PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE
ŁÓDŹ - WARSZAWA 2018 | ISSN 2543-8190
XIX TOM
1 ZESZYT
III CZĘŚĆ

Redakcja naukowa:
Zofia Wilk-Woś
Andrzej Marjański

Bezpieczeństwo i zarządzanie kryzysowe. Wybrane problemy

WYDAWNICTWO
SPOŁECZNEJ AKADEMII NAUK

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE

ŁÓDŹ - WARSZAWA 2018 | ISSN 2543-8190

XIX TOM
1 ZESZYT
III CZĘŚĆ

Redakcja naukowa:

Zofia Wilk-Woś

Andrzej Marjański

Bezpieczeństwo i zarządzanie kryzysowe.

Wybrane problemy

WYDAWNICTWO
SPOŁECZNEJ AKADEMII NAUK

Zeszyt recenzowany

Redakcja naukowa: Zofia Wilk-Woś, Andrzej Marjański

Korekta językowa: Małgorzata Pająk, Lidia Pernak, Beata Siczek
Agnieszka Śliz, Dominika Świech
Komputerowy skład tekstu: Jadwiga Poczyczyńska

Projekt okładki: Marcin Szadkowski

ISSN: 2543-8190

Wydawnictwo
Społecznej Akademii Nauk
e-mail: **wydawnictwo@spoleczna.pl**
tel. 42 632 50 23, 42 632 50 26 w. 339

Wersja elektroniczna jest wersją podstawową publikacji, dostępną na stronie:
http://piz.san.edu.pl

WYDAWNICTWO
SPOŁECZNEJ AKADEMII NAUK

Spis treści

Wstęp

Problemy bezpieczeństwa należą do najistotniejszych kwestii zarówno w badaniach teoretycznych, jak i w obszarze praktycznych rozwiązań dla państwa, stojącego w obliczu rosnących zagrożeń, które charakteryzują się coraz większą zmiennością i wielowymiarowością. Współczesne zagrożenia bezpieczeństwa dotyczą większości obszarów funkcjonowania społeczeństwa i mogą wystąpić z różną intensywnością oraz mieć nieprzewidywalne skutki. Bezpieczeństwo ma charakter podmiotowy i stanowi naczelną potrzebę jednostek i grup społecznych, ale także kluczowa potrzebę państwa. Ważne staje się poznanie i opisanie nowych wyzwań tak w środowisku wewnętrznym, jak zewnętrznym państwa, aby w odpowiedni sposób kształtować strategie i rozwijać skuteczne metody zarządzania bezpieczeństwem.

Zasadniczym celem prezentowanego zeszytu jest dostarczenie Czytelnikowi interesujących i aktualnych studiów, które skłonią go do refleksji nad złożoną problematyką bezpieczeństwa i zarządzania kryzysowego. Kluczowym elementem doskonalenia systemu bezpieczeństwa są badania naukowe oraz wykorzystanie ich wyników w praktycznym doskonaleniu zarządzania bezpieczeństwem.

Pierwsza część niniejszej publikacji poświęcona jest zagadnieniom zarządzania kryzysowego i ratownictwa. Zarządzanie kryzysowe stanowi niewątpliwie jeden z najbardziej złożonych rodzajów zarządzania, ponieważ powstanie sytuacji kryzysowej z powodu występowania presji czasu, silnej presji społecznej i na ogół ograniczonej przestrzeni wystąpienia ogniskuje niemal wszystkie problemy zarządcze i ujawnia wady złych rozwiązań. W systemie zarządzania kryzysowego konieczne jest współdziałanie i koordynacja wielu służb ratowniczych. Autor pierwszego artykułu wskazuje na znaczenie i istotę planowania w sytuacji kryzysowej, drugi badacz szuka odpowiedzi na pytanie czy, a jeśli tak, to w jakim zakresie, rozszerzona rzeczywistość podnosi poziom bezpieczeństwa, kolejny zaś poprzez analizę organizacji oraz zakresu działalności Wojewódzkiego Centrum Zarządzania Kryzysowego w Kielcach stara się określić, w jaki sposób organizacja Centrum przekłada się na jego funkcjonowanie. Autorzy czwartej dysertacji w tej części publikacji podejmują próbę oceny systemu powiadamiania ratunkowego oraz określenia w nim roli Centrów Powiadamiania Ratunkowego w oparciu o systemowy model organizacji zaproponowany przez Harolda Leavitta.

Policja jest największą formacją mundurową w Polsce, realizującą bardzo szeroki zakres zadań w obszarze bezpieczeństwa, istotne jest więc dokonanie oceny istniejącego w Policji systemu szkolenia i doskonalenia zawodowego pod kątem możliwości budowania i utrzymania przez policjantów kompetencji dowódczych umożliwiających sprawne i skuteczne realizowanie działań w przypadku wystąpienia zdarzenia kryzysowego. Zagadnienie to jest tematem kolejnego artykułu, w którym autor akcentuje potrzebę stworzenia całościowego systemu budowania kompetencji dowódczych. Ostatni tekst tej części zeszytu omawia zastosowanie założeń nowej ustawy antyterrorystycznej w systemie zarządzania kryzysowego RP.

Kolejne trzy prace dotyczą aktualnych problemów bezpieczeństwa w cyberprzestrzeni, w tym niezwykle istotnej kwestii zagrożeń i sposobów ochrony dzieci w Internecie. Ten obszar staje się coraz istotniejszy dla zapewnienia bezpieczeństwa zarówno w przestrzeni publicznej, jak i wymiarze indywidualnym.

W ostatniej – trzeciej – części zeszytu znalazły się prace omawiające kolejno: możliwość wykorzystania podejścia scenariuszowego w badaniach bezpieczeństwa, kluczowe kwestie związane z bezpieczeństwem społeczności lokalnych (rolę Obrony Cywilnej, Policji i Straży Pożarnej w kreowaniu bezpieczeństwa na poziomie lokalnym), bezpieczeństwo energetyczne, kwestie bezpieczeństwa międzynarodowego, w tym między innymi problem zaangażowania polskich okrętów w działania stałych zespołów NATO.

Autorzy oraz redaktorzy niniejszej publikacji mają nadzieję, że zaprezentowane w tomie prace będą stanowić istotny głos w dyskusji o bezpieczeństwie i zarządzaniu kryzysowym pozwalający na implementację dorobku badań naukowych do praktycznych rozwiązań stosowanych w systemie zarządzania bezpieczeństwem.

Zofia Wilk-Woś
Andrzej Marjański

Zarządzanie kryzysowe i ratownictwo

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **9–21**

Monika Ostrowska[1]
Wydział Nauk o Bezpieczeństwie, Krakowska Akademia im. A. F. Modrzewskiego

Planowanie w sytuacji kryzysowej

Planning in the Crisis Management

Abstract: It is fairly common for crisis events to occur unexpectedly and to bring consequences whose negative nature goes well beyond the means available to local rescue services. Therefore, measures taken at the first stage of the crisis are usually chaotic, especially in terms of organisation. This also results from the lack of sufficient knowledge regarding the intensity and consequences of emergency events. These seem to be the most essential factors to be considered in the entire crisis management process. The article describes the role and significance of planning in the crisis management system.
Key words: security, management, crisis management, emergency planning

Wprowadzenie

Zarządzanie to koordynowanie działań ludzkich dla osiągnięcia zamierzonych celów, w sposób możliwie najbardziej efektywny. Zarządzanie definiowane jest także jako działalność kierownicza, polegająca na ustaleniu celów oraz powodowaniu ich realizacji poprzez wykorzystanie odpowiednich zasobów, procesów informacji w istniejącym otoczeniu (kulturowym, prawnym, społecznym, ekonomicznym itp.) [Daniluk 2011/2012, ss. 83–85]. Wykorzystanie to musi odbyć się w sposób sprawny oraz skuteczny i zgodny z racjonalnością zadań. Inna definicja zarządzania mówi, że jest to dysponowanie zasobami dla uzyskania korzyści, panowanie nad różnorodnością i przekształcenie potencjalnego konfliktu we współpracę [Walas-Trębacz, Ziarko 2010, ss. 10–11].

[1] m.ostrowska@onet.pl

Zarządzanie jest systemem organizowania się społeczeństwa. Zawiera elementy planowania, oceny warunków aktualnych oraz umiejętność zbierania, analizowania i przetwarzania informacji w celu podnoszenia jakości w określonej sferze [Sienkiewicz-Małyjurek, Krynojewski 2010, ss. 11–13]. Zarządzanie ma wiele definicji. Bardzo często jest definiowane w konkretnym kontekście, możemy mówić zarówno o zarządzaniu w strefie prywatnej (np. zarządzanie swoim własnym czasem, zdolnościami itp.), jak i publicznej (np. zarządzanie zasobami w przedsiębiorstwie, zarządzanie ryzykiem, zarządzanie systemowe połączone z określoną dziedziną) [Charette, Mitchell, Mazur, McSweeney 2004, ss. 23–26]. Zarządzanie obejmuje bardzo różne zagadnienia. W jego ramach możemy omawiać sposób, formę, zakres zarządzania, wpływ zarządzania na możliwości dokonywania zmian. Zarządzanie możemy ujmować nie tylko w kontekście jego efektów, ale i w perspektywie samej techniki zarządzania [Mikuła, Pietruszka-Ortyl, Potocki 2002, ss. 39–45]. Każdorazowo jednak zarządzanie musi uwzględniać kilka stałych elementów, wspomnianych powyżej. Podstawą zarządzania w ogóle jest określenie konkretnej dziedziny, którą ma ono obejmować. Z tego też względu często niemożliwe będzie porównywanie zarządzania w różnych sferach, ponieważ metody zarządzania w jednej dziedzinie będą zupełnie różne od metod zarządzania w innej. Na przykład w zarządzaniu systemem ochrony zdrowotnej priorytetem powinno być ratowanie życia ludzkiego i zapewnianie tej opieki wszystkim osobom uprawnionym, z kolei w przypadku zarządzania przedsiębiorstwem nastawionym na zysk, które musi opierać się na sprzedaży, wymagane jest agresywne zarządzanie nastawione na podnoszenie efektów pracy [Lewandowski, Kautsch, Sułkowski 2013, ss. 179–345].

W aspekcie systemowym, jak twierdzi Penc [1998, s. 25], zarządzanie pozwala na wykorzystanie całości zasobów organizacji ujętych w fundamentalnych podsystemach, takich jak zasoby ludzkie, technologie, struktury organizacyjne i cele.

Celem artykułu jest przedstawienie znaczenia i istoty planowania w sytuacji kryzysowej.

Rola i zasady zarządzania kryzysowego

Zarządzanie kryzysowe jest nieodzownym elementem bezpieczeństwa narodowego. Pełni bardzo ważną rolę w rozwiązywaniu wszelkich problemów związanych z bezpieczeństwem, przeciwdziałaniu oraz przygotowywaniu się na zagrożenia, które mogą wystąpić. Polega na podtrzymaniu oraz przywracaniu sytuacji stabilizacji. Zarządzanie kryzysowe to celowe działanie podejmowane przez organy rządu na wszystkich poziomach organizacji państwa, z uwzględnieniem wyspecjalizowanych organizacji,

straży i inspekcji, a także angażujące społeczeństwo [Sienkiewicz-Małyjurek, Krynojewski 2010, s. 11]. Postrzeganie zarządzania kryzysowego jako zespołu zamiarów związanych z działalnością po wystąpieniu niebezpieczeństwa jest spojrzeniem bardzo wąskim. Dzisiejsze zarządzanie kryzysowe stanowi zbiór działań, które składają się ze współgrających ze sobą elementów. Obejmuje struktury organizacyjne, a także zadania pozwalajace na osiągnięcie celu:

- zmniejszenie prawdopodobieństwa działania kryzysu,
- osiąganie kontroli nad konfliktem,
- ograniczenie rezultatów kryzysu,
- usunięcie skutków i odnowę,
- umożliwienie władzy podjęcie odpowiednich kroków, które pozwolą na rozwój kryzysu w odpowiednim kierunku, by osiągnąć optymalne rozwiązania.

Zarządzanie kryzysowe, za które odpowiedzialne są organy administracji publicznej, jest elementem kierowania bezpieczeństwem narodowym. Polega ono 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 [Więcek, Bieniek 2014, s. 38].

