka,
f) systemy i programy szkolenia pracowników,
g) stosowane rozwiązania, umożliwiające dostęp oraz wymianę informacji związanych z bezpieczeństwem,
h) procedury zgłaszania i dokumentowania wypadków i incydentów,
i) postanowienia o częstotliwości i trybie audytów wewnętrznych oraz kontroli systemu bezpieczeństwa,
j) inne postanowienia np. w sprawie systemów alarmowania.

Ponadto systemy zarządzania bezpieczeństwem powinny być tworzone w oparciu o regulacje wewnętrzne [Dz. U. z 2007 r. nr 60, poz. 407]:

1. dla zarządcy infrastruktury, dotyczące:
   a) prowadzenia ruchu pociągów i techniki manewrowej oraz sygnalizacji,
   b) radiołączności pociągowej,
   c) obsługi ruchowych posterunków technicznych,
   d) regulaminów technicznych,
   e) obsługi przejazdów kolejowych,
   f) urządzeń sterowania ruchem kolejowym oraz detekcji stanów awaryjnych taboru,
   g) nawierzchni kolejowej, rozjazdów i obiektów inżynieryjnych,
   h) przesyłek nadzwyczajnych,
   i) wypadków i incydentów.
2. Dla przewoźników, dotyczące:
   a) eksploatacji i utrzymania pojazdów kolejowych,
   b) prowadzenia pojazdów trakcyjnych,
   c) zestawiania pociągów, rozmieszczania taboru i ładunku,
   d) organizacji pracy manewrowej,
   e) przewozu przesyłek nadzwyczajnych i towarów niebezpiecznych,
   f) wypadków i incydentów.

Wdrożenie i użytkowanie Systemów Zarządzania Bezpieczeństwem na kolei w Polsce

W 2006 roku, na mocy Ustawy o transporcie kolejowym z 22 lipca 2006 r., wprowadzono konieczność posiadania przez przewoźnika oraz zarządcę infrastruktury systemu zarządzania bezpieczeństwem w przypadku ubiegania się o wydanie certyfikatu lub autoryzacji bezpieczeństwa [Dz. U. z 2007 r. nr 60, poz. 407]. Brak certyfikatu lub autoryzacji bezpieczeństwa, w świetle obowiązującego prawa oznaczał brak możliwości prowadzenia działalności na rynku usług transportu kolejowego.

Wydane do lipca 2006 r. świadectwa bezpieczeństwa utraciły ważność najpóźniej 31 grudnia 2010 r. Zarządcy infrastruktury oraz przewoźnicy kolejowi zostali zobowiązani do wystąpienia o certyfikat lub autoryzację bezpieczeństwa do 30 czerwca 2010 r. [Rozporządzenie Komisji UE 1158/2010].

Zmiany legislacyjne spowodowały konieczność wprowadzenia i wdrożenia do użytkowania przez przedsiębiorstwa kolejowe ich własnych systemów zarządzania bezpieczeństwem, zgodnych z Dyrektywą 2004/49/WE oraz krajowymi przepisami bezpieczeństwa.

W przypadku przewoźników kolejowych, posiadanie systemu zarządzania bezpieczeństwem polega na rozpoznawaniu, ocenie i analizie działań zapobiegawczych odnośnie zagrożeń związanych z prowadzoną działalnością. W praktyce sprowadza się to do:

- przeprowadzania audytów wewnętrznych (np. w obszarze utrzymania pojazdów kolejowych),
- opracowywania rocznych planów poprawy bezpieczeństwa,
- opracowywania raportów bezpieczeństwa za dany rok,
- analizy i oceny ryzyka dla prowadzonej działalności,
- propozycji działań zapobiegawczych dla występujących zagrożeń.

Kształtowanie się wskaźników bezpieczeństwa w transporcie kolejowym w Polsce

Publikowane przez Państwową Komisję Badania Wypadków Kolejowych od II połowy 2007 raporty roczne z prac Komisji pozwalają na zebranie szczegółowych

danych odnośnie wszystkich zdarzeń, wypadków i incydentów, jakie wystąpiły na kolei w Polsce. Dodatkowo opracowywane przez Urząd Transportu Kolejowego – Oceny funkcjonowania rynku transportu Kolejowego i Stanu Bezpieczeństwa Ruchu Kolejowego w Polsce oraz dane statystyczne odnośnie wykonanej pracy przewozowej pozwalają ocenić wpływ SMS na bezpieczeństwo transportu kolejowego.

Tabela 1. Liczba zdarzeń na sieci PKP PLK w stosunku do wykonywanej pracy przewozowej

Rok	Zdarzenia				Przewozy towarów				Przewozy pasażerskie			
	Poważne wypadki	Wypadki	Incydenty	SUMA	Praca przewozowa [mln tkm]	Masa towarów [t]	Liczba zdarzeń/Praca przewozowa [tys tkm]	Liczba zdarzeń/Masa towarów [mln t]	Praca przewozowa [mln pkm]	Liczba pasażerów [mln]	Liczba zdarzeń/Praca przewozowa [tys pkm]	Liczba zdarzeń/Liczba pasażerów [mln]
2008	149	771	419	1339	51570	276,2	25,965	4,848	20255	292,2	66,11	4,58
2009	82	788	244	1114	43601	242,8	25,550	4,588	18679	283,3	59,64	3,93
2010	65	809	245	1119	48842	235,3	22,911	4,756	17907	261,8	62,49	4,27
2011	62	815	294	1171	53974	249,2	21,696	4,699	18164	264,1	64,47	4,43
2012	1	709	244	954	48903	231,3	19,508	4,125	17860	273,9	53,42	3,48
2013	1	690	200	891	50881	233,2	17,511	3,821	16797	270,4	53,05	3,30
2014	1	670	345	1016	50007	228,9	20,317	4,439	16071	269,1	63,22	3,78
2015	2	629	521	1152	50603	224,8	22,765	5,125	17443	280,3	66,04	4,11
2016	2	688	853	1543	50620	222,2	30,482	6,944	19181	292,6	80,44	5,27
2017	4	743	1272	2019	54829	239,9	36,824	8,416	20321	303,6	99,36	6,65

Źródło: opracowanie własne na podstawie: GUS 2019, UTK 2019.

W tabeli 1 zestawiono dane dotyczące wykonanej pracy przewozowej przez przewoźników pasażerskich i towarowych oraz liczby odnotowanych w danym roku zdarzeń (poważnych wypadków, wypadków, incydentów). Ich porównanie jednoznacznie wskazuje, że w latach 2008–2014 miał miejsce systematyczny spadek zdarzeń na kolei, co można uznać za pozytywny wpływ stosowania SMS przez przewoźników. Znaczące zmniejszenie liczby poważnych wypadków kolejowych od 2012 r. jest efektem zmiany definicji tego zdarzenia. Jednakże od roku 2015 ma miejsce regularny wzrost zdarzeń niebezpiecznych w stosunku do przewożonej masy. Jest to widoczne nawet po zmianie zasad prowadzenia statystyki i uwzględnieniu w niej od marca 2016 roku zdarzeń, które miały miejsce na bocznicach kolejowych. Prawdopodobną przyczyną tej negatywnej tendencji jest brak zmian legislacyjnych mających na celu zlikwidowanie słabych punktów Systemów Zarządzania Bezpieczeństwem.

Zasady wyznaczania wartości ryzyka dla potencjalnych zagrożeń jako determinanta systemu – studium przypadku

Dyrektywy oraz krajowe przepisy bezpieczeństwa nie narzucają przewoźnikom i zarządcom infrastruktury metody oceny ryzyka występującego dla prowadzonej działalności. Urząd Transportu Kolejowego (UTK), jako regulator rynku kolejowego w Polsce, jest m.in. odpowiedzialny za monitorowanie bezpieczeństwa transportu kolejowego oraz nadzorowanie wykonywania obowiązków w tym obszarze przez podmioty/ przedsiębiorstwa uczestniczące w procesie świadczenia usług przewozowych przez tę gałąź transportu [Sitarz, Chruzik, Mańka 2012], co wyrażone jest w misji urzędu: „Kreowanie bezpiecznych i konkurencyjnych warunków świadczenia usług transportu kolejowego" [www.utk.gov.pl]. Jednocześnie UTK, oprócz realizacji ustawowych obowiązków regulacji i nadzoru nad funkcjonowaniem rynku kolejowego w Polsce, podejmuje szereg inicjatyw mających zwiększyć poziom wiedzy w zakresie kształtowania bezpieczeństwa przez firmy – uczestników tego rynku ,co przejawia się w wizji UTK: „Nowoczesny i otwarty urząd dbający o wysokie standardy wykonywania usług na rynku transportu kolejowego" [www.utk.gov.pl]. Jedną z takich inicjatyw jest Akademia Bezpieczeństwa UTK, która działa od 24 października 2019 r, to projekt współfinansowany przez Unię Europejską ze środków Funduszu Spójności w ramach Programu Operacyjnego Infrastruktura i Środowisko 2014-2020, oś priorytetowa: V Rozwój transportu kolejowego w Polsce, działanie: 5.2 Rozwój transportu kolejowego poza TEN. Celem projektu jest kształtowanie bezpiecznego i konkurencyjnego oraz sprawnie funkcjonującego systemu kolejowego przez wyrównywanie poziomu wiedzy i kompetencji uczestników sektora transportu kolejowego. Akademia Bezpieczeństwa Kolejowego (ABK) stanowi także platformę upowszechniającą i wspomagającą wymianę dobrych praktyk, co daje szansę na ujednolicenie podejścia różnych uczestników rynku usług kolejowych w zakresie systemu zarządzania bezpieczeństwem.

Proces oceny ryzyka w transporcie kolejowym zasadniczo składa się z następujących elementów: (i) **identyfikacji ryzyka**, (ii) **szacowania ryzyka**, które można określić jako przypisanie „wagi" poszczególnym parametrom ryzyka, np. prawdopodobieństwu, skutkom, wykrywalności, a następnie na ich podstawie określenia poziomu ryzyka, (iii) **wyceny ryzyka,** czyli dokonania oceny, czy określony poziom ryzyka w konkretnym funkcjonującym systemie jest dopuszczalny, czy poziom ten został przekroczony (przyrównując osiągniętą wartość ryzyka do wartości ryzyka, jaka uznana została za progową) oraz (iiii) **określenia środków**

bezpieczeństwa, które należy rozumieć jako określone konkretne działania, jakie należy podjąć w przypadku zidentyfikowanego zagrożenia w celu utrzymania ryzyka na poziomie dopuszczalnym. W sytuacji, gdy poziom ryzyka przekracza poziom dopuszczalny, podmiot odpowiedzialny za bezpieczeństwo (przewoźnik, zarządca infrastruktury) powinien określić dodatkowe środki bezpieczeństwa, czyli takie, które przyczynią się do obniżenia wartości ryzyka. Środki bezpieczeństwa określane są dla każdego zidentyfikowanego zagrożenia. Środki bezpieczeństwa to działania podejmowane w codziennej pracy podmiotu realizującego usługi na rynku usług usługowych, stale utrzymujące ryzyko na poziomie dopuszczalnym. Należy je formułować w taki sposób, aby określały konkretne działania, których wynik w sposób ilościowy można wykorzystać w trakcie procesu monitorowania ich efektów.

Identyfikację zagrożeń oraz szacowanie ryzyka można określić jako **analizę ryzyka,** rozumianą jako systematyczne wykorzystywanie wszystkich dostępnych informacji służącą realizacji tych dwóch wyżej wymienionych celów.

Proces oceny ryzyka prezentuje poniższy rysunek.

Rysunek 2. Proces oceny ryzyka

Źródło: https://utk.gov.pl/pl/bezpieczenstwo-systemy/praktyczne-stosowanie-w/14060,Praktyczne-stosowanie-wspolnej-metody-oceny-bezpieczenstwa.html, dostęp: 20.12.2019.

W praktyce dostępne są różne metody oceny ryzyka – delficka, FMEA, 635 i inne. Ze względu na skuteczność, prostotę i przejrzystość, najczęściej stosowaną metodą oceny ryzyka jest metoda FMEA. Metoda FMEA, czyli *Failure Mode and Effect Analysis* (Analiza błędów i skutków) [Soliński 2020] polega na wyznaczeniu wartości w skali od 1–10 dla 3 parametrów: prawdopodobieństwo wystąpienia (W), prawdopodobieństwo wykrycia (Z), skutki (S). Wartość 1 przyjmuje się dla minimalnego prawdopodobieństwa, a wartość 10 dla maksymalnego. Następnie, wykonując iloczyn tych 3 wskaźników (R):

$$R=W*Z*S$$

wyznacza się wartość ryzyka R. W zależności od wartości R ryzyka, uznaje się, że:

Tabela 2. Wartość ryzyka R

R≤120	Nie ma ryzyka wystąpienia niebezpieczeństwa
120≤R≤150	Należy podjąć kroki eliminujące ryzyko
R>150	Zagrożenie krytyczne – należy podjąć kroki eliminujące

Źródło: opracowanie własne na podstawie: System Zarządzania Bezpieczeństwem jednego z podmiotów działającego na rynku polskim transportu kolejowego.

Zasady wyznaczania wskaźnika ryzyka metodą FMEA są opisane w normie PN-EN IEC 60812:2018-12. Jednakże nie ma określonych wartości, jakie należy przyjąć dla składowych iloczynu R. Również rozporządzenie wykonawcze Komisji UE nr 402/2013 w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka, Dyrektywa 2004/49/WE ani krajowe przepisy bezpieczeństwa nie regulują dokładnie zasad oceny ryzyka. Ustawodawca zostawia przewoźnikom i zarządcom infrastruktury swobodę w kwestii oceny ryzyka, narzucając jedynie konieczność przeprowadzenia fachowego osądu z wykorzystaniem specjalistycznej wiedzy kompetentnego zespołu [Rozporządzenie Komisji UE 402/2013]. Bazując na obowiązującym prawie, każdy przewoźnik/ zarządca infrastruktury dokonuje indywidualnej oceny ryzyka. Ta subiektywna ocena każdego użytkownika SMS-a jest często przedmiotem sporów z krajowymi organami bezpieczeństwa.