Do głównych zasad zarządzania kryzysowego należą:

1. Zasada prymatu układu terytorialnego – uznaje za podstawową konstrukcję modelu terytorialnego układ państwa oraz sprowadza do funkcji pomocniczej układ branżowy.
2. Zasada jednoosobowego kierownictwa – oznacza, że wszystkie decyzje podejmuje się jednoosobowo i odpowiada się za nie także jednoosobowo.
3. Zasada odpowiedzialności organów władzy publicznej – oznacza, że organy władzy publicznej przyjmują kompetencje oraz odpowiedzialność w zakresie podejmowania decyzji w określonej sytuacji kryzysowej.
4. Zasada zespolenia – oznacza przyznanie organom władz administracyjnych głównej kompetencji, gwarantującej wywiązanie się z nałożonej na nie odpowiedzialności.
5. Zasada kategoryzacji zagrożeń – dotyczy podziału zagrożeń na grupy według rodzaju oraz rozmiaru. Dodatkowo przyporządkowuje się zagrożeniom określone rozwiązania prawne, organizacyjne i finansowe.
6. Zasada powszechności – oznacza, że zarządzanie kryzysowe organizują organy władzy publicznej we współdziałaniu z istniejącymi specjalistycznymi instytucjami i organizacjami oraz ogółem społeczeństwa [Sobolewski 2011, s. 67].

Głównym celem zarządzania kryzysowego według Sienkiewicz-Małyjurek [2015, ss. 12–14] jest zapewnienie bezpieczeństwa ludności oraz stworzenie warunków do rozwoju wszelkim podmiotom na określonym obszarze. Zarządzanie kryzysowe obejmuje:

1) wszystkie trzy rodzaje zagrożeń:
   - naturalne i nienaturalne,
   - techniczne,
   - wojenne,
2) wszystkie poziomy zarządzania (związane z poziomami władzy):
   - lokalny,
   - wojewódzki,
   - centralny.

Po zapoznaniu się z literaturą oraz aktami normatywnymi można stwierdzić, że na zarządzanie kryzysowe składają się określone fazy:

a) Zapobieganie, czyli działania mające za zadanie wyeliminowanie lub redukcję prawdopodobieństwa wystąpienia katastrofy albo ograniczanie jej skutków poprzez:
   - analizę (kategoryzację zagrożeń),
   - ocenę wrażliwości społeczeństwa na zagrożenia,
   - regulacje prawne,
   - racjonalne planowanie zagospodarowania przestrzennego,
   - gospodarkę budżetową,
   - ocenę strat ludzkich, mienia i infrastruktury powodowanych przez katastrofę,
   - określenie planu działań zapobiegawczych,
   - określenie zasad i sposobów kontroli i nadzoru.
b) Przygotowanie, którego celem jest wskazanie, jak należy zareagować w przypadku wystąpienia katastrofy oraz jakie podjąć działania w celu powiększenia zasobów sił i środków niezbędnych do efektywnego reagowania poprzez:
   - opracowanie planu zarządzania kryzysowego,
   - budowę centrum zarządzania kryzysowego,
   - określenie zasad komunikacji,
   - określenie systemów monitorowania,
   - organizację systemu alarmowania i ostrzegania ludności,
   - określenie procedur zwracania się o pomoc i jej udzielania,
   - określenie zasad stosowania przymusu prawnego w stosunku do ludności, organizacji pozarządowych i sektora prywatnego,

- tworzenie baz magazynowych oraz baz danych zbierających informacje o możliwości pozyskania środków i materiałów,
- opracowanie baz danych,
- edukację społeczeństwa,
- doskonalenie służb ratowniczych,
- akceptację społeczną poniesionych kosztów,
- uaktualnianie elementów przygotowania.

c) Reagowanie, czyli zespół przedsięwzięć następujących po wystąpieniu katastrofy. Z kolei celem reagowania jest dostarczenie pomocy poszkodowanym i ograniczenie wtórnych zniszczeń i strat poprzez:
   - uruchomienie procesu ciągłej informacji (zarządzanie informacją),
   - zorganizowanie punktu kontaktowego (informowanie ludności),
   - uruchomienie systemu ostrzegania i alarmowania,
   - natychmiastową reakcję społeczności lokalnej,
   - uruchomienie procedur,
   - uruchomienie struktur ratowniczych,
   - uruchomienie procesu ewakuacji,
   - neutralizację ognisk zagrożeń,
   - organizowanie samopomocy społecznej,
   - wsparcie operacyjne sił zbrojnych,
   - udział organizacji społecznych i humanitarnych,
   - uruchomienie ochrony psychologicznej ofiar,
   - stworzenie doraźnych warunków do przetrwania osób poszkodowanych.

d) Odbudowa, czyli działania mające na celu przywrócenie stanu poprzedniego oraz odtworzenie infrastruktury mniej wrażliwej na kolejną katastrofę poprzez:
   - szacowanie szkód,
   - zapewnienie pomocy ludności,
   - leczenie i rehabilitację,
   - wypłacenie odszkodowań poszkodowanym,
   - informowanie o prawach i obowiązkach,
   - odtwarzanie i uzupełnianie zapasów,
   - zapewnienie gotowości służb ratowniczych,
   - przywrócenie równowagi i bezpieczeństwa ekologicznego,
   - odbudowę i przywrócenie sprawności infrastruktury,
   - inicjatywę legislacyjną,
   - sprawne administrowanie,
   - rozliczenie kosztów reagowania (rozliczenie zobowiązań),

- podsumowanie i wnioski,
- modyfikację i aktualizację planów reagowania,
- prace dokumentacyjne (sprawozdania i raporty) [Szczupaczyński 2002; Grocki 2012; Sienkiewicz-Małyjurek 2015].

Na zarządzanie, czyli planowanie, analizę, sterowanie składają się:

- cele, czyli plany, zadania,
- działania, czyli dysponowanie, kierowanie, planowanie, kontrolowanie,
- władza, czyli kierownik, zwierzchnik,
- zasoby, czyli informacje,
- obiekt, czyli organizacja, motywacje, potrzeby.

Ustawa o zarządzaniu kryzysowym

Ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 r. [Dz. U. z 2007 r. Nr 89, poz. 590] jest jednym z podstawowych dokumentów regulujących sposób prowadzenia działań w celu zwiększenia poziomu bezpieczeństwa lokalnego. Ponieważ kwestie te są regulowane w wielu ustawach, często bardzo odległych od siebie tematycznie, sama ustawa w wielu miejscach powtarza te uregulowania bądź przyjmuje jedynie ogólne założenia, których rozwinięciem mają być akty prawa wewnętrznego czy inne akty rangi ustawy, bądź rozporządzenia. Wprowadzenie ustawy wydaje się jednak uzasadnione – zbiera ona w jednym miejscu wszystkie najistotniejsze dla bezpieczeństwa państwa i poszczególnych regionów kwestie, a więc staje się faktyczną podstawą działania wszystkich jednostek

Ustawa zobowiązuje bezpośrednio organy administracji samorządowej oraz rządowej do planowania różnych możliwości i sposobów reagowania na wszelkiego rodzaju zdarzenia i przeciwności losu.

Przedmiotowa ustawa jest regulacją dość krótką, jednak w szerokim zakresie prezentuje wiele różnych systemów składających się na system bezpieczeństwa. Ustala system przekazu informacji ze szczebla niższego do szczebla wyższego administracji publicznej, wskazuje osoby, grupy osób i instytucje odpowiedzialne za bezpieczeństwo w różnych, wycinkowych sferach. Określa stosunek zależności i formy współdziałania między tymi osobami w zakresie przygotowania na sytuację zagrożenia oraz w czasie jej wystąpienia. Dzięki odniesieniu się do innych dokumentów regulujących wprost kompetencje poszczególnych osób określa bardzo szeroki zakres faktycznych możliwości współpracy i obowiązków poszczególnych osób.

W myśl ustawy oraz literatury planowanie kryzysowe jest elementem kierowania, polegającym na decydowaniu o racjonalnym wykorzystaniu sił oraz środków na polu walki z określonym kryzysem.

Istotą planowania jest rozpoznanie przyszłości i określenie w dokumencie zwanym planem zadań środków potrzebnych do realizacji przyszłych działań jednostki dla realizacji założonego celu (społecznego) w odniesieniu do zadań strategicznych, taktycznych i operacyjnych.

Praktyczny wymiar planowania obejmuje wiele ważnych czynności, w szczególności zaś: poznanie terenu własnego działania, poznanie istniejących w tym środowisku procesów, zaznajomienie się z dotychczasowymi postępami, zagrożeniami i możliwościami. Konieczne jest jak najpełniejsze poznanie całego środowiska i natury procesu, który będziemy kontrolować, by podczas późniejszej analizy wiedzieć, które zmienne były brane pod uwagę, a które pojawiły się lub ujawniły już po wprowadzeniu planu w życie. Cechami dobrego planu powinny być z tego względu: szczegółowość, dogłębność, zapewnienie możliwości działania alternatywnego, wieloaspektowość i wnikliwość [Naruć, Nowak, Wieloch 2008, ss. 19–23].

Dzięki temu, że istnieją wieloletnie plany w zakresie zarządzania kryzysowego oraz powtarzane przez lata działania, osoby zajmujące się planowaniem dysponują dość dużą pulą informacji.

Znaczenie planowania w zarządzaniu kryzysowym

Schemat procesu planowania według R. Grockiego [2012, s. 105] obejmuje następujące punkty:

- Jakie działanie musi być podjęte?
- Dlaczego to działanie musi być podjęte?
- Gdzie zostanie podjęte działanie?
- Kiedy działanie zostanie podjęte?
- Kto odpowiada za działanie?
- Jak podjęte zostanie działanie?

Według Grockiego [2012, s. 105] do rozpoczęcia planowania konieczne jest posiadanie wiedzy dotyczącej zakresu opracowania planu, jego struktury, zawartości oraz przeznaczenia. W teorii zarządzania wyróżnia się trzy rodzaje planów:

- plan strategiczny – ogólny plan zawierający decyzje dotyczące alokacji zasobów, priorytetów i działań niezbędnych do osiągnięcia celów strategicznych, zaliczany do planów długookresowych;

– plan taktyczny – plan nakierowany na osiągnięcie celów taktycznych, opracowany dla realizacji elementów planu strategicznego, zaliczany do planów średniookresowych;
– plan operacyjny – plan nastawiony na wykonanie planów taktycznych dla osiągnięcia celów operacyjnych, zaliczany do planów krótkookresowych.

Można dokonać typologii procesu planowania, zarówno jeśli chodzi o:

1) planowanie wojskowe – związane z niszczeniem nieprzyjaciela, jak i
2) planowanie cywilne – które ma za zadanie ratowanie życia, zdrowia ludzi.

W narodowym procesie dowodzenia H. Bieniok [1999, ss. 57–58] wyróżnione zostały cztery fazy:

– ustalenie położenia,
– planowanie,
– stawianie zadań,
– kontrola.

Do zadań planowania cywilnego należy:

1) określenie zagrożeń, jakie mogą wystąpić w obszarze działania;
2) ustalenie środków celem zwalczania zagrożeń:
   – osobowych,
   – sprzętowych,
   – materiałowych;
3) ustalenie zespołów oraz struktur, a co za tym idzie, przygotowanie ich do wykonywania działań ratowniczych;
4) ustalenie zasad współdziałania z:

– przełożonymi (starostwo, województwo, rząd),
– sąsiadami (gminy, powiaty, województwa),
– innymi krajami.

Planowanie podlega także typologii ze względu na kryterium czasu realizacji. Wówczas rozróżniamy:

– planowanie strategiczne – powyżej 5 lat,
– planowanie długoterminowe – od 2 do 5 lat,
– planowanie średnioterminowe – od kilku miesięcy do roku,
– planowanie krótkoterminowe – do trzech miesięcy,
– planowane bieżące – szczegółowe czynności realizowane codziennie lub w skali tygodnia [Sienkiewicz-Małyjurek, Krynojewski 2010, ss. 90–91].

Plan kryzysowy to dokument publiczny, w którym ustala się cele, podaje podstawy prawne oraz określa przyjęte założenia. Plany reagowania kryzysowego powinny być opracowane na wszystkich szczeblach zarządzania. Dzieje się tak dlatego, iż zarządza-

nie kryzysowe stanowi niezbywalny obowiązek władz wszystkich szczebli. Treść planów reagowania kryzysowego określa zadania władz różnych szczebli, które będą realizowane w trakcie reagowania w sytuacji kryzysowej. Warto dodać, cytując za K. Sienkiewicz-Małyjurek i F. Kryjojewskim [2010, ss. 111–112], że powiatowe i gminne plany reagowania kryzysowego powinny koncentrować się na przedsięwzięciach elementarnych dla ochrony ludności. Chodzi głównie o ostrzeganie i informowanie ludności, na przykład o możliwościach i sposobach ewakuacji czy ukrycia ewakuowanych osób.

Powiatowe plany reagowania kryzysowego powinny skoncentrować się także na wykorzystaniu posiadanych sił oraz środków do walki z zagrożeniem. W tym celu należy uwzględnić charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, informacje o infrastrukturze krytycznej oraz mapy ryzyka i mapy zagrożeń. Infrastrukturę tworzą systemy oraz wchodzące w ich skład powiązane ze sobą obiekty, takie jak: obiekty budowlane, urządzenia, instalacje oraz usługi kluczowe dla bezpieczeństwa państwa i jego obywateli czy usługi, które służą zapewnieniu sprawnego funkcjonowania organów oraz instytucji czy przedsiębiorców.