W tabeli 3 zawarto wartości prawdopodobieństwa wystąpienia zagrożenia, przyjęte przez podmioty posiadające certyfikaty/autoryzacje bezpieczeństwa:

Tabela 3. Prawdopodobieństwa wystąpienia zagrożenia

Prawdopodobieństwo wystąpienia zagrożenia (W)	Częstotliwość [1 błąd/ 1 [poc. km]			Punktacja (W)
	Podmiot 1	Podmiot 2	Podmiot 3	
Niebezpieczeństwo prawie wykluczone	1/1.000.000	1/25.000	1/50.000	1
Przyczyna zagrożenia występuje bardzo rzadko	1/900.000 1/800.000	1/15.000 1/12.500	1/45.000 1/40.000	2 3
Duże prawdopodobieństwo wystąpienia, ale bez dużego wpływu na proces	1/700.000 1/600.000 1/500.000	1/10.000 1/7.500 1/5.000	1/35.000 1/30.000 1/25.000	4 5 6
Wysoka możliwość wystąpienia zagrożenia. Przyczyna występuje regularnie	1/400.000 1/300.000	1/4.000 1/2.500	1/20.000 1/15.000	7 8

Prawdopodobieństwo wystąpienia zagrożenia (W)	Częstotliwość [1 błąd/ 1 [poc. km]			Punktacja (W)
	Podmiot 1	Podmiot 2	Podmiot 3	
Bardzo wysoka możliwość wystąpienia. Niemal pewne wystąpienie zagrożenia	1/200.000 1/100.000	1/1.500 1/1.000	1/10.000 1/5.000	9 10

Źródło: opracowanie własne na podstawie: Systemy Zarządzania Bezpieczeństwem podmiotów działających na polskim rynku transportu kolejowego.

Widoczne w tabeli 3 wartości punktów (składnik iloczynu R) różnią się dla podmiotów działających na tym samym rynku. Czynnikiem, mającym wpływ na przedstawione tutaj wartości, jest wielkość wykonywanej przez dany podmiot pracy przewozowej – jednakże żadne regulacje prawne nie regulują tych wartości. Powoduje to, że w tym obszarze panuje dowolność przyjmowanych wartości.

W przypadku wartości punktacji (Z) dla prawdopodobieństwa wykrycia zagrożenia oraz (S) skutków zagrożenia, wszystkie trzy analizowane podmioty przyjęły identyczne wartości – w tabelach 4 i 5 zamieszczono wartości dla parametrów prawdopodobieństwa wykrycia zagrożenia (Z) i skutków wystąpienia zagrożenia (S).

Tabela 4. Prawdopodobieństwo wykrycia zagrożenia (Z)

Prawdopodobieństwo wykrycia zagrożenia (Z)	Punktacja
Bardzo duże prawdopodobieństwo wykrycia zagrożenia. Ustalenie przyczyn błędu jest pewne.	1
Duże prawdopodobieństwo wykrycia zagrożenia. Ustalenie przyczyn błędu następuje w oparciu o znane czynniki.	2 3
Normalne prawdopodobieństwo wykrycia zagrożenia. Ustalenie przyczyny błędu opiera się na więcej wymiernych charakterystykach.	4 5 6
Nieznaczne prawdopodobieństwo wykrycia zagrożenia. Ustalenie przyczyny błędu jest bardzo trudne.	7 8
Bardzo małe prawdopodobieństwo wykrycia zagrożenia. Niemożliwe jest wykrycie przyczyn błędu.	9 10

Źródło: opracowanie własne na podstawie: Systemy Zarządzania Bezpieczeństwem jednego z podmiotów działających na polskim rynku transportu kolejowego.

Tabela 5. Skutek zagrożenia (S)

Skutek zagrożenia	Punktacja
Skutki wystąpienia zagrożenia nie mają znaczenia dla poziomu bezpieczeństwa. Bez kosztów	1
Skutki wystąpienia zagrożenia mogą być niewielkie i doprowadzić jedynie do nieznacznego obniżenia poziomu bezpieczeństwa oraz kosztów do 10.000 EUR (2) i do 50.000 EUR (3)	2 3
Skutki wystąpienia zagrożenia mogą być dość znaczne i doprowadzić do obniżenia poziomu bezpieczeństwa (np. incydent, ranni) oraz kosztów do 100.000 EUR (4), do 250.000 EUR (5) i do 500.000 EUR (6)	4 5 6
Skutki wystąpienia zagrożenia mogą być poważne i doprowadzić do obniżenia poziomu bezpieczeństwa (np. wypadek kolejowy, ciężko ranni) oraz kosztów do 750.000 EUR (7) i do 1.000.000 EUR (8)	7 8
Skutki wystąpienia zagrożenia mogą być bardzo poważne i doprowadzić do obniżenia poziomu bezpieczeństwa (np. poważny wypadek, ofiary śmiertelne) oraz kosztów do 200.000 EUR (9) i do 2.000.000 EUR (10)	9 10

Źródło: opracowanie własne na podstawie: Systemy Zarządzania Bezpieczeństwem jednego z podmiotów działających na polskim rynku transportu kolejowego.

Największe różnice widoczne są w wartościach oceny dla poszczególnych ryzyk. Każdy podmiot na potrzeby certyfikatu/ autoryzacji bezpieczeństwa ma obowiązek zdefiniować zagrożenia, jakie mogą wystąpić w związku z prowadzoną działalnością i większość z nich dokonuje oceny ryzyka dla tych samych zdarzeń. Mimo że korzystają z podobnego sprzętu, tej samej infrastruktury, specjalistów wyszkolonych na tym samym poziomie – mają różne wyniki. Dla zobrazowania tego zjawiska poniżej przywołano przykłady 1–4, które zaprezentowano w kolejnych tabelach od 6 do 9.

Przykład 1 – Brak lub nieprawidłowe wykonanie próby hamulca

Tabela 6. Wartość ryzyka dla braku lub niewłaściwego wykonania próby hamulca

Podmiot	Ew. konsekwencje	W	Z	S	R	Zalecane środki kontroli
Podmiot 1	Wykolejenie	1	2	8	16	Brak potrzeby stosowania dodatkowych środków
Podmiot 2	Udział w zdarzeniu kolejowym, zagrożenie w ruchu	3	4	5	60	1 kontrola w miesiącu. Dodatkowe omówienie nieprawidłowości na pouczeniach
Podmiot 3	Zwiększone ryzyko zaistnienia wypadku/ uszkodzenia pojazdu	2	2	4	16	Kontrole stanu technicznego taboru

Źródło: opracowanie własne na podstawie: Systemy Zarządzania Bezpieczeństwem podmiotów działających na polskim rynku transportu kolejowego.

Ryzyko związane z brakiem lub nieprawidłowym wykonaniem próby hamulca polega na przeoczeniu przez pracownika uszkodzenia układu hamulcowego lub niewłaściwego nastawienia hamulca pojazdu. Próba hamulca jest podstawową czynnością wykonywaną przez wykwalifikowanych pracowników (rewidenci taboru/ maszyniści). Najczęstszym skutkiem niedopełnienia obowiązków jest zdarzenie kolejowe (np. wykolejenie) oraz uszkodzenie pojazdu, co stanowi zagrożenie w ruchu. Dane zawarte w tabeli 6 uwidoczniają duże rozbieżności w ocenie prawdopodobieństwa wystąpienia, wykrycia oraz skutków zagrożenia. Podmioty 1 i 3 oceniły ryzyko na bardzo niskim poziomie (R=16), podczas gdy podmiot 2 wyznaczył wartość ryzyka prawie 4 razy większą (R=60). Uwidacznia się tutaj brak ograniczeń prawnych, uniemożliwiających dowolne przyjmowanie składników iloczynu R.

Przykład 2 – *Niestosowanie się do wskazań urządzeń sygnalizacyjnych*

Tabela 7. Wartość ryzyka dla niestosowania się do wskazań urządzeń sygnalizacyjnych

Podmiot	Ew. konsekwencje	W	Z	S	R	Zalecane środki kontroli
Podmiot 1	Wykolejenie/ kolizja	1	2	8	16	Brak potrzeby stosowania dodatkowych środków
Podmiot 2	Udział w zdarzeniu kolejowym, zagrożenie w ruchu	3	5	5	75	Pouczenia okresowe i bieżący nadzór przełożonego
Podmiot 3	Uszkodzenie pojazdów, nawierzchni oraz ofiary	5	3	7	105	Szkolenia i kontrole

Źródło: opracowanie własne na podstawie: Systemy Zarządzania Bezpieczeństwem podmiotów działających na polskim rynku transportu kolejowego.