Plan reagowania kryzysowego bezpośrednio służy określeniu zakresu działań przygotowawczych. Od planu zależą także szkolenia i ćwiczenia. Szkolenie daje szanse personelowi i załodze reagowania kryzysowego na zapoznanie się nie tylko z obowiązkami, ale także na zdobycie umiejętności koniecznych do prawidłowego wykonywania przydzielonych zadań. Z drugiej strony, ćwiczenia dają bezpośrednio szanse na sprawdzenie planu oraz procedur reagowania, pozwalają także ocenić same umiejętności załogi i personelu reagowania.

Do zadań i obowiązków uczestników zarządzania kryzysowego zgodnie z Zarządzeniem nr 23 Ministra Administracji i Cyfryzacji z dnia 13 grudnia 2013 roku w sprawie wytycznych do wojewódzkich planów zarządzania kryzysowego zaliczamy siatkę bezpieczeństwa, która jest rozumiana jako zestawienie zagrożeń, jakie są zawarte w katalogu ze wskazaniem wiodącego podmiotu i współpracujących podmiotów wraz z działaniami dotyczącymi danego zagrożenia[2]. Zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych to zestawienie zasobów, które mogą zostać bezpośrednio wykorzystane w określonych przedziałach czasowych w danej sytuacji kryzysowej. Takie zestawienie powinno być przygotowane w postaci stale aktualizowanej bazy danych.

[2] Zarządzenie nr 23 Ministra Administracji i Cyfryzacji z dnia 13 grudnia 2013 r. w sprawie wytycznych do wojewódzkich planów zarządzania kryzysowego. Na podstawie art. 14 ust. 3 Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2013 r., poz. 1166).

W myśl Zarządzenia nr 23 Ministra Administracji i Cyfryzacji z dnia 13 grudnia 2013 r. w sprawie wytycznych do wojewódzkich planów zarządzania kryzysowego „Plan powinien być spójny z rozwiązaniami zawartymi w Krajowym Planie Zarządzania Kryzysowego i obejmować zadania realizowane we wszystkich fazach zarządzania kryzysowego (zapobiegania, przygotowania, reagowania, odbudowy)".
Struktura i treść planu powinny wynikać z zadań, jakie mają być realizowane i celu, jaki ma być osiągnięty. Zadaniem planu jest:

- ujednolicenie zasad prowadzenia działań przez różne rodzaje służb oraz organizacji zarządzania kryzysowego,
- określenie zasad współistnienia różnych szczebli administracyjnych w zależności od zakresu powstałego zagrożenia lub określonej sytuacji kryzysowej,
- określenie niezbędnych dokumentów planistycznych w organach administracji rządowej, zespolonej, specjalnej, samorządowej oraz podmiotów odpowiedzialnych za prowadzenie działań w sytuacjach kryzysowych,
- określenie potencjalnych rodzajów zagrożeń oraz funkcji poszczególnych organów zapewniających właściwe prowadzenie działań, głównie w zakresie odpowiedzialności: łączności, opieki medycznej, zaopatrzenia w wodę, żywność, pomocy społecznej, ewakuacji, transportu, energetyki, alarmowania i ostrzegania, współpracy z mediami, finansowania, porządku publicznego, prawa czy ochrony infrastruktury krytycznej [Grocki 2012, s. 106].

Plan reagowania kryzysowego, opracowany przy wykorzystaniu podejścia funkcyjnego, składa się z:

- planu głównego oraz aneksów funkcyjnych, które zawierają informację dla konkretnych zdarzeń;
- organizacji, którym w planie głównym czy aneksach funkcyjnych przydzielono zadania oraz harmonogramy do wdrożenia planu reagowania kryzysowego.

Plan główny zawiera:

- charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia,
- zadania i obowiązki uczestników zarządzania kryzysowego,
- zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych.

Do planu głównego powinny także powstać załączniki funkcjonalne zawierające określone procedury i wytyczne. W cytowanym wyżej zarządzeniu mowa o:

- procedurach organizacji zadań z zakresu zarządzania kryzysowego;
- organizacji łączności pomiędzy podmiotami realizującymi zadania z zakresu zarządzania kryzysowego;
- organizacji systemu monitorowania zagrożeń, ostrzegania czy alarmowana;
- zasadach informowania ludności o zagrożeniach oraz o sposobach postępowania w wypadku zagrożeń;

- organizacji ewakuacji z obszarów zagrożonych;
- organizacji ratownictwa oraz opieki medycznej czy pomocy społecznej albo pomocy psychologicznej;
- organizacji ratownictwa albo opieki medycznej oraz pomocy społecznej czy pomocy psychologicznej;
- organizacji ochrony przed zagrożeniami, które są charakterystyczne dla obszaru województwa;
- wykazie zawartych umów oraz porozumień bezpośrednio związanych z realizacją zadań, które są zawarte w planie zarządzania kryzysowego;
- zasadach i trybie oceniania oraz dokumentowania szkód;
- procedurach uruchamiania rezerw strategicznych;
- wykazie infrastruktury krytycznej.

Plan reagowania kryzysowego bezpośrednio służy określeniu zakresu działań przygotowawczych. Od planu zależą także szkolenia i ćwiczenia. Szkolenie daje szansę personelowi i załodze reagowania kryzysowego na zapoznanie się nie tylko z obowiązkami, ale także na zdobycie umiejętności koniecznych do prawidłowego wykonywania przydzielonych zadań. Z drugiej strony, ćwiczenia dają bezpośrednio szansę na sprawdzenie planu oraz procedur reagowania. Ćwiczenia pozwalają także na ocenę samych umiejętności załogi i personelu reagowania.

Zakończenie

Procesowe podejście do zarządzania kryzysowego prezentuje Sienkiewicz-Małyjurek [2011, ss. 119–129], podkreślając, że zarzadzanie zawsze powinno być kompleksowe i uwzględniać w ocenie skuteczności działania wszystkie dostępne możliwości, takie jak: dostępność środków, osób, kwalifikacje osób, aktualność danych dotyczących zagrożenia, bieżące działania wpływające pośrednio na poziom bezpieczeństwa i inne. Kluczem do odpowiedniej analizy może stawać się więc regulacja ustawowa, opisująca strategiczne elementy planów kryzysowych i infrastrukturę krytyczną. Procesowość może być więc uwzględniona w działaniach wycinkowych, które jednocześnie mogą obnażać niedoskonałości, braki i problemy w różnych sferach.

Planowanie kryzysowe ułatwia także reagowanie oraz odbudowę krótkookresową. Jeśli plan jest dostatecznie elastyczny i jest szansa na wykorzystanie go w przypadku jakiegokolwiek zagrożenia, to stanowi on bazę dla zarządzania kryzysowego. Dzięki tej bazie społeczność ma szansę kontynuować działania polegające na zapobieganiu długookresowemu, konkretnemu zagrożeniu.

Reasumując, przygotowanie planu dla wszystkich zagrożeń daje szansę rozpoczęcia działań z pozycji względnie bezpiecznej, choć opracowanie dobrego planu zarządzania kryzysowego nie jest przedsięwzięciem łatwym. Podczas opracowania planu napotykamy na wiele trudności związanych nie tylko z organizacją pracy, ale także brakiem niezbędnych informacji, opóźnieniami czasowymi w realizacji zadań członków zespołu.

Współpraca tak różnorodnego zespołu (specjaliści od łączności, opieki medycznej, zaopatrzenia w wodę, żywności, pomocy społecznej, ewakuacji, transportu, energetyki, alarmowania i ostrzegania, współpracy z mediami, finansowania, porządku publicznego, prawa czy ochrony infrastruktury krytycznej) wymaga dobrego przygotowania organizacyjnego, czyli opracowania planu działania i koncepcji planu zawierającego wykaz zagadnień do opracowania oraz sposób ich opracowania. Przed przystąpieniem do realizacji tych działań niezbędna jest ocena własnych zasobów, zarówno ludzkich, jak i materiałowych. Celowe byłoby także określenie jednostki wiodącej, opracowującej plan, określenie jednostek współpracujących, powołanie zespołu planującego oraz stworzenie lokalnej koalicji na rzecz planu.

Bibliografia

Bieniok H. (red.) (1999), *Metody sprawnego działania, Planowanie, Organizowanie, Motywowanie, Kontrola*, Placet, Warszawa.

Charette P., Mitchell A., Mazur S., McSweeney E. (2004), *Zarządzanie projektem. Poradnik dla samorządów terytorialnych*, Program Rozwoju Instytucjonalnego, Kraków.

Daniluk P. (2011/2012), *Myślenie strategiczne w naukach o bezpieczeństwie*, „Rocznik Bezpieczeństwa Międzynarodowego", Dolnośląska Szkoła Wyższa, Wrocław.

Grocki R. (2012), *Zarządzanie kryzysowe. Dobre praktyki*, Difin, Warszawa.

Lewandowski R., Kautsch M., Sułkowski Ł. (2013), *Współczesne problemy zarządzania w ochronie zdrowia z perspektywy systemu i organizacji*, „Przedsiębiorczość i Zarządzanie", t. XIV, z. 10, cz.1, Łódź.

Mikuła B., Pietruszka-Ortyl A., Potocki A. (2002), *Zarządzanie przedsiębiorstwem XXI wieku. Wybrane koncepcje i metody*, Difin, Warszawa.

Naruć W., Nowak J., Wieloch M. (2008), *Operacyjne planowanie finansowe*, CDiI, Difin, Warszawa.

Penc J. (1998), *Zarządzanie dla przyszłości. Twórcze kierowanie firmą*, Profesjonalna Szkoła Biznesu, Kraków.

Sienkiewicz-Małyjurek K, Krynojewski F.R. (2010), *Zarządzanie kryzysowe w administracji publicznej. Zarządzanie bezpieczeństwem*, Difin, Warszawa.

Sienkiewicz-Małyjurek K. (2015), *Skuteczne zarządzanie kryzysowe*, Difin, Warszawa.

Sienkiewicz-Małyjurek K. (2011) *Problemy organizacyjne zarządzania kryzysowego w samorządach*, „Zeszyty Naukowe Politechniki Śląskiej", Katowice.

Sobolewski G. (red.) (2011), *Zagrożenia kryzysowe*, Akademia Obrony Narodowej, Warszawa.

Szczupaczyński J. (2012), *Anatomia zarządzania organizacją*, Międzynarodowa Szkoła Menedżerów, Warszawa.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 późn. zm.).

Walas-Trębacz J., Ziarko J. (2010), *Podstawy zarządzania kryzysowego*, Cz. 1: *Zarządzanie kryzysowe w administracji publicznej*, Oficyna Wydawnicza AFM, Kraków.

Więcek W., Bieniek J. (2014), *Podstawy zarządzania kryzysowego i scenariusze ćwiczeń,* Akademia Obrony Narodowej, Warszawa.

Zarządzenie nr 23 Ministra Administracji i Cyfryzacji z dnia 13 grudnia 2013 r. w sprawie wytycznych do wojewódzkich planów zarządzania kryzysowego.

Zarządzenie nr 86 Prezesa Rady Ministrów z dnia 14 sierpnia 2008 r. w sprawie organizacji i trybu pracy Rządowego Zespołu Zarządzania Kryzysowego (Dz. U. Nr 61, poz. 538).

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **23–38**

Jan Zych[1]
Wydział Nauk Społecznych, Uniwersytet im. Jana Kochanowskiego w Kielcach

Umieć odróżniać tropy obiecujące, interesujące wyniki dociekań od tych nieistotnych
– to również sztuka uprawiania nauki
[parafraza myśli zaczerpniętej z: Beveridge 1960, s. 56].

Rozszerzona rzeczywistość w ratownictwie i zarządzaniu kryzysowym

Augmented Reality in Emergency and Crisis Management

Abstract: The discourse presented in the article refers to a new technology implemented in the field of security. The subject of AR – Augmented Reality is highlighted. The consequence of this technology revolutionizes educational processes, changes management models, modifies social communication. This article presents Augmented Reality based computer applications. The context in which the author's research on the expanded reality is presented the improvement of communication processes for saving lives, health, property and the environment.
Key words: augmented reality, visualization systems, Layar, Junairo, Legion.

Wstęp

Służby odpowiedzialne za ratowanie życia, zdrowia, mienia i środowiska [Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2007 Nr 89 poz. 590 z późn. zm.] w miarę rozwoju teleinformatyki coraz częściej zobligowane są do dokonywania wyborów związanych z adaptacją do swojej pracy jeszcze niedostatecznie przetestowanych aplikacji komputerowych. Eksperci dziedzinowi z obszaru Commu-

[1] cyberman.com.pl

nications and Information Technology [Amanowicz, Dąbrowski, Suchański, Gajewski, Hołubowicz, Zych, Flizikowski] są zgodni w opinii, iż adaptacja tych nowych rozwiązań, zorientowanych na wsparcie procesów informacyjno-analityczno-decyzyjnych, nie jest już opcją – a nieuniknioną koniecznością. Część z tych technologii ewidentnie wnosi wartość dodaną do usprawnienia czy wręcz optymalizacji tych procesów, przez co istotnie przyczynia się do zwiększenia poziomu bezpieczeństwa. Istnieje wiele nowatorskich pomysłów, które wymagają jeszcze wielu udoskonaleń przed wdrożeniem. Technologią względnie mało znaną, w której upatruje się istotnego skoku jakościowego w obszarze bezpieczeństwa, jest tzw. *rozszerzona rzeczywistość*.

Terminologia stosowana w publikacjach naukowych, dotycząca rozszerzonej rzeczywistości (w skrócie „RR"), to kalka terminu angielskiego: *augmented reality* (w skrócie „AR"). Idea działania urządzenia wykorzystującego RR polega na generowaniu, cyfrowej wersji obrazu świata naturalnego, wraz z naniesionymi na obraz dodatkowymi elementami graficznymi i tekstowymi, poszerzającymi wiedzę, uszczegóławiającymi informację, geotagującymi obiekt znajdujący się na ekranie urządzenia.

W artykule zaprezentowano aplikacje komputerowe klasy RR. Kontekst, w jakim prezentowane są dociekania autora na temat rozszerzonej rzeczywistości, to **usprawnienie procesów komunikacyjnych dla ratowania życia, zdrowia, mienia i środowiska**.

Wybitny naukowiec, filozof nauki, Sir Karl Rajmund Popper twierdził, że przyszłości nie da się precyzyjnie przewidzieć, ponieważ żadnymi racjonalnymi i naukowymi metodami nie da się przewidzieć przyszłego rozwoju wiedzy [Popper 1984, ss. 14–28]. Możemy jednak diagnozować wydarzenia, procesy oraz technologie, które pozwalają wnikliwemu obserwatorowi i analitykowi trafnie zidentyfikować trend rozwojowy w krótkim horyzoncie czasowym.

Dyskurs prezentowany w artykule odwołuje się do nowych technologii implementowanych w obszarze bezpieczeństwa powszechnego. W ostatnich kilku latach, w tym kontekście pojawiły się dwa istotne i względnie dojrzałe rozwiązania technologiczne, zwane wirtualną rzeczywistością (ang. Virtual Reality, w skrócie „VR") i wspomniana już rzeczywistość rozszerzona RR, które rewolucjonizują procesy edukacyjne, zmieniają modele zarządzania, modyfikują komunikację społeczną, wpływają istotnie na skuteczność i jakość działania służb. O ile problematyka VR przebiła się do świadomości społecznej i pojawia się dość często w dyskursie naukowym, to AR stanowi ciągle niszę wiedzową. Artykuł jest próbą zapełnienia tej niszy.

Problem naukowy, stanowiący oś narracji, zawarto w ogólnym pytaniu: Czy, a jeśli tak, to w jakim zakresie, rozszerzona rzeczywistość podnosi poziom bezpieczeństwa? Tak postawiony problem naukowy koncentruje rozważania na identyfikacji mechani-

zmów RR poszerzających świadomość sytuacyjną uczestników przedsięwzięć dotyczących ratowania życia, zdrowia, mienia i środowiska [Zych 2017, ss. 224–242].

Sytuacja problemowa

Refleksja nad implikacjami wdrażania technologii RR w obszar bezpieczeństwa wymaga sformułowania kilku trudnych pytań oraz podejmowania prób odpowiedzi na te pytania. W jakim zakresie nowinki technologiczne, takie jak rozszerzona rzeczywistość, przerodzą się w powszechnie użytkowane technologie, istotnie wspomagające procesy informacyjno-analityczno-decyzyjne dla zwiększenia bezpieczeństwa obywateli? Czy rozszerzona rzeczywistość stanie się Świętym Graalem, pozwalającym przezwyciężyć kolejne bariery percepcji świata, który nas otacza i przenieść na wyższy, lepszy poziom radzenia sobie w sytuacjach zagrożenia? Czy ta nowa technologia pozwoli lepiej, szybciej i dokładniej identyfikować zagrożenia? Jak zrealizować tzw. *business intelligence*, czyli wdrożenie rozszerzonej rzeczywistości, aby kreować wyższy i lepszy poziom bezpieczeństwa? Jakie zmiany w komunikacji społecznej służb wymusza ta technologia? Oczywiście lista pytań jest otwarta. Co więcej – wraz ze wzrostem aspiracji naukowych, prowadzenia coraz bardziej zaawansowanych dociekań, liczba trudnych pytań wciąż się powiększa.

W kontekście prowadzonego wywodu, autor utożsamia się z poglądami, jakie poczynił William Gibson. Uważana aktualnie za kultową pozycja, „Neuromancer" W. Gibsona, w latach 80. klasyfikowana była jako literatura science fiction. Gibson opisał tam elementy cyberprzestrzeni i wirtualnej rzeczywistości w środowiskach wytwarzanych przez komputery o dużych mocach obliczeniowych [Gibson 1992, ss. 9–44]. Wydaje się, że mimo upływu lat spostrzeżenia Gibsona na temat rozszerzonej rzeczywistości są ciągle aktualne w odniesieniu do obszaru technologii teleinformatycznych – ICT (akronim od ang. *Information and Communication Technologies*). Termin ten obejmuje szeroki zakres wszystkich technologii umożliwiających gromadzenie, przetwarzanie i wizualizację informacji. Autor, analizując współczesne możliwości technologiczne, zgadza się z Gibsonem, że zdecydowana większość, (jeśli nie wszystkie) przełomowych innowacji technicznych, jakie wejdą w życie w ciągu najbliższej dekady, już potencjalnie istnieje.

Procesy informacyjne oraz analityczno-decyzyjne stanowią największą nadzieję dla adaptacji rzeczywistości rozszerzonej w ratownictwie i zarządzaniu kryzysowym. Próby adaptacji rzeczywistości rozszerzonej do sfery operacyjnego działania służb to względnie nowatorska inicjatywa w obszarze badań naukowych, w szczególności w dyscyplinie: nauki o bezpieczeństwie. Znaczenie ma również fakt, iż moce oblicze-

niowe współczesnych komputerów pozwalają na uzyskanie w czasie rzeczywistym wysokiej rozdzielczości realistycznych scen, atrakcyjnych grafik, wielosensorycznej interakcji użytkownika z komputerem.

Należy też odnotować fakt ciągle rosnących potrzeb szkolenia operacyjnego osób biorących udział w akcjach ratunkowych. Problem doposażenia w nowe technologie dotyczy zarówno ratowników zaangażowanych operacyjnie na miejscu zdarzenia, menedżerów bezpieczeństwa koordynujących lub kierujących tego typu akcjami, jak i obywateli, którzy zupełnie przypadkowo stali się uczestnikami lub świadkami akcji ratunkowych. Adaptacja innowacji technologicznych jest uzasadniona i pożądana w różnych sytuacjach działania służb. Na przykład podejmuje się próby wdrożenia systemów wspierania analiz, decyzji i interaktywnego szkolenia zespołów ratowniczych na bazie standardowych urządzeń mobilnych, takich jak smartfony, iPady czy smartwatche.

Wśród ekspertów dziedzinowych panuje również zgoda co do opinii diagnostycznej, iż centra analityczno-decyzyjne poszukują nowoczesnych systemów wsparcia wykorzystujących powszechnie użytkowane urządzenia mobilne, postrzegane jako dodatkowe urządzenia nadawczo-odbiorcze. Pozytywnym trendem implementacji nowoczesnych technologii w tę sferę działań ratowniczych są systemy wizualizacji w czasie rzeczywistym, bazujące na mechanizmach rozszerzonej rzeczywistości (rysunek 1, 2 i 3).

Rysunek 1. Elementy rozszerzonej rzeczywistości na ekranie smartfona – wariant z napisami

Źródło: https://pl.pinterest.com/pin/517843657144123651/?lp=true, dostęp: 07.07.2017.

Rysunek 2. Elementy rozszerzonej rzeczywistości na ekranie smartfona – wariant z ikonami i napisami

Źródło: https://www.linkedin.com/pulse/bim-ar-wearable-technology-ricardo-khan, dostęp: 07.07.2017.

Rysunek 3. Elementy rozszerzonej rzeczywistości na ekranie iPada, z zaznaczonymi strefami oraz pojazdami straży pożarnej, karetkami pogotowia ratunkowego i patrolami policyjnymi

Źródło: Zrzut z ekranu z aplikacji LEGION.

Wspólny Obraz Operacyjny (ang. COP – Common Operational Picture) jest współdzielony między dotykową tablicą cyfrową w centrum analityczno-decyzyjnym a sensorami, urządzeniami mobilnymi w terenie, w miejscu prowadzenia akcji i uzupełniany w czasie rzeczywistym w dodatkowe informacje o obiektach szczególnych. Sztandarowym przypadkiem tego typu implementacji jest wykorzystywanie specjalistycznych aplikacji instalowanych na przykład na smatfonach i iPadach jako platformy wizualizacji rozszerzonej rzeczywistości do wspierania akcji ratunkowych (rysunek 3).

Przykładowe aplikacje klasy rozszerzona rzeczywistość – RR

Nowoczesne, a nawet awangardowe rozwiązania teleinformatyczne mogą być wykorzystywane w akcjach ratunkowych. Do najbardziej znanych aplikacji z zaimplementowanymi funkcjami rozszerzonej rzeczywistości należy zaliczyć:

- Layar;
- Junairo;
- Teodolit Droid;
- Libre Geo Social;
- Wikitude API;
- Kooaba;
- Sekai Camera;
- Legion.

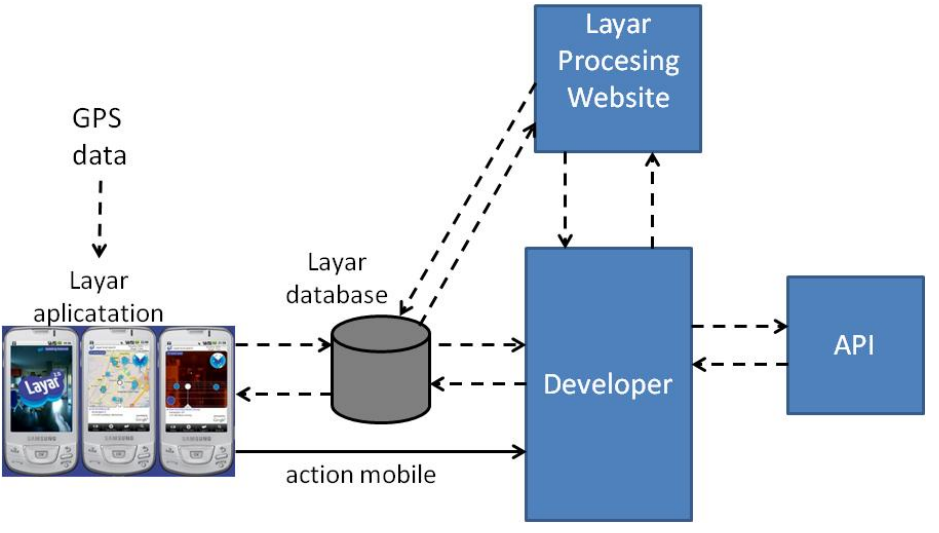
Każdy z tych programów komputerowych korzysta z podobnych platform i funkcjonalności: kamery, kompasu, połączenia internetowego, akcelerometru, visualizera oraz żyroskopu. Owe akcesoria są standardowym wyposażeniem urządzeń mobilnych. Najbardziej znaną aplikacją klasy RR jest program Layar, który przez niecałą dekadę zdobył ogromne powodzenie na świecie, w Europie, w tym również w Polsce.

Layar

Layar jest aplikacją rzeczywistości rozszerzonej, która powstała w Holandii w 2009 roku, dzięki firmie SPRX Mobile. Aplikacja ta ma dobrą opinię na rynku elektronicznym, posiada znacząco więcej zalet, w stosunku do innych programów komputerowych tej klasy.

Celem producenta było dostarczenie wysokiej jakości usług rzeczywistości rozszerzonej. Początkowo aplikacja była do kupienia tylko w Holandii, lecz z czasem jej zasięg systematycznie wzrastał. Layar funkcjonuje przede wszystkim na mobilnych platformach typu smartfon i tablet. W rozwój aplikacji Layar zaangażowanych jest liczny zespół programistów z różnych stron świata, co istotnie wpływa na umiędzynarodowienie produktu.