Ryzyko związane z niezastosowaniem się do wskazań urządzeń sygnalizacyjnych przez drużynę trakcyjną polega tutaj na przeoczeniu lub niezrozumieniu podanego sygnału. Konsekwencje wystąpienia tego zagrożenia mogą być bardzo poważne i nieść za sobą spore szkody. W tabeli 7 zawarto wyniki oceny wykonanych przez badane podmioty. Podmiot 1 wyznaczył wartość ryzyka R=16, podmiot 2 R=75, a pomiot 3 R=105. Widoczny tutaj rozrzut wartości ryzyka dla tego samego zagrożenia pokazuje, jak brak odgórnie narzuconych wartości współczynników wpływa na ocenę ryzyka i w skrajnym przypadku może doprowadzić do zaniżenia jego wartości. W tym wypadku taka niska wartość R powoduje, że podmiot 1 nie

zakłada jakichkolwiek środków zapobiegawczych i kontrolnych, kiedy podmiot 3 zakłada przeprowadzanie kontroli i szkoleń mających na celu zapobieganie tego typu zdarzeniom.

Przykład 3 – *Nieprawidłowe wykonywanie prac manewrowych*

Tabela 8. Wartość ryzyka dla nie nieprawidłowego wykonywania prac manewrowych

Podmiot	Ew. konsekwencje	W	Z	S	R	Zalecane środki kontroli
Podmiot 1	Wykolejenie	1	1	5	6	Brak potrzeby stosowania dodatkowych środków
Podmiot 2	Udział w zdarzeniu kolejowym, zagrożenie w ruchu	3	5	4	60	Pouczenia okresowe. W razie potrzeby zwiększenie ilości jazd instruktażowych
Podmiot 3	Uszkodzenia taboru, zagrożenia życia pracowników	2	6	5	60	Kontrole bieżące wykonywanych czynności

Źródło: opracowanie własne na podstawie: Systemy Zarządzania Bezpieczeństwem podmiotów działających na polskim rynku transportu kolejowego.

Ryzyko związane z nieprawidłowym wykonywaniem prac manewrowych polega na przestawianiu pojazdów w sposób niezgodny z regulacjami wewnętrznymi przewoźników/ zarządców infrastruktury/ bocznic kolejowych, bez zachowania ogólnie przyjętych zasad bezpieczeństwa. Skutkami wystąpienia tej nieprawidłowości mogą być szkody w infrastrukturze, taborze, ładunku oraz uszczerbek na zdrowiu lub nawet utrata życia pracowników. W tabeli 8 zawarto wyniki oceny dokonanej przez badane podmioty. Jest to kolejny przypadek, w którym wyznaczone przez podmioty wartości ryzyka cechuje duża różnica wartości. Dla podmiotu 1 R=6, a dla podmiotów 2 i 3 R=60. Różnica ta wynika z przeszacowania albo niedoszacowania ryzyka przez podmioty.

Przykład 4 –– *Skierowanie do pracy pracowników bez wymaganych uprawnień*

Tabela 9. Wartość ryzyka dla skierowania do pracy pracowników bez wymaganych uprawnień

Podmiot	Ew. konsekwencje	W	Z	S	R	Zalecane środki kontroli
Podmiot 1	Wykolejenie	1	1	6	6	Brak potrzeby stosowania dodatkowych środków
Podmiot 2	Udział w zdarzeniu kolejowym, zagrożenie w ruchu	3	3	5	45	Bieżący nadzór nad uprawnieniami i rejestrami egzaminów pracowników
Podmiot 3	Zwiększone ryzyko wystąpienia wypadku, awarii pojazdu	4	2	3	24	Analiza dokumentów/ uprawnień pracowników

Źródło: opracowanie własne na podstawie: Systemy Zarządzania Bezpieczeństwem podmiotów działających na polskim rynku transportu kolejowego.

Ryzyko związane ze skierowaniem do pracy pracowników bez wymaganych uprawnień polega na niewłaściwym zaplanowaniu pracy maszynistów lub drużyn manewrowych z użyciem określonego taboru. Konsekwencjami tych nieprawidłowości może być zdarzenie kolejowe lub uszkodzenie taboru. W tabeli 9 zawarto wyniki oceny wykonanych przez badane podmioty. Podmioty określiły ryzyko na poziomach: podmiot 1 R=6, podmiot 3 R=24, podmiot 2 R=45. Największy wpływ na poziom tego ryzyka ma czynnik ludzki. Istnieją różne sposoby zabezpieczenia się przed wystąpieniem tego zagrożenia – wewnętrzne procedury (np. z SMS), systemy zarządzania przedsiębiorstwem itp. W tym przypadku różnica wartości może wynikać z faktycznych różnic między przedsiębiorstwami w zakresie stosowanych standardów zarządzania. U jednego z podmiotów decyzja o skierowaniu pracowników do pracy może być samodzielnie podejmowana przez dyspozytora, u innego przez dyspozytora z autoryzacją szefa dyspozytury, a u innego przez algorytm komputerowy, analizujący bazę dostępnych pracowników wraz z ich uprawnieniami i czasami pracy.

Podsumowanie

Wdrożenie systemów zarządzania bezpieczeństwem na kolei w Polsce miało pozytywny wpływ na spadek liczby zdarzeń (sumy poważnych wypadków, wypadków i incydentów). Widoczne jest to w statystykach zawartych w raportach rocznych publikowanych przez Państwową Komisję Badania Wypadków Kolejowych. Jednakże w ciągu ostatnich kilku lat widzimy przyrost liczby zdarzeń w stosunku do wykonywanej pracy przewozowej. Przeprowadzona analiza wykonywanych w ramach systemów zarządzania bezpieczeństwem ocen ryzyka oraz obowiązujących w obszarze bezpieczeństwa kolejowego przepisów pozwala stwierdzić prawdopodobną przyczynę zwiększenia liczby zdarzeń w Polsce. Obowiązujące w Polsce regulacje prawne odnośnie systemów zarządzania bezpieczeństwem w niewystarczający sposób regulują zasady wyznaczania wartości ryzyka dla potencjalnych zagrożeń. Żadne z obowiązujących rozporządzeń, ustaw, dyrektyw nie reguluje szczegółowo ogólnie występujących zagrożeń w transporcie kolejowym ani zasad ich oceny. Doprowadza to do sytuacji, w której przewoźnicy i zarządcy infrastruktury osiągają bardzo różne wyniki w poziomie ryzyka dla tych samych zagrożeń w tych samych warunkach.

Celem wyeliminowania tego typu przypadków konieczne jest:

- Empiryczne określenie przez panel ekspertów zasad określania prawdopodobieństwa wystąpienia zagrożenia (W), w zależności od wielkości pracy przewozowej wykonanej przez przewoźników i zarządców infrastruktury. Widoczne w tabeli 2 wartości dla 3 badanych podmiotów nie są w żaden sposób regulowane, a wartości okazują się bardzo rozbieżne, co nie do końca znajduje uzasadnienia w doświadczeniu eksploatacyjnym.
- Empiryczne określenie przez panel ekspertów prawdopodobieństwa wykrycia zagrożenia. Na tą chwilę każdy przewoźnik lub zarządca infrastruktury, stosując te same metody pracy, uzyskuje różne wartości współczynnika wykrycia zagrożenia (Z) dla tych samych zagrożeń.
- Empiryczne określenie przez panel ekspertów skutków wystąpienia zagrożenia (S). Obecnie przewoźnicy i zarządcy infrastruktury dla tych samych zdarzeń przyjmują różne wartości (S), co widoczne jest w tabelach 5, 6, 7 i 8.
- Stworzenie listy stałych zagrożeń dla przewoźników i zarządców infrastruktury, które muszą być zawarte w systemach zarządzania bezpieczeństwem. Obecnie podmioty w różny sposób nazywają identyczne zagrożenia, utrudniając ich ocenę organom bezpieczeństwa.