Rysunek 4. Zasadnicze elementy architektury systemu Layar



Źródło: opracowanie własne na podstawie https://www.fastcodesign.com/1305986/layar-opens-api-to-developers-what-augmented-reality-apps-do-you-want, dostęp: 07.07.2017.

Program wspomagany jest sygnałami synchronizującymi GPS. Do stabilnej pracy aplikacja Layar potrzebuje połączeń internetowych, minimum w technologii 2G. Technologia 2G to telefonia bezprzewodowa, określana jako telefonia drugiej generacji, bazująca na sieci cyfrowej. Technologia 2G zapewnia przesyłanie dźwięku cyfrowego podczas prowadzenia rozmów po łączach telefonicznych oraz wiadomości tekstowych SMS. Technologią bezpośrednio poprzedzającą 2G była technologia analogowa 1G. Layar jest połączony z akcelerometrem oraz żyroskopem (urządzeniem do pomiaru lub utrzymywania położenia kątowego). Obecnie Layar może być instalowany na większości tego typu urządzeń mobilnych, ponieważ wszystkie smartfony i iPady spełniają wymagania systemowe (Android, Symian, BadaOS, IOS, RIM) [Rawski, Szadura, Laskowski 2012, s. 76].

Po uruchomieniu aplikacji Layar zostaje włączona kamera, dzięki której na wyświetlaczu pojawia się obraz z kamery, z otaczającego użytkownika miejsca. Następnie zostaje nałożona na taki obraz siatka z danymi, które uzupełniają informacje na obrazie z kamery, na przykład wyświetlane są: przeznaczenie budynku, terminy i godziny otwarcia, kierunki ewakuacji w sytuacji zagrożenia, punkty z pomocą medyczną. Wiadomości te zostają przedstawione na wyświetlaczu urządzenia mobilnego. W przypadku zidentyfikowania poszkodowanego użytkownik ma wskazane miejsca pomocy medycznej. Layar systematycznie się rozwija, liczba i różnorodność tematyczna

warstw informacyjnych stale się zwiększa. W standardzie jest opis danego miejsca, dokładna mapa ze współrzędnymi, animacje ze sposobami udzielania pierwszej pomocy, zdjęcia oraz linki do stron internetowych – w jeszcze większym stopniu poszerzających informacje o danym obiekcie. Należy zaznaczyć, że wszystkie warstwy informacyjne są precyzyjnie połączone i zsynchronizowane bez opóźnień, dzięki czemu w przyjazny i intuicyjny sposób można uzyskać te najbardziej potrzebne w sytuacji zagrożenia. Jest to konsekwencja precyzyjnego powiązania obiektów wg koordynat geograficznych z sygnałami synchronizującymi dane zaczerpnięte z baz tematycznych. Jeżeli użytkownik zechce wizualizować na wyświetlaczu urządzenia podkłady mapowe wraz z informacjami uszczegóławiającymi, zaznacza to miejsce poprzez dotknięcie określonego miejsca na ekranie, w wyniku czego otrzymuje natychmiast zwrotnie, informacje naniesione na mapę o drogach dojazdowych, a także punktach szczególnych, takich jak: posterunek policji, punkty medyczne, punkty informacyjne. Aktualna wersja tej aplikacji (lipiec 2017), mimo względnie dużego transferu danych działa stabilnie w czasie rzeczywistym [http://www.slideshare.net/layarmobile/layar-november-5-webinar-discover-the-new-geo-sdk, dostęp: 07.07.2017].

Wikitude

Aplikację Wikitude opracowano w firmie Mobilizy. Za pomocą tego programu można połączyć obraz rzeczywisty oraz wirtualny na jednym wyświetlaczu. Na przykład możemy zobaczyć miejsce stacjonowania Jednostek Ratowniczo-Gaśniczych, a także uzyskać podstawowe informacje na temat wybranego obiektu. Celem twórców Wikitude było dostarczenie odpowiednich informacji przede wszystkim pracodawcom, a także udrożnienie współpracy na styku B2B [B2B – ang. *business-to-business* – przypis autora], B2C [B2C – ang. *business-to-consumer* – przypis autora]. Program dostarcza informacji na temat poszczególnych obiektów, ulic, dzielnic, miast, państw itp. Wiadomości, które są dostarczane odbiorcy, pochodzą z ponad 3 500 źródeł, takich jak Wikipedia, YouTube, Wheelmap [http://aplikacje.orange.pl/cid,66,id,2770,nazwa,Wikitude,plid,81,prid,3842,opis-aplikacji.html?smzbovyrznexrgbenatrticaid=614cc2, dostęp 07.07.2017].

Aplikacja jest mało popularna w Polsce, skutkuje to małą ilością dostarczanych informacji na temat organizacji imprez masowych. Twórcy aplikacji, aby zapobiec przeciążeniu kanałów informacyjnych, wprowadzili limity uzyskania wyników otrzymywanych wiadomości (obecnie można uzyskać nie więcej niż 70). Resumując, program ten jest ciekawą inicjatywą na rynku elektronicznym, lecz nie stanowi istotnej konkurencji dla aplikacji Layar [http://pej.cz/Aplikacja-Wikitude-zobacz-co-sie-dzieje-naokolo-a2495, dostęp: 07.07.2017].

Rysunek 5. Interfejs aplikacji Wikitude

Źródło: http://www.talkandroidphones.com/wp-content/uploads/2011/05/LG-Wikitude-3D-Augmented-Reality.jpg, dostęp: 07.07.2017.

Teodolit Droid

Cechą charakterystyczną aplikacji Teodolit Droid jest podobieństwo do narzędzi geodezyjnych i meteorologicznych. Tak jak we wcześniejszych aplikacjach program ten można użytkować na smartfonach, tabletach i innych urządzeniach mobilnych.

Rysunek 6. Interfejs aplikacji Teodolit Droid

Źródło: https://www.pinterest.co.uk/dev2448/augmented-reality/?lp=true, dostęp: 08.07.2017.

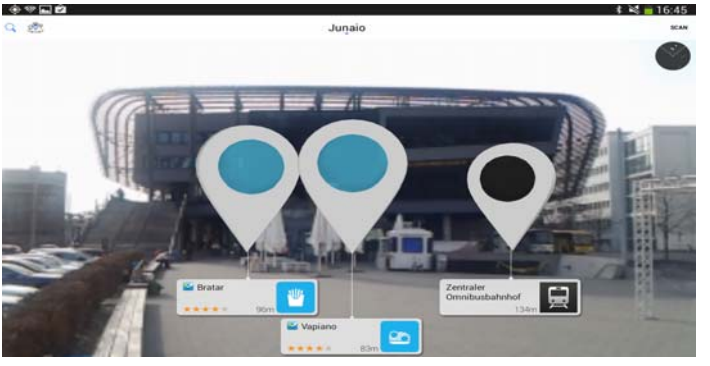
Dzięki tej aplikacji uzyskujemy bardzo precyzyjne informacje na temat długości i szerokości geograficznej miejsca, w którym się znajdujemy, wysokości względem poziomu morza, daty, godziny, kierunku geograficznego. W przeciwieństwie do Layar i Wikitude aplikacja ta skierowana jest głównie do geologów, archeologów, inżynierów, geodetów i innych powiązanych tematycznie specjalistów. W gronie klientów, którzy korzystają z tego programu, znajdują się także turyści, sportowcy oraz służby zarządzania kryzysowego.

Dużą zaletą aplikacji jest oddzielenie informacji bazowych o aktualnym położeniu użytkownika aplikacji od informacji z różnych serwisów społecznościowych typu: Facebook, Twetter, LinkedIn, YouTube, Google+, Instagram, Snapchat. Cechą pozytywnie wyróżniającą tę aplikację jest także brak możliwości dystrybuowania informacji komercyjnych i reklamowych. Niestety nie ma możliwości uzyskania informacji na temat osób znajdujących się w danym obszarze (dzielnica, obiekt sportowy) [https://play.google.com/store/apps/details?id=com.shopzeus.android.majorforms_1012, dostęp: 08.07.2017].

Junaio

Junaio jest jedną z największych, najpopularniejszych aplikacji rzeczywistości rozszerzonej wykorzystywanej dla celów komercyjnych, lecz zawierającej informacje tylko śladowo przydatne z punktu widzenia bezpieczeństwa. Dzięki tej aplikacji możemy uzyskać informację na temat miejsc użyteczności publicznej i charakteru wydarzeń mających tam miejsce: restauracji, wydarzeń sportowych, zniżek na bilety, punktów medycznych, miejsc, gdzie można uzyskać pomoc w razie wypadku. Poza tym Junaio rozpoznaje zdjęcia, reklamy, opakowania produktów. Czyta i interpretuje kody paskowe oraz kody QR. Aplikacja zapewnia włączenie kamery zamontowanej w urządzeniu mobilnym, co daje możliwość uzyskania informacji na temat obiektu znajdującego się pod danym adresem. Zaletą aplikacji jest dostarczenie wskazówek na temat dojazdu na miejsce wydarzenia, specjalnych ofert skierowanych dla konsumentów, warunków bezpieczeństwa i procedur postępowania w przypadku zaistnienia zagrożenia. Wadą programu jest brak szczegółowych informacji dotyczących bezpośredniego obszaru przylegającego do obiektu wizualizowanego na wyświetlaczu. Aplikacja skierowana jest do użytkownika, zorientowanego przede wszystkim na rozrywkę. Warstwa informacyjna na temat bezpieczeństwa jest reprezentowana tylko śladowo. Junaio nie cieszy się dużą popularnością na polskim rynku, brakuje spolszczenia menu, a także informacji w języku polskim [http://mobilemarketing.pl/reklama-sieci-restauracji-sausalitos-z-wykorzystaniem-aplikacji-junaio-oraz-augmented-reality, dostęp: 8.07.2017].

Rysunek 7. Interfejs aplikacji Junaio



Źródło: http://www.1mobile.com/junaio-augmented-reality-72709.html, dostęp: 08.07.2017.

Rozszerzona rzeczywistość w praktyce zarządzania kryzysowego

Autor zidentyfikował dychotomiczny podział w zbiorze publikacji naukowych na temat rozszerzonej rzeczywistości. Otóż w obszarze zarządzania kryzysowego, publikacje sytuowane są w zasadzie w dwóch kategoriach: systemach wspomagania decyzji (DSS – Decision Support System) lub opisie interfejsów tych urządzeń z użytkownikami. Wielu z tych użytkowników jest już zaznajomiona z oferowanymi im możliwościami technologicznymi rozszerzonej rzeczywistości i entuzjastycznie podchodzi do wprzęgnięcia tych technologii w praktykę.

Rysunek 8. Interfejs wyświetlający koordynaty, dane pogodowe w danym miejscu oraz odległości do najbliższej komendy policji i punktu medycznego

Źródło: opracowanie własne, zrzut z ekranu z iPada.

RR, bazując na idei bardziej efektywnego niż dotychczas oddziaływania na zmysły odbiorcy, zapewnia lepsze oddanie realizmu sytuacji oraz dążenie do maksymalnego efektu imersji w świat kreowany za pomocą technologii informatycznych, w tym poprzez efekty multimedialne. Aktualnie najintensywniej wykorzystywane są w tym celu dwa zmysły człowieka: wzrok i słuch, ale prace B+R sięgają coraz śmielej po pozostałe zmysły (dotyk, smak i węch).

Należy zdać sobie sprawę, że w naukach o bezpieczeństwie, badania o charakterze czysto poznawczym i badania praktyczne dzieli czasami bardzo subtelna granica. Kilka podstawowych odkryć, takich jak nowe struktury węglowe: fulereny [fulereny – cząsteczki składające się z parzystej liczby atomów węgla, tworzące zamkniętą, pustą w środku bryłę - przypis autora] i grafen [grafen – płaska struktura złożona z atomów węgla, połączonych w sześciokąty – przypis autora], otworzyło niezwykłe możliwości przed rozwojem technologii RR. Postęp w badaniach nad mózgiem, zarówno w wymiarze czysto poznawczym, jak i rozwoju technik badawczych, doprowadził do niezwykłych rozwiązań technicznych, jak możliwość sterowania funkcjami urządzeń elektronicznych za pomocą fal mózgowych. Jeśli potraktować dosłownie opinię Poppera, jak to często czynią sceptycy – to wówczas należałoby uznać, że takie przedsięwzięcie, jak wskazywanie wiodących technologii przyszłości nie ma sensu. Perspektywa Gibsona z kolei pokazuje, że wprost przeciwnie, istnieje głęboki sens poszukiwania przyszłości w teraźniejszości, a od filozoficznych refleksji nie mniej ważna jest operacjonalizacja zaawansowanych idei w praktyce.

Jak wynika z zaprezentowanych analiz kilku sztandarowych aplikacji klasy RR – niektóre z nich są już odpowiednio przetestowane, zebrane są spostrzeżenia odnośnie ich funkcjonowania, wypracowywane są wnioski i rekomendacje mające na celu skonstruowanie kolejnych jeszcze bardziej zaawansowanych wersji tych urządzeń. Istnieją jednak rozwiązania, które znajdują się dopiero w fazie zalążkowej, w fazie krystalizowania się wersji docelowych, dopiero dojrzewających w głowach wynalazców. Jedne i drugie wymagają konsekwentnego monitorowania.

Rozszerzona rzeczywistość wizualizowana na wyświetlaczach urządzeń mobilnych to szczególny przypadek implementacji technologii HUD (ang. *Head-Up Display*). [Implementacja technologii HUD oznacza zastosowanie wyświetlacza przeziernego, który prezentuje dodatkowe informacje na specjalnie przystosowanej do tego powierzchni, przypis autora].

Powstało już wiele symulatorów z elementami rozszerzonej rzeczywistości, mogą być one wykorzystane do podniesienia umiejętności analityczno-decyzyjnych w ratowaniu życia, zdrowia, mienia i środowiska. Rozwój tej kategorii produktów na świecie jest wręcz spektakularny. Poniżej tylko zasygnalizowano istnienie oprogramowania symulacyjnego tej klasy.

Rysunek 9. Przykłady interfejsów typu HUD

Źródło: https://www.google.pl/search?biw=wywietlacz+typu+HUD oraz http://www.armia24.pl/technologie/2718-systemy-rozszerzonej-rzeczywistosci-bae-systems-rewolucja-na-polu-bitwy, dostęp: 09.07.2017.

System CRIMSON opracowany przy wsparciu Komisji Europejskiej łączy symulacje i technologię AR w celu symulacji złożonych scenariuszy kryzysowych i awaryjnych, które są trudne do odtworzenia i potwierdzenia w realnych warunkach [Balet, Duysens, Compdaer et al. 2012, s. 44]. System CRIMSON został przyjęty przez przemysł i wojsko. Inny produkt promuje Akademia Akcji – oferuje ponad 16 godzin praktycznego szkolenia dotyczącego różnego rodzaju zagrożeń, np.: zagrożenia chemicznego, biologicznego, radiologicznego, jądrowego i wybuchowego. Zajęcia szkoleniowe zawierają wiele symulacji w stylu gier wideo, które zanurzają gracza w praktyczne problemy decyzyjne. Opracowana przez Public Health Games z University of Illinois

w Chicago, sieciowa, wieloosobowa symulacja, która łączy technologię gier wideo z elementami rozszerzonej rzeczywistości w celu wyszkolenia osób do odpowiedniego reagowania na zagrożenia związane z substancjami chemicznymi i materiałami niebezpiecznymi. Główny cel tych symulacji to poprawienie komunikacji, obserwacji i podejmowania optymalnych decyzji. Instruktor tworzy hipotetyczny scenariusz z wybranym rodzajem zagrożenia (np. wyciek amoniaku), symuluje skutki (objawy), jakie wywołuje ten środek chemiczny, w określonych warunkach pogodowych. Szkoleni przyjmują rolę koordynatora akcji i uczą się organizowania strefy odkażania. Warstwa RR w tym symulatorze daje dodatkowe informacje zmniejszające poziom entropii przy podejmowaniu decyzji, np. zapewniając informacje potrzebne do rozdysponowania sił i środków do konkretnego wypadku. Pozostali szkoleni komunikują się poprzez radio i odpowiednio reagują na sytuacje przygotowane w scenariuszu.

Jeszcze inne rozwiązanie promuje (ECASC, Francja). To również oprogramowanie, które poprzez rzeczywistość rozszerzoną uczy reagowania na sytuacje zagrożenia mogące wystąpić w środowisku miejskim. Celem kreowania tego typu sytuacji jest zapewnienie szkolonym możliwości wpływania na rozwój sytuacji poprzez podejmowanie decyzji w warunkach zagrożenia życia i zdrowia oraz poprzez dokładne odtworzenie kontekstu operacyjnego, poprzez realistyczną wizualizację wydarzeń.

W procesie ratowania ludzkiego życia i zdrowia pojawiają się liczne dylematy dotyczące wykorzystania nowych technologii. Adaptacja tych nowych technologii w obszar zarządzania kryzysowego zazwyczaj ma podłoże komercyjne. Analizując chociażby wspomniane aplikacje klasy RR pod względem ich przydatności dla akcji ratowniczych, wyraźnie eksponowane są funkcjonalności, które pomagają w skróceniu procesu decyzyjnego, przyspieszeniu identyfikacji danego zagrożenia, a także dostarczeniu niezbędnych informacji dla zarządzających akcją [Zych 2013, ss. 71–84]. Producenci dość konsekwentnie pomijają aspekt biznesowy. W każdym zdarzeniu kryzysowym, obsługiwanym przez system z rozszerzoną rzeczywistością, zazwyczaj uwydatnia się oczywisty konflikt pomiędzy oczekiwaniami służb zarządzania kryzysowego a funkcjonalnościami, jakie zapewniają te systemy. Oczywiście wymaga to rozstrzygnięcia dylematu, czy konstruktorzy i dostawcy nowych technologii rozszerzonej rzeczywistości, a nawet sami operatorzy telekomunikacyjni mają wprowadzać nowsze rozwiązania tylko jako potencjalną opcję dodatkową (płatną extra), czy też powinni wprowadzać zmiany, nawet gdyby wiązały się z dodatkowymi inwestycjami uznawanymi za konieczne, a generującymi zyski w odległym horyzoncie czasowym. Problem na dzień dzisiejszy pozornie jest nieusuwalny, gdyż publiczne systemy teleinformatyczne niezbędne do właściwego działania aplikacji klasy augmented reality są zestawiane dla potrzeb i specyfiki użytkowników środnio obciążających sieci telekomunikacyjne (bo takie rozwiązania generują największe zyski operatom). Odpowiednio są

optymalizowane pod względem: pokrycia sygnałem danego terenu, jego pojemności dotyczącej przechowywania danych multimedialnych, prędkości transmisji, szybkości połączeń, stabilności działania. A przecież potrzeby służb zarządzania kryzysowego, tam gdzie istnieje zagrożenie życia i zdrowia, szczególnie w fazie reagowania, są skrajnie inne niż te stawiane standardowym systemom teleinformatycznym [więcej w: Flizikowski, Zych 2016, ss. 201–216].

Jaka zatem przyszłość czeka aplikacje klasy RR implementowane w zarządzaniu kryzysowym? W opinii autora, ta nowa technologia nie ma już statusu *in statu nascendi*, ma natomiast potencjał, który nie jest aktualnie wykorzystywany dla bezpieczeństwa. Można ostrożnie prognozować, że sytuacja ulegnie szybkiej zmianie na lepsze, bo rozwoju tak atrakcyjnej dla użytkownika końcowego technologii nie da się zatrzymać.

Podsumowanie

W ratowaniu życia, zdrowia, mienia i środowiska pojawiają się liczne dylematy dotyczące wykorzystania nowych technologii. Analizując aplikacje klasy RR pod względem ich przydatności dla akcji ratowniczych, ewidentnie dostrzegalne są funkcjonalności, które pomogą w skróceniu procesu decyzyjnego, przyspieszeniu oceny danego zagrożenia, a także dostarczeniu niezbędnych informacji dla koordynatorów tych akcji.
Dziś urządzenia mobilne, takie jak smartfony i iPady to jedne z najpopularniejszych urządzeń elektroniki użytkowej, wykraczające poza tradycyjne funkcje telefonu, zapewniające już dziś stały dostęp do mediów społecznościowych, aktualnych wiadomości i wielu innych źródeł informacji. Odpowiednia konwergencja różnych, do tej pory nie skorelowanych ze sobą informacji z różnych baz danych, odpowiednio wizualizowana za pomocą rozszerzonej rzeczywistości, wniesie nową jakość w ratowaniu życia, zdrowia, mienia i środowiska.

Jednak wątpliwości i pytań w tej kwestii jest ciągle wiele. Czy aplikacje klasy RR poradzą sobie z dokładnym wskazaniem współrzędnych geograficznych w dużej dynamice? Czy synchronizacja informacji z baz danych na wielu urządzeniach mobilnych, zmuszonych do współpracy, będzie możliwa w czasie rzeczywistym? Czy urządzenia te będą odporne na ataki hakerów? Czy możliwe będzie na odległość dokładne określanie poziomów ryzyka dla użytkownika? Czy usprawniając proces decyzyjny go nie zakłócą? Czy wdrożenia wspomnianej technologii nie wygenerują zbyt dużych kosztów?

Autor postuluje kontynuowanie badań nad aplikacjami klasy AR, w tym specjalistycznych ekspertyz w zakresie użyteczności omawianych technologii w akcjach ra-

towniczych. Ponadto, koniecznością jest preparacja ćwiczeń w formule symulacji i gier bazujących na scenariuszach zdarzeń o charakterze kryzysowym, jak również szkoleń dotyczących wykorzystania technologii RR.

Bibliografia

Beveridge W.I.B. (1960), *Sztuka badań naukowych*, PZWL, Warszawa.

Balet O., Duysens J., Compdaer J., Gobbetti E., Scopigno R. (2012), *The Crimson Project. Simulating populations in massive urban environments*, World Congress on Computational Mechanics, Vancouver, Canada.

Flizikowski A., Zych J. (2016), *Sieci WiMAX w zarządzaniu kryzysowym,* [w:] O. Oszowska, S. Mikołajczak, K. Rokiciński (red.), *Paradygmaty badań nad bezpieczeństwem. Bezpieczeństwo na początku XXI wieku – wyzwania, szanse i zagrożenia*, WSB, Poznań.

Gibson W. (1992), *Neuromancer*, Fenix Publication, Szczecin.

Popper K.R. (1984), *Nędza historycyzmu*, Wydawnictwo Krąg, Warszawa.

Rawski D., Szadura P., Laskowski M. (2012), *Layar – wirtualna rzeczywistość drogą do stworzenia inteligentnego miasta*, Zeszyty Naukowe Uniwersytetu Szczecińskiego NR 721, Studia Informatica nr 29*,* Wydawnictwo Naukowe Uniwersytetu Szczecińskiego, Szczecin.

Ustawa o zarządzaniu kryzysowym z 26 kwietnia 2007 r. Dz.U. 2007 Nr 89 poz. 590 z późniejszymi zmianami.

Zych J. (2013), *Gry decyzyjne dla kształtowania kompetencji kadr menedżerskich zarządzania kryzysowego*. Akademia Marynarki Wojennej, Gdynia.

Zych J. (2017), *Świadomość sytuacyjna w wojnie hybrydowej na Ukrainie,* [w:] . B. Pacek, J.A. Grochocka (red.), *Wojna hybrydowa na Ukrainie. Wnioski i rekomendacje dla Europy i świata*, Wydawnictwo Jana Kochanowskiego w Kielcach, Filia w Piotrkowie Trybunalskim, Piotrków Trybunalski.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **39–52**

Radosław Harabin[1]
Społeczna Akademia Nauk

Organizacja i funkcjonowanie Wojewódzkiego Centrum Zarządzania Kryzysowego w Kielcach

Organizational Structure and Coverage of the County Crisis Management Center in Kielce

Abstract: The article was written on the basis of the interviews with County Crisis Management Center's head director, literature and documents received in the Department. Those are the main but not only research sources. Outcomes are presented in twofold order. The paper starts with descriptions of the center's organizational structure: its organizational principles and accoutrements. Further on the center's director and officer's on duty coverages are presented. The author tries to combine theoretical knowledge drawn from documents with practical experience of interviewed persons.
Key words: county, crisis management, organizational structure, coverage.

Wstęp

Tytuł artykułu *Organizacja i funkcjonowanie Wojewódzkiego Centrum Zarządzania Kryzysowego w Kielcach* wynika z przyjętych rozstrzygnięć językowych. Ze względu na zakres terytorialny właściwym określeniem przedmiotowego Wojewódzkiego Centrum Zarządzania Kryzysowego (WCZK) byłoby WCZK województwa świętokrzyskiego, jednakże ze względów stylistycznych, tytuł artykułu sformułowano, uwzględniając lokalizację siedziby WCZK. Nie zmienia to jednak zasadniczego celu artykułu: prezentacji sposobu organizacji oraz zakresu działalności WCZK. Nie ma to również wpływu

[1] harabinradek@o2.pl

na określenie problemu badawczego pracy, którym jest rozpoznanie, w jaki sposób organizacja centrum przekłada się na jego funkcjonowanie. Problem badawczy znalazł swoje rozwinięcie w hipotezie sformułowanej w następujący sposób: potencjał infrastrukturalny oraz osobowy ma kluczowe znaczenie w realizacji przez centrum zadań określonych aktami prawa.