Wyżej wymienione zmiany należy wdrożyć wyłącznie dla zagrożeń występujących dla wszystkich podmiotów objętych obowiązkiem posiadania SMS-a oraz

niedających się na tę chwilę całkowicie wyeliminować. Doskonałym przykładem jest nieprawidłowe wykonanie próba hamulca. Każdy przewoźnik przeprowadza próbę hamulca praktycznie w ten sam sposób. W tym wypadku należy zapobiegać dowolności w przyjmowaniu wartości współczynników przy określaniu ryzyka. Zagrożenia spowodowanego niewłaściwym wykonaniem próby hamulca obecnie nie da się całkowicie wyeliminować ze względu na błędy ludzkie – próby hamulca nie może wykonać robot ani komputer. Z tego powodu to zagrożenie powinno zostać doprecyzowane w zakresie oceny ryzyka. Celem uniknięcia przeregulowania należy pamiętać, że nie każde zagrożenie wymaga osobnych regulacji prawnych. Przykładem takiego zagrożenia jest skierowanie do pracy pracowników bez wymaganych uprawnień. Każdy podmiot może w inny sposób kontrolować ważność uprawnień pracowników. W tym wypadku można to zagrożenie całkowicie wyeliminować np. zastępując człowieka komputerem w kwestii decyzji, który pracownik ma zostać skierowany do danej pracy. Z tego powodu to zagrożenie nie wymaga regulacji prawnych w zakresie oceny ryzyka.

Wdrożenie tych prostych zmian systemowych pozwoli na uzyskanie bardziej realnych wyników oceny zagrożeń, a tym samym na skupienie uwagi przewoźników, zarządców oraz organów bezpieczeństwa na wspólnym i efektywnym rozwiązywaniu realnych problemów związanych z bezpieczeństwem kolei bez tworzenia zbędnych regulacji.

Bibliografia

Dyrektywa 2004/49/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie bezpieczeństwa kolei wspólnotowych oraz zmieniająca dyrektywę Rady 95/18/WE w sprawie przyznawania licencji przedsiębiorstwom kolejowym, oraz dyrektywę 2001/14/WE w sprawie alokacji zdolności przepustowej infrastruktury kolejowej i pobierania opłat za użytkowanie infrastruktury kolejowej oraz certyfikację w zakresie bezpieczeństwa (Dyrektywa w sprawie bezpieczeństwa kolei, Dz. Urz. UE L.220/2004).

Encyklopedia Zarządzania, https://mfiles.pl/pl/index.php/Piramida_Maslowa , dostęp: 14.04.2019.

Fehler W. (2009), *Bezpieczeństwo publiczne*, „Społeczeństwo i polityka", vol. 21, issue 4, ss. 30–39.

Flejterski S., Zioło M. (2015), *Ordofinanse. W poszukiwaniu nowego ładu w nauce i praktyce finansów*, „Finanse", nr 1.

Gierszewski J. (2013), *Bezpieczeństwo wewnętrzne*, Zarys Systemu, Difin.

Lis W. (2015), *Bezpieczeństwo wewnętrzne i porządek publiczny jako sfera działania administracji publicznej*, Lublin, ss. 36–37.

Niedzielski P. (2013), *Kreatywność i procesy innowacyjne na rynku usług transportowych. Ujęcie modelowe*, Polskie Towarzystwo Ekonomiczne Oddział w Szczecinie.

Podręcznik Zarządzania Bezpieczeństwem (ULC 2009), wydanie drugie, Urząd Lotnictwa Cywilnego, Warszawa.

Rozporządzenie Ministra Transportu z dnia 19 marca 2007 r. w sprawie systemu zarządzania bezpieczeństwem w transporcie kolejowym, Dz. U. z 2007 r. nr 60, poz. 407.

Rozporządzenie Komisji (UE) nr 1158/2010 z dnia 9 grudnia 2010 r. w sprawie wspólnej metody oceny bezpieczeństwa w odniesieniu do zgodności z wymogami dotyczącymi uzyskania kolejowych certyfikatów bezpieczeństwa.

Rozporządzenie Komisji (UE) nr 1169/2010 z dnia 10 grudnia 2010 r. w sprawie wspólnej metody oceny bezpieczeństwa w odniesieniu do zgodności z wymogami dotyczącymi uzyskania kolejowych autoryzacji w zakresie bezpieczeństwa.

Rozporządzenie wykonawcze Komisji (UE) nr 402/2013 z dnia 30 kwietnia 2013 r. w sprawie wspólnej metody oceny bezpieczeństwa w zakresie wyceny i oceny ryzyka i uchylające rozporządzenie (WE) nr 352/2009.

Sienkiewicz-Małyjurek K., Niczyporuk Z. (2010), *Bezpieczeństwo publiczne. Zarys problematyki*, Wydawnictwo Politechniki Śląskiej.

Sitarz M., Chruzik K., Mańka I. (2012), *Zintegrowany System Zarządzania Bezpieczeństwem Transportu Kolejowego w Polsce*, „Mechanika", 7-M.

Soliński B., *Metody zarządzania jakością FEMA. Analiza przyczyn wadliwości i krytyczności wad*, www.zarz.agh.edu.pl/bsolinsk/fmea.html, dostęp: 10.04.2019.

System Zarządzania Bezpieczeństwem wybranych licencjonowanych przewoźników kolejowych działających na rynku polskim, materiały wewnętrzne w formie powielonej.

www.utk.gov.pl/pl/raporty-i-analizy/analizy-i-monitoring, Statystyki przewozów pasażerskich i towarowych za lata 2007–2017, dostęp: 20.06.2019.

www.gov.pl/web/infrastruktura/raporty, Raporty roczne z prac Komisji Badania Wypadków Kolejowych za lata 2007–2017, dostęp: 15.06.2019.

Marek Krzywonos
marek.krzywonos@pwsz.krosno.pl
Państwowa Wyższa Szkoła Zawodowa im. Stanisława Pigonia w Krośnie,
Zakład Zarządzania

Działania interesariuszy wewnętrznych i zewnętrznych w poprawie bezpieczeństwa drogowego transportu towarów na terenie UE

Wprowadzenie

Celem rozdziału jest prezentacja i analiza działań interesariuszy wewnętrznych i zewnętrznych w celu poprawy bezpieczeństwa podczas realizacji usług transportowych na terenie UE. Działania, mające na celu zwiększenie bezpieczeństwa w drogowym transporcie towarów na terenie Unii Europejskiej, muszą być prowadzone kompleksowo. Istnieje konieczność podjęcia szeroko zakrojonych działań, aby zapewnić bezpieczeństwo w transporcie drogowym, zwłaszcza biorąc pod uwagę jego udział w PKB i liczbę zatrudnionych. Niniejszy rozdział jest rozwinięciem opublikowanych badań pilotażowych odnośnie zagrożeń w transporcie oraz sposobów przeciwdziałania im przez polskich przedsiębiorców realizujących usługi transportowe na obszarze UE [Krzywonos 2018].

Transport drogowy towarów w Unii Europejskiej jest najpopularniejszą gałęzią transportu, a jego znaczenie stale wzrasta.

Tabela 1. Udział gałęzi transportu w przewozie towarów w 2015 i 2017 roku (udział procentowy w przewozie tonokilometrów)

	Drogowy		Kolejowy		Wodny (śródlądowy)		Rurociągami	
Rok	2015	2017	2015	2017	2015	2017	2015	2017
Unia Europejska – 28	71,7	73,3	17,4	16,5	6,1	5,8	4,8	4,5
Polska	67,0	69,6	23,0	21,9	0,1	0,0	9,9	8,4
Niemcy	69,5	71,4	18,7	17,3	8,9	8,6	2,8	2,8
Hiszpania	89,3	90,7	5,6	4,9	-	-	5,1	4,4

Źródło: opracowanie własne na podstawie: *EU Transport in Figures, Statistical pocketbook 2017* oraz *EU Transport in Figures, Statistical pocketbook 2019*, https://www.ec.europa.eu, dostęp: 10.10.2019.

W tabeli 1 zaprezentowano dane odnośnie procentowego udziału w przewozie tonokilometrów w Unii Europejskiej, jak i kilku wybranych krajach. Oprócz Polski wybrano Niemcy (nasz największy partner gospodarczy) oraz Hiszpanię (kraj o podobnej liczbie ludności). Zaprezentowano dane dostępne w aktualnym raporcie *Transport in Figures* z 2019 roku (prezentującym dane z 2017 roku) oraz z roku 2017 (prezentującym dane z 2015 roku). Zarówno w całej Unii Europejskiej, jak i w wybranych krajach, daje się zauważyć wzrost udziału drogowego transportu towarów. Pomimo „szumnych" zapowiedzi (np. tiry na tory), a także promowania przez UE przewozów koleją oraz transportem śródlądowym, ich udział w przewozie towarów zmniejszył się w 2017 roku w porównaniu do 2015. Rokrocznie wzrasta ilość przewożonych towarów na obszarze UE, największym tego beneficjentem jest transport drogowy. Wiąże się to z jego zaletami, m.in. możliwością bezpośredniego przejazdu od miejsca załadunku do odbiorcy, możliwością przewozu niewielkich ilości różnorodnych towarów. W Europie Zachodniej transport kolejowy osiąga już maksimum swojej wydajności, zaś w Polsce jeszcze przez kilka lat będą trwały prace modernizacyjne na liniach kolejowych. W związku z tym wzrost przewozów kolejowych nie będzie wzrastał w szybkim tempie. Nie należy też spodziewać się wzrostu przewozów w transporcie wodnym śródlądowym. Zmiany klimatu (susze) powodują zmniejszenie transportu rzecznego, dało się to zwłaszcza zauważyć w 2018 roku na rzece Ren [https://www.dw.com/pl/susza-w-niemczech-problemy-z-transportem-rzecznym, 2018], jak i innych wykorzystywanych w transporcie. W Polsce transport śródlądowy ma marginalne znaczenie, w 2015 roku stanowił 0,1% przewozów (w tonokilometrach), zaś w 2017 roku jego udział spadł do poziomu niewykazywanego w danych opracowania *Transport in figures 2019*. W Polsce ok. 90% towarów transportowanych jest Odrzańską Drogą

Wodną. Postępująca degradacja tego szlaku wodnego powoduje utrudnienia podczas realizacji usług transportowych. Transport śródlądowy Wisłą możliwy jest tylko w górnym jej biegu (do Włocławka) oraz w okolicach Krakowa. Możliwość wykorzystania Wisły na dolnym jej biegu będzie wymagać budowy licznych stopni wodnych [Kulczyk, Skupień 2016]. Pomimo przeznaczania środków z funduszy europejskich, jest to mało prawdopodobne. Dochodzi tutaj też prawdopodobieństwo protestów organizacji ekologicznych w obronie „dzikiej Wisły".

Transport drogowy jako istotny element rynku pracy w Polsce i Unii Europejskiej

Drogowy transport towarów stanowi podstawę działalności wielu przedsiębiorstw, zarówno w Polsce, jak i pozostałych krajach Unii Europejskiej. Jest także miejscem pracy znacznej liczby osób. W tabeli 2 przedstawiono zatrudnienie w gałęzi transportu drogowego oraz liczbę przedsiębiorstw prowadzących taką działalność w 2014 i 2016 roku. Zaprezentowano dane dostępne w aktualnym raporcie *Transport in Figures* z 2019 roku (prezentującym dane z 2016 roku) oraz z roku 2017 (prezentującym dane z 2014 roku).

Tabela 2. Liczba przedsiębiorstw prowadzących działalność w drogowym transporcie towarów oraz zatrudnienie w nich w 2014 i 2016 roku

	Zatrudnienie (w tys.)		Liczba przedsiębiorstw	
Rok	2014	2016	2014	2016
Unia Europejska – 28	2 896,2	3 235,1	553 873	589 095
Polska	303,0	356,8	79 062	86 565
Niemcy	369,7	433,5	31 019	37 529
Hiszpania	302,6	320,6	102 535	106 405

Źródło: opracowanie własne na podstawie: *EU Transport in Figures, Statistical pocketbook 2017* oraz *EU Transport in Figures, Statistical pocketbook 2019*, https://www.ec.europa.eu, dostęp: 10.10.2019.

Zarówno w Unii Europejskiej, jak i w poszczególnych krajach, zauważalny jest wzrost liczby zatrudnionych i liczby przedsiębiorstw. Związane to jest z zapotrzebowaniem na transport rozwijającej się europejskiej gospodarki. Widać jednak

postępujący brak pracowników. W mediach podawana jest informacja o braku 100 tysięcy kierowców (Filary 2010, money.pl 2019). Rośnie też średnia wieków pracowników. Nie jest to zawód dający perspektywy rozwoju, młodzi ludzie nie są nim zainteresowani, zwłaszcza przy niskim bezrobociu. Kierowcy z Ukrainy też nie zapełnią wakatów, pomimo że już 80 tysięcy z nich zdobyło w Polsce prawo jazdy na ciężarówki. Praca w transporcie międzynarodowym nie jest obecnie konkurencyjna w stosunku do innych zawodów. System pracy (np. 3/1, 4/1) wpływa negatywnie na życie prywatne oraz zdrowie. Także warunki bytowe i sanitarne mają wpływ na negatywne postrzeganie pracy jako kierowca. W stosunku do wykonywanej pracy oraz odpowiedzialności, niski jest poziom wynagrodzeń. Po zakończeniu jazdy kierowca zostaje dozorcą przewożonego ładunku podczas postojów. Dochodzą także kwestie związane z bezpieczeństwem, kierowcy padają ofiarami przestępstw. Działania, mające na celu poprawę bezpieczeństwa pracy jako kierowca, wpłyną na lepsze postrzeganie tego zawodu oraz większe zainteresowanie nim.

Zagrożenia występujące podczas realizacji usług transportowych na terenie UE

Podczas realizacji usług transportowych należy brać pod uwagę możliwość wystąpienia różnorodnych zagrożeń. Kompleksowe przeciwdziałanie im przez organy państwa jest niemożliwe ze względu na ich zmienność oraz rozproszenie działań firm transportowych. Zagrożenia mogą występować pojedynczo lub łącznie, co utrudnia przeciwdziałanie.