Artykuł powstał na podstawie badań idiograficznych, które charakteryzują się dążeniem do jak największego uprawdopodobnienia ustaleń. Jeśli chodzi o zastosowaną w nim zasadę rozumowania uprawdopodobniającego, najwłaściwiej należałoby wskazać model wnioskowania przez indukcję enumeracyjną niezupełną [Ziembiński 2015, ss. 182–183]. Liczba zgromadzonych źródeł, potwierdzających tę samą informację określa stopień jej uprawdopodobnienia. Podstawowe badania sprowadzają się do wywiadów przeprowadzonych w różnych okresach czasu od stycznia do połowy maja 2017 r. z Krzysztofem Bartoszem – Kierownikiem WCZK w Kielcach. Uzyskane informacje na temat m.in. źródeł finansowania zarządzania kryzysowego, działalności szkoleniowej i planistycznej, sytuacji kryzysowych w województwie świętokrzyskim oraz zasad i sposobu organizacji centrum zostały porównane z ogólną literaturą przedmiotu oraz dokumentami dostępnymi w Świętokrzyskim Urzędzie Wojewódzkim. Informacje na temat zdarzeń terenowych, w przypadku prezentowanego artykułu – kryzysu energetycznego z 2014 r., zostały zweryfikowane w trakcie wizyt w urzędach gmin, których tereny dotknął kryzys.

W literaturze przedmiotu nie odnaleziono artykułów oraz pozycji zwartych na temat WCZK w Kielcach. Najbliższym tematycznie opracowaniem jest książka G. Sobolewskiego *Organizacja i Funkcjonowanie Centrum Zarządzania Kryzysowego* [Sobolewski 2011]. Pozycja ta pochodzi z 2011 r., więc wiele zagadnień – np. struktura organizacyjna Rządowego Centrum Bezpieczeństwa (RCB) – uległo zmianie. Autor porusza kwestie wojewódzkiego centrum zarządzania kryzysowego na przykładzie województwa lubuskiego. Niemniej jednak sam układ tematyczny rozdziału uznano za wzorcowy i adaptowano go na potrzeby prezentowanego artykułu. Pracę rozpoczyna opis zasad organizacji WCZK w Kielcach, następnie omówiono strukturę i wyposażenie (w tym informatyczne) centrum, aby przejść do wyjaśnień na temat zakresu zadań oraz działań osób funkcyjnych.

Zasady organizacji Wojewódzkiego Centrum Zarządzania Kryzysowego w Kielcach

Podstawą prawną utworzenia Wojewódzkiego Centrum Zarządzania Kryzysowego jest art. 16 ustawy z 26 kwietnia 2007 r. [Ustawa z dnia 26 kwietnia 2007 r. o zarządza-

niu kryzysowym 2007, s. 22]. Ustawa nie określa dokładnej formy organizacji centrum w ramach urzędu wojewódzkiego. Praktyka wskazuje, że najczęstszym rozwiązaniem jest utworzenie centrum w ramach wydziału bezpieczeństwa urzędu wojewódzkiego. Również w województwie świętokrzyskim – co prawda po perturbacjach i początkowym zatrudnieniu dyżurnych w Wydziale Spraw Obywatelskich i Cudzoziemców Świętokrzyskiego Urzędu Wojewódzkiego [Wywiad z K. Bartoszem Kierownikiem WCZK w Kielcach] – ostatecznie centrum powstało jako jednostka Wydziału Bezpieczeństwa i Zarządzania Kryzysowego [Załącznik nr 1 do Zarządzenia nr 62/2016 Wojewody Świętokrzyskiego z dnia 1 czerwca 2016 r. w sprawie ustalenia regulaminu Świętokrzyskiemu Urzędowi Wojewódzkiemu w Kielcach 2016, s. 73]. W Świętokrzyskim Urzędzie Wojewódzkim przyjęto tym samym trójstopniowy model odpowiedzialności za zarządzanie kryzysowe. Wojewoda zgodnie z art. 22 ustawy o wojewodzie i administracji rządowej w województwie „wykonuje i koordynuje zadania w zakresie obronności i bezpieczeństwa państwa oraz zarządzania kryzysowego" [Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie 2009, s. 6]. W art. 14 ustawy o zarządzaniu kryzysowym uściślono obowiązki wojewody jako organu właściwego w sprawach zarządzania kryzysowego na terenie województwa [Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym 2007, ss. 19–20]. Zgodnie z art. 7.1 Regulaminu Świętokrzyskiego Urzędu Wojewódzkiego, wojewoda sprawuje swoje zadania przy pomocy właściwego dyrektora wydziału [Załącznik nr 1 do Zarządzenia nr 62/2016 Wojewody Świętokrzyskiego z dnia 1 czerwca 2016 r. w sprawie ustalenia regulaminu Świętokrzyskiemu Urzędowi Wojewódzkiemu w Kielcach 2016, s. 4]. W tym wypadku jest to dyrektor Wydziału Bezpieczeństwa i Zarządzania Kryzysowego. Zgodnie z §68.1.8. Regulaminu Świętokrzyskiego Urzędu Wojewódzkiego wydziały dzielą się na inne komórki – w tym Centrum Zarządzania Kryzysowego z kierownikiem na czele. *De facto* – w trójstopniowym podziale obowiązków – to kierownik Wojewódzkiego Centrum Zarządzania Kryzysowego ponosi ciężar realizacji zadań zarządzania kryzysowego. Świadczą o tym m.in. pełnomocnictwa wojewody do podpisu dokumentów na wypadek sytuacji kryzysowych oraz konieczność składania dziennych raportów dyrektorowi wydziału oraz wojewodzie – raportuje organ, który wykonuje zadania.

Zarządzenie Wojewody Świętokrzyskiego nr 3/2011 z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach należy uznać za podstawowy dokument regulujący zasady organizacji centrum. Komplementarny akt stanowi Zarządzenie Wojewody Świętokrzyskiego z dnia 24 stycznia 2017 r. w sprawie powołania Wojewódzkiego Zespołu Zarządzania Kryzysowego w nowej strukturze. Zarządzenie

nakłada i określa zakres obowiązków WCZK związanych z obsługą Wojewódzkiego Zespołu Zarządzania Kryzysowego. Wyznacza zadania z zakresu alarmowania, organizacji przepływu informacji oraz obsługi kancelaryjno-biurowej tego zespołu [Załącznik nr 1 do Zarządzenia nr 9/2017 Wojewody Świętokrzyskiego z dnia 24 stycznia 2017 r. w sprawie powołania Wojewódzkiego Zespołu Zarządzania Kryzysowego 2017, ss. 5–6]. Innymi słowy: określa relacje organu opiniodawczo-doradczego wojewody z jednostką utrzymującą 24-godzinną gotowość do podjęcia działań [Mazurek-Kucharska, Wojciechowska-Filipek 2014, s. 76]. W województwie świętokrzyskim Wojewódzkie Centrum Zarządzania Kryzysowego obsługuje poszerzony Zespół Zarządzania Kryzysowego. W jego skład włączono Zespół ds. Handlu Ludźmi oraz Zespół ds. Organizacji Imprez Masowych [Załącznik nr 1 do Zarządzenia nr 9/2017 Wojewody Świętokrzyskiego z dnia 24 stycznia 2017 r. w sprawie powołania Wojewódzkiego Zespołu Zarządzania Kryzysowego 2017, s. 16].

Struktura organizacyjna oraz wyposażenie Wojewódzkiego Centrum Zarządzania Kryzysowego w Kielcach

Strukturę organizacyjną WCZK w Kielcach tworzą kierownik, pracownicy merytoryczni do spraw:

- planowania ochrony infrastruktury krytycznej i bezpieczeństwa energetycznego,
- łączności oraz systemu wykrywania i alarmowania,
- planowania reagowania kryzysowego,
- ochrony przed powodzią

oraz dyżurni analitycy – 5 etatów [Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 5].

Pracownik do spraw ochrony infrastruktury krytycznej i bezpieczeństwa energetycznego pełni funkcję nieetatowego zastępcy kierownika. Liczba etatów (pięć) zarezerwowanych dla dyżurnych analityków wynika z trybu prowadzenia całodobowych dyżurów w centrum. Utrzymanie całorocznych, całodobowych i dwuzmianowych dyżurów wymaga podpisania pięciu umów o pracę w wymiarze 40 godzin tygodniowo. Dodatkowo w komórce obowiązuje zasada wymienności funkcji, która oznacza, że w razie sytuacji kryzysowej pracownicy merytoryczni – w tym również kierownik – mogą pełnić dyżury [Wywiad z K. Bartoszem Kierownikiem WCZK w Kielcach]. W razie konieczności na wniosek kierownika dyrektor wydziału może oddelegować dodatkowych pracowników do pomocy w wykonywaniu zadań centrum [Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia

regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 5]. Inaczej niż np. w województwie lubuskim lekarz koordynator nie wchodzi w skład WCZK w Kielcach (jest przypisany do Oddziału Ratownictwa Medycznego), chociaż korzysta z pomieszczeń służbowych centrum [Sobolewski 2011, s. 51, Załącznik nr 1 do Zarządzenia nr 62/2016 Wojewody Świętokrzyskiego z dnia 1 czerwca 2016 r. w sprawie ustalenia regulaminu Świętokrzyskiemu Urzędowi Wojewódzkiemu w Kielcach 2016, s. 79].

W skład pomieszczeń Wojewódzkiego Centrum Zarządzania Kryzysowego w Kielcach wchodzi 8 lokali służbowych rozmieszczonych w strefie administracyjnej Świętokrzyskiego Urzędu Wojewódzkiego. Umiejscowienie centrum w bezpośrednim sąsiedztwie biur wojewody oraz pozostałych osób funkcyjnych zapewnia sprawną koordynacje działań zarówno w zwykłym, jaki i alarmowym (kryzysowym) trybie pracy. Bazę lokalową WCZK w Kielcach tworzą: sala narad na 32 osoby, wyizolowane i wyposażone w system obserwacji wizyjnej pomieszczenie kierownika WCZK, pomieszczenie lekarza koordynatora, pomieszczenie pracowników WCZK – ds. ochrony przed powodzią, ds. planowania zarządzania kryzysowego, pomieszczenie pracowników WCZK – ds. łączności oraz systemu wykrywania i alarmowania, ds. ochrony infrastruktury krytycznej i planowania bezpieczeństwa energetycznego, pomieszczenie operacyjne WCZK, pomieszczenie dyżurnego WCZK, pomieszczenie socjalne dyżurnego WCZK [Logistyka szczegółowa…, s. 1].

WCZK w Kielcach tworzy strefę z ograniczonym dostępem dla osób nieuprawnionych, w ten sposób wyeliminowano ewentualne zakłócenia pracy centrum przez petentów Świętokrzyskiego Urzędu Wojewódzkiego. Centrum, oprócz standardowego wyposażenia biurowego, wykorzystuje szeroki zakres urządzeń technicznych, poczynając od radiotelefonów Motorola GM 360 oraz Dm 3400, poprzez aparaty telefoniczne, telefony komórkowe, kończąc na specjalistycznym sprzęcie typu: rejestrator rozmów telefonicznych i radiowych SIM Logger, stacje pogodowe OREGON WMR 928, barometr elektroniczny Oregon, radiostacja ICOM IC 7400 – nasłuch w sieci COP WP, radiostacja lotnicza ICOM IC-A110EURO oraz system nadzoru syren elektronicznych Vektra. Sala narad, pomieszczenia lekarza koordynatora oraz dyżurnych zostały wyposażone w telewizory [Logistyka szczegółowa…, ss. 2–6]. Służą one śledzeniu doniesień medialnych, stanowiących jedno ze źródeł sporządzania dobowych raportów bezpieczeństwa [Wywiad z K. Bartoszem Kierownikiem WCZK w Kielcach]. Wyposażenie techniczne centrum wykorzystuje się nie tylko w zakresie bieżących zadań lub do zapewnienia przepływu informacji w systemie zarządzania kryzysowego, lecz stanowi ono przede wszystkim zabezpieczenie na wypadek sytuacji kryzysowych. W styczniu 2014 r., podczas kryzysu energetycznego w części województwa świętokrzyskiego

(przede wszystkim rejony energetyczne: Skarżysko Kamienna, Ożarów, Ostrowiec Świętokrzyski), w obliczu rozładowania zasilania przekaźników telekomunikacyjnych, wykorzystywano łączność radiową [Baran 2014, Gminny Zespół Zarządzania Kryzysowego w Bodzentynie 2014, s. 5, Wojewódzkie Centrum Zarządzania Kryzysowego 2014, ss. 1–2]. W przypadku powodzi w 2010 r., która w województwie świętokrzyskim szczególnie dotknęła Sandomierz i gminy przyległe, Powiatowe Centrum Zarządzania Kryzysowego w Tarnobrzegu oparło łączność na telefonii abonenckiej [Wywiad z Tadeuszem Blachą Kierownikiem PCZK w Tarnobrzegu].