Przeprowadzone w 2018 roku badania ankietowe na próbie przedsiębiorstw transportowych funkcjonujących na terenie Polski południowo-wschodniej, realizujących przewozy na terenie UE, wykazały, z jak różnorodnymi zagrożeniami stykają się te firmy. Najczęstszymi z nich są: przestępczość kryminalna, kradzieże (lub próby kradzieży) paliwa, przewożonego ładunku, rzeczy osobistych kierowcy. Kierowcy ankietowanych firm stykali się także z zagrożeniami związanymi z masową migracją: uszkodzeniem naczepy i/lub przewożonego ładunku podczas próby dostania się do naczepy pojazdu przez nielegalnych emigrantów; blokadami dróg, mającymi na celu wymuszenie ukrycia w naczepie nielegalnych emigrantów i przewiezienia ich przez granicę. Wystąpienie zagrożeń prowadziło

do zakłóceń w realizacji przewozów, m.in. uszkodzenia ładunku, nieterminowej dostawy [Krzywonos 2018].

Działania interesariuszy wewnętrznych i zewnętrznych

W tabeli 3 przedstawiono zidentyfikowanych interesariuszy wewnętrznych i zewnętrznych, których działania mają wpływ na zapewnianie bezpieczeństwa w drogowym transporcie towarów.

Tabela 3. Interesariusze wewnętrzni i zewnętrzni prowadzący działania mające wpływ poprawę bezpieczeństwa w drogowym transporcie towarów

Interesariusze wewnętrzni:	Interesariusze zewnętrzni:
Kierowcy	Klienci
Kadra zarządzająca	Dostawcy
	Konkurenci (głównie zagraniczni)
	Stowarzyszenia przewoźników
	Związki zawodowe kierowców
	Władze państwowe
	Służby mundurowe (policja, straż graniczna, inspekcja transportu)

Źródło: opracowanie własne.

Zarówno interesariusze wewnętrzni, jak i zewnętrzni, podejmują wiele działań mających na celu poprawę bezpieczeństwa w transporcie. Działania te nie są jednak skoordynowane ze sobą, przez to nieosiągany jest efekt synergii.

Przeprowadzone w 2018 roku badania pokazują, iż w 2/3 przedsiębiorstw prowadzone są działania mające na celu poprawę bezpieczeństwa kierowców, pojazdów oraz przewożonych ładunków [Krzywonos 2018].

Kadra zarządzająca przedsiębiorstwami transportowymi realizuje wiele działań w celu zapewniania bezpieczeństwa. Pierwsze z nich to korzystanie z lokalizatorów GPS, dzięki nim dyspozytorzy mają możliwość określenia miejsca, w którym znajduje się pojazd. Dzięki temu istnieje możliwość monitorowania i przekazania informacji o potencjalnie niebezpiecznych miejscach na trasie. Prowadzone są także szkolenia dla kierowców odnośnie reakcji na wystąpienie zagrożenia, jak również metod minimalizacji prawdopodobieństwa ich wystąpienia. Podczas szkoleń kierowcom przekazywane są informacje w zakresie konieczności wyboru

bezpiecznych miejsc parkingowych, jednak często jest to tylko porada teoretyczna. Na terenie całej Unii Europejskiej brakuje miejsc parkingowych dla pojazdów ciężarowych, a rozwój infrastruktury parkingowej nie nadąża za wzrostem liczby przewozów. Niestety tylko część przedsiębiorstw transportowych umożliwia korzystanie z płatnych (strzeżonych) parkingów na koszt firmy. Na szkoleniach przekazywane są także informacje dotyczące reakcji na wystąpienie zagrożenia np. żeby w trakcie próby kradzieży paliwa nie wychodzić z kabiny, tylko oczekiwać na przyjazd wezwanej policji. Część firm dostosowuje trasy przejazdów w ten sposób, aby planowane postoje (pauzy) odbywały się w miejscach bezpiecznych. Zdarzają się również sytuacje rezygnacji z realizacji zlecenia, np. ze względu na to, że załadunek lub wyładunek miałby odbyć się w niebezpiecznej okolicy.

Podczas realizacji przewozów kierowcy także podejmują działania mające na celu zapewnianie bezpieczeństwa zarówno im samym, jak i przewożonemu ładunkowi oraz pojazdowi ciężarowemu. Powszechnie stosowane są aplikacje mobilne, ułatwiające wiele aspektów działań związanych z zapewnianiem bezpieczeństwa. Najpopularniejsze są aplikacje nawigacyjne, ułatwiające wyznaczanie tras przejazdów oraz poszukiwanie miejsc na postój. Jednak niekiedy korzystanie z nawigacji może spowodować wystąpienie zagrożenia, nie ma tam bowiem wprowadzonych obszarów tzw. *no-go zone* (określane we Francji jako *zone urbaine sensible* – wrażliwy obszar miejski). Są to tereny, na których policja nie ma pełnej kontroli, a jeśli stara się ją odzyskać, to tylko w większych grupach. Aplikacje nawigacyjne wyznaczają trasy przez niebezpieczne tereny, może też dojść do konieczności przerwy (pauzy) w takim miejscu. Drugą z aplikacji stosowanych powszechnie przez kierowców są aplikacje wyszukujące parkingi dla ciężarówek, a także rezerwacji miejsca parkingowego, niektóre z nich umożliwiają też dokonywanie opłat za parkowanie. Dzięki takim aplikacjom kierowcy mają możliwość odpoczynku nocnego w bezpiecznym miejscu. Kolejnymi przydatnymi z punktu widzenia zapewniania bezpieczeństwa aplikacjami są informujące o zakazach ruchu pojazdów ciężarowych. Terminy ich obowiązywania różnią się w poszczególnych państwach UE. Zależą m.in. od świąt narodowych, obowiązujących przepisów (np. w weekendy) [Kuczerska 2017].

Kierowcy podejmują także działania bezpośrednie. W przypadku dłuższego postoju bez ładunku (np. w nocy) pozostawiają tzw. okienko (otwór w plandece), umożliwiające obejrzenie wnętrza naczepy potencjalnemu przestępcy, aby nie dokonywał zniszczeń podczas próby dostania się do pojazdu. W przypadkach braku możliwości pozostawienia okienka, zostawiane są uchylone drzwi naczepy.

W okresie kryzysu migracyjnego w latach 2015–2016 występowały przypadki, gdy polscy kierowcy z różnych firm tworzyli konwoje podczas przejazdów

na terenie Europy Zachodniej. Była to szczególna sytuacja. Poprzednio konwoje tworzone były na początku lat dziewięćdziesiątych podczas przewozów towarów na obszarze krajów Wspólnoty Niepodległych Państw.

Nie należy zapominać, że kierowcy są skonsolidowaną grupą zawodową. Wymieniają się informacjami i poradami odnośnie zapewniania bezpieczeństwa, zarówno na postojach, jak i poprzez CB radio oraz media społecznościowe.

Poprawą bezpieczeństwa w drogowym transporcie towarów na obszarze Unii Europejskiej zainteresowani są także liczni interesariusze zewnętrzni. Pośród nich można wymienić: klientów, dostawców, konkurentów (głównie zagranicznych), stowarzyszenia przewoźników, związki zawodowe kierowców, władze państwowe, służby mundurowe (policja, straż graniczna, inspekcja transportu). Podejmują oni działania we współpracy ze sobą, często jednak prowadzą samodzielnie działania nieskoordynowane.

Jednym z problemów, z jakimi borykają się kierowcy, jest brak parkingów, a w szczególności bezpiecznych miejsc parkingowych. Brak odpowiedniej infrastruktury wymusza parkowanie w miejscach nieoświetlonych, nieogrodzonych, często nawet niedozwolonych. Problem ten w szczególności dotyczy Niemiec, głównego kraju tranzytowego dla polskich przewoźników. Szacuje się, że codziennie 50 tys. kierowców ma problemy ze znalezieniem odpowiedniego miejsca parkingowego w Niemczech. Sytuacja ta nie dotyczy tylko Niemiec, ale wszystkich krajów UE. Rodzaj miejsca parkingowego ma wpływ na odpowiedzialność finansową przewoźnika w przypadku potencjalnej kradzieży. Konieczność poszukiwania miejsca parkingowego powoduje przekroczenie czasu pracy przez kierowców, narażając ich oraz przewoźników na kary finansowe [Kulikowska-Wielgus i in. 2019]. Interesariusze zewnętrzni podejmują działania mające na celu zapewnienie odpowiedniej liczby bezpiecznych miejsc parkingowych. Stowarzyszenia przewoźników oraz związki zawodowe kierowców prowadzą działania lobbingowe w celu budowy parkingów przez władze państwowe. Postulują zmiany prawne zapewniające na parkingach odpowiednią infrastrukturę, a także wprowadzające ułatwienia proceduralne przy budowie nowych parkingów. Klienci również mają wpływ na dostępność miejsc parkingowych. Często kierowca spędza noc pod miejscem załadunku lub wyładunku, nie zawsze z możliwością wjazdu na ogrodzony teren firmy. Taki postój na terenie ogrodzonym, który najczęściej też jest chroniony, znacznie ogranicza występowanie potencjalnych zagrożeń.

Pośrednio na bezpieczeństwo w transporcie wpływają także przepisy odnośnie delegowania pracowników i płacy minimalnej. Polscy przewoźnicy w szczególności muszą stosować przepisy wprowadzone w Niemczech, „Mindestlohngesetz”,

określane jako MiLoG oraz we Francji – „Loi Macron" (od nazwiska prezydenta, który był ich projektodawcą). Przepisy MiLoG wprowadziły zagrożenie sankcją karną do 500 tys. euro w przypadku niezapłacenia stawki minimalnej dla pracownika lub pracownika podwykonawcy. Zdarzają się przypadki, iż niemiecki zleceniodawca odmówił zapłaty za przewóz kabotażowy polskim firmom, dopóki nie wykażą, że wypłata wynagrodzenia zgodna była z przepisami MiLoG. Zaś niemieckie sądy w takich przypadkach mają niespójną linię orzeczniczą. Stosowanie tych przepisów uderza w polskich przedsiębiorców transportowych, są to dla nich ważne rynki, jak również kraje tranzytowe. Będzie miało też wpływ na bezpieczeństwo. Przewoźnicy i kierowcy będą mieli mniejsze zaufanie do zarządzeń i zaleceń organów ww. państw [Bujak, Wieczorek 2017; Liberadzki 2015].

Wnioski

Polskie firmy transportowe zaczynają odgrywać dominującą rolę na europejskim rynku przewozowym. Jest to rynek, na którym corocznie zwiększa się liczba zleceń oraz przewożonych ładunków. Dzięki długoletniemu rozwojowi polscy przedsiębiorcy i kierowcy wyrobili sobie dobrą markę na rynkach krajów UE. Jednak dalszy rozwój niesie za sobą wiele wyzwań, w tym związanych z koniecznością zapewniania bezpieczeństwa. Podczas realizacji przewozów pojawiają się ciągle nowe zagrożenia, a występujące od lat wcale nie zmniejszają częstości występowania. Wprowadzenie kompleksowych metod zapewniania bezpieczeństwa kierowców, pojazdów i ładunków jest konieczne, aby zapewnić utrzymanie pozycji rynkowej, a nawet dalszy rozwój. Większość polskich przedsiębiorstw transportowych to małe firmy, samodzielnie niebędące w stanie podołać temu organizacyjnie i finansowo. Konieczna jest współpraca z interesariuszami zewnętrznymi. Szczególnie predystynowane do takich działań są stowarzyszenia przewoźników, zajmujące się transportem międzynarodowym. Stowarzyszenia są żywotnie zainteresowane rozwojem przedsiębiorstw (ich członków), a także posiadają zdolności organizacyjne, aby podjąć się wypracowania kompleksowych metod zapewnienia bezpieczeństwa. Cenna byłaby także współpraca stowarzyszeń. W Polsce funkcjonuje już 26 organizacji konsolidujących przewoźników międzynarodowych [gitd.gov.pl 2019].

Przydatna byłaby też współpraca z organami państwa polskiego. Jednak pomimo faktu, że przedsiębiorstwa transportowe stanowią istotny element

gospodarki narodowej, dostarczając niebagatelnych wpływów do budżetu, wszystko zależy od woli politycznej.

Także nauka musi mieć swój udział we wspomaganiu rozwoju polskich przedsiębiorstw transportowych. Współpraca z biznesem przyniosłaby korzyści obydwu stronom.

Bibliografia

Bujak A., Wieczorek G. (2017), *Szanse i zagrożenia funkcjonowania oraz rozwoju transportu drogowego w europejskiej przestrzeni gospodarczej w ocenie firm transportowych Dolnego Śląska,* „Zeszyty Naukowe Politechniki Śląskiej, Seria Organizacja i Zarządzanie", z. 103, ss. 17–32.

Filary S. (2010). *Bezpieczeństwo w komunikacji powszechnej i transporcie*, Poznań: Wydawnictwo Wyższej Szkoły Bankowej w Poznaniu.

https://www.dw.com/pl/susza-w-niemczech-problemy-z-transportem-rzecznym, dostęp: 20.09.2019.

https://gitd.gov.pl/dla-przedsiebiorcow/zezwolenia/przewoz-rzeczy/stowarzyszenia/wykaz-stowarzyszen-przewoznikow-miedzynarodowych/, dostęp: 10.10.2019.

https://www.money.pl/gospodarka/brakuje-zawodowych-kierowcow-ponad-100-tys-wolnych-etatow-6408418941367937a.html, dostęp: 20.09.2019.

Komisja Europejska (2018), *EU Transport in Figures, Statistical pocketbook 2017*, https://www.ec.europa.eu, dostęp: 10.10.2019.

Komisja Europejska (2019), *EU Transport in Figures, Statistical pocketbook 2019*, https://www.ec.europa.eu, dostęp: 10.10.2019.

Krzywonos M. (2018), *Analiza występowania zagrożeń podczas realizacji usług transportowych na terenie UE,* „Przedsiębiorczość i Zarządzanie", T. XIX, z. 8, cz. II, ss. 233–246.

Kulczyk J., Skupień E. (2016), *Śródlądowy transport wodny w Polsce – stan obecny i perspektywy rozwoju,* „Problemy Transportu i Logistyki", nr 4(36), ss. 59–70.

Kulikowska-Wielgus A., Ziemkowska D., Wawrzyszuk B. i in. (2019), *Bariery w transporcie drogowym*, Wydawnictwo Fundacji Republikańskiej, Warszawa.

Kuczerska D. (2017), *Aplikacje mobilne w aspekcie ich wykorzystania przez kierowców zawodowych*, „Przegląd Nauk Ekonomicznych", nr XXVI, ss. 277–290.

Liberadzki B. (2015), *Konkurencja i kooperacja w europejskim transporcie samochodowym a niemiecka ustawa Milog*, „Problemy Transportu i Logistyki", nr 29, ss. 147–179.

ISBN 978-83-64971-79-2

Społeczna Akademia Nauk
Łódź

www.san.edu.pl