Wykorzystywane systemy informatyczne

W pracy Wojewódzkiego Centrum Zarządzania Kryzysowego w Kielcach wykorzystywanych jest wiele systemów i ułatwień informatycznych. System łączności radiowej oraz kablowej uzupełnia system wideokonferencji MSWiA [Logistyka szczegółowa…, s. 1]. Sprawny obieg dokumentów umożliwia EZD Edicta – system elektronicznego zarządzania dokumentacją, będący platformą zarządzania: korespondencją, dokumentami, projektami, poleceniami, terminami oraz czasem pracy pracowników. Zgromadzone w nim dokumenty tworzą centralną bazę informacji. Uzupełnia go System Niejawnej Poczty Internetowej OPAL, zaprojektowany przez MSWiA, którego gestorem jest dyrektor Rządowego Centrum Bezpieczeństwa. OPAL umożliwia przesyłanie informacji niejawnych, stanowiących tajemnicę służbową, oznaczonych klauzulą „Zastrzeżone" oraz informacji klasyfikowanych „NATO Restricted" i „UE Restricted", pomiędzy upoważnionymi podmiotami. Utajnianiu informacji służy program szyfrujący PEM-HEART oraz klucze podmiotów uprawnionych do zabezpieczania podpisu elektronicznego i szyfrowania wiadomości [Logistyka szczegółowa…, ss. 1–2]. W celu sporządzania dokumentacji niejawnej wykorzystuje się system POPIEL [Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 12]. Centrum korzysta również z Elektronicznej Platformy Usług Administracji Publicznej (ePUAP) w zakresie określonym przez rozporządzenie Ministra Administracji i Cyfryzacji z 6 maja 2014 r. [Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej 2014]. Niezwykle istotna dla przepływu informacji w systemie zarządzania kryzysowego jest Centralna Aplikacja Raportująca (CAR), czyli system raportowania o zagrożeniach. CAR tworzy jednolity i spójny systemu raportowania spajający powiatowe, wojewódzkie centra zarządzania kryzysowego oraz Rządowe Centrum Bezpie-

czeństwa [Domański 2016, s. 247]. „W ramach CAR został utworzony jednolity katalog zagrożeń – wszystkie informacje wprowadzone do systemu są przyporządkowane odpowiedniej kategorii. Jest ich około 20, na przykład katastrofy naturalne czy wypadki komunikacyjne. Taki podział ujednolica system raportowania, ułatwia wyszukiwanie informacji, a co najważniejsze skraca czas reagowania na zdarzenie" [Rządowe Centrum Bezpieczeństwa 2013].

Wojewoda świętokrzyski w §14 pkt 7 Regulaminu WCZK w Kielcach nałożył na centrum obowiązek realizacji zadań w ramach Systemu Wykrywania i Alarmowania oraz Systemu Wczesnego Ostrzegania [Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 17]. Centrum prowadzi stały dozór hydrologiczny i metrologiczny na podstawie Monitora Instytutu Meteorologii i Gospodarki Wodnej Państwowego Instytutu Badawczego [Instytut Meteorologii i Gospodarki Wodnej 2014a, 2014b]. Monitor jest narzędziem gromadzenia i wizualizacji danych pomiarowych. Dane pochodzą z automatycznej sieci pomiarowej IMGW-PIB, jak również są wynikiem pomiarów wykonywanych przez obserwatorów. Dostęp do serwisu odbywa się za pomocą przeglądarki internetowej. Dane udostępniane są równocześnie pracownikom IMGW-PIB oraz zewnętrznym użytkownikom statutowym, takim jak: służby kryzysowe, instytucje rządowe, wojsko, czy straż pożarna [Centrum Hydrologicznej Osłony Kraju 2015, s. 2]. Monitoring hydrologiczny odbywa się również na podstawie komunikatów otrzymywanych od Wydziału Centrum Operacyjnego Zarządzania Przeciwpowodziowego Wisły Środkowej Regionalnego Zarządu Gospodarki Wodnej w Warszawie [Regionalny Zarząd Gospodarki Wodnej 2017]. Kierownik oraz dyżurni są uprawnieni do korzystania z Regionalnego Systemu Ostrzegania (RSO) – usługi Ministerstwa Administracji i Cyfryzacji umożliwiającej powiadamianie obywateli o lokalnych zagrożeniach [Domański 2016, s. 241]. WCZK w Kielcach na podstawie porozumienia z lokalnym oddziałem TVP nadaje ostrzeżenia w telewizji naziemnej (do telegazety i w postaci paska na ekranie telewizora), a także Radiu Kielce [Wojewoda Świętokrzyski, Dyrektor OT TP SA 2008, Wojewoda Świętokrzyski, Dyrektor OT TP SA 2008, Wojewoda Świętokrzyski, Zarząd Polskiego Radia Regionalnej Rozgłośni w Kielcach „Radio Kielce" SA 2013] za pomocą aplikacji telefonicznej RSO oraz na stronie internetowej Świętokrzyskiego Urzędu Wojewódzkiego. Funkcja RSO-SMS została zarezerwowana dla priorytetowych komunikatów, dotyczących np. powodzi, wiatrów huraganowych lub innych równie gwałtownych i niebezpiecznych zjawisk. Centrum uczestniczy w ćwiczeniach Krajowego Systemu Wykrywania Skażeń i Alarmowania [Załącznik nr 1 do Zarządzenia nr 62/2016 Wojewody Świętokrzyskiego z dnia 1 czerwca 2016 r. w sprawie ustalenia

regulaminu Świętokrzyskiemu Urzędowi Wojewódzkiemu w Kielcach 2016, s. 74]. Korzysta też z Systemu Informacji Geograficznej (GIS – Geographic Information System). GIS jest narzędziem gromadzenia i wizualizacji danych. Pozwala tworzyć i nakładać na siebie mapy przygotowane na potrzeby bezpieczeństwa. Gromadzenie informacji odbywa się zarówno za pomocą sieci czujników, jaki i w wyniku wykorzystania gotowych baz danych przygotowanych np. przez PSP czy WOPR [Domański 2016, ss. 238–239]. W województwie świętokrzyskim GIS uzupełniają: Program Pakiet Grafiki Operacyjnej (PGO) oraz mapy cyfrowe połączone z uniwersalnym Systemem Wspomagania Zarządzania Kryzysowego PROMIEŃ [Logistyka szczegółowa…, s. 2].

Zadania i zakres działań Wojewódzkiego Centrum Zarządzania Kryzysowego w Kielcach

W literaturze przedmiotu jako główne zadanie centrów zarządzania kryzysowego wymienia się zapewnienie całodobowego przepływu informacji w systemie zarządzania kryzysowego [Krynojewski, Sienkiewicz-Małyjurek 2010, s. 52]. Ta teoretyczna konstatacja znajduje potwierdzenie w praktyce i w sposób szczególny uwidacznia się w działalności powiatowego centrum zarządzania kryzysowego. Po godzinach urzędowania starostwa, powiatowe centra – najczęściej na zasadach porozumienia z odpowiednimi służbami (np. Miejską Komendą Straży Pożarnej) – cedują na nie wymóg całodobowych dyżurów [Załącznik do Zarządzenia nr 152/2015 Starosty Kieleckiego z dnia 6 listopada 2015 r. Regulamin Organizacyjny Powiatowego Centrum Zarządzania Kryzysowego 2015, s. 4]. Innymi słowy: ograniczają swoją działalność do podstawowej, lecz zarazem konstytutywnej funkcji – zapewnienia drożności przepływu informacji w systemie zarządzania kryzysowego. Co prawda ustawa o zarządzaniu kryzysowym nakłada na wojewódzkie centra szerszy katalog zadań, m.in. nadzór nad systemami wykrywania i alarmowania oraz wczesnego ostrzegania ludności oraz współpracę z wyspecjalizowanymi służbami, lecz zapewnienie całodobowych dyżurów nadal należy uznać za ich zadanie podstawowe. [Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym 2007, s. 22].

Regulamin WCZK w Kielcach, w rozdziale IV i V, kolejno określa zadania ogólne centrum oraz zadania szczegółowe osób funkcyjnych – kierownika oraz dyżurnych. Do zadań ogólnych zalicza się m.in.:

- współdziałanie z powiatowymi centrami zarządzania kryzysowego w zakresie reagowania kryzysowego;
- opracowywanie przetwarzanie, sprawdzanie i przekazywanie informacji dotyczących sytuacji nadzwyczajnych;

- opracowanie procedur dotyczących uruchomienia i koordynacji działań w zakresie udzielania i odbioru pomocy humanitarnej;
- pozyskiwanie informacji i opracowywanie dobowych meldunków o sytuacji w województwie, a także opracowywanie zbiorczych raportów tygodniowych, miesięcznych i kwartalnych o sytuacji i prognozowanych zagrożeniach;
- stałą wymianę informacji ze służbami dyżurnymi administracji zespolonej i niezespolonej oraz innymi służbami i inspekcjami;
- w przypadku zagrożenia i zaistnienia stanu kryzysowego, niezwłoczne i ciągłe, informowanie o rozwoju sytuacji Rządowego Centrum Bezpieczeństwa;
- nadzór nad funkcjonowaniem systemu wykrywania i alarmowania oraz wczesnego ostrzegania ludności [Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 6].

Na podstawie §13 Regulaminu WCZK w Kielcach, zadania kierownika można pogrupować w następujące kategorie:

1. Zadania nadzorcze – nadzór nad obsługą kancelaryjno-biurową Wojewódzkiego Zespołu Zarządzania Kryzysowego; nadzór nad systemem obiegu dokumentów WCZK w Kielcach; nadzór nad systemami monitorowania i ostrzegania; nadzór w zakresie całokształtu prac dotyczących przygotowania i zabezpieczenia funkcjonowania dyżuru; nadzór nad prowadzoną w ramach działalności centrum dokumentacją dyżuru; nadzór nad opracowywanymi na podstawie meldunków zbiorczych informacji dla wojewody i Rządowego Centrum Bezpieczeństwa; czuwanie nad przestrzeganiem tajemnicy państwowej określonej przez poszczególne klauzule tajności w zakresie zadań wykonywanych przez WCZK.
2. Zadania organizacyjne – organizowanie pracy centrum; opracowanie grafików pełnienia dyżuru w WCZK w Kielcach; udział przy opracowywaniu informacji, analiz, ocen i opinii w sprawach dotyczących zakresu działania komórki organizacyjnej; zabezpieczanie danych przed dostępem niepowołanych osób, uszkodzeniem lub zniszczeniem; udostępnianie danych.
3. Zadania kierownicze – ponoszenie odpowiedzialności za nielegalne ujawnianie danych osobowych, również po ustaniu zatrudnienia; szkolenie obsad dyżurnych w WCZK w Kielcach; zawiadamianie dyrektora wydziału i wojewody o powstaniu sytuacji kryzysowej oraz podwyższaniu gotowości obronnej państwa [Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 6].

W sytuacji kryzysowej kierownik odpowiada za kontakty z mediami. Pełni dyżur oraz nadzoruje pracę dyżurnych analityków, na tej podstawie posiada pełne i aktualne rozpoznanie terenowe. Dodatkowo, najczęściej, utrzymuje kontakty bezpośrednie z dowódcami akcji, co pozwala mu śledzić dynamikę rozwoju sytuacji [Wywiad z K. Bartoszem Kierownikiem WCZK w Kielcach].

Wojewódzkie Centrum Zarządzania Kryzysowego w Kielcach wykonuje również szereg zadań z zakresu obrony cywilnej oraz obronności kraju. Prowadzi działalność, która nie jest związana *stricte* z zarządzaniem kryzysowym. Zgodnie z orzeczeniem Trybunału Konstytucyjnego [Trybunał Konstytucyjny 2009, 2012], działania z zakresu stanów nadzwyczajnych nie stanowią przedmiotu zarządzania kryzysowego. Regulamin WCZK w Kielcach w §9, §14 i §22 nakłada jednak na centrum obowiązki dotyczące stanów nadzwyczajnych [Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 6, 10 i 12]. Kierownik oraz pracownicy merytoryczni WCZK w Kielcach uczestniczą w opracowywaniu planów właściwych Wydziałowi Bezpieczeństwa, lecz wykraczających poza ramy zarządzania kryzysowego [Załącznik nr 1 do Zarządzenia nr 62/2016 Wojewody Świętokrzyskiego z dnia 1 czerwca 2016 r. w sprawie ustalenia regulaminu Świętokrzyskiemu Urzędowi Wojewódzkiemu w Kielcach 2016, s. 81]. Przygotowują m.in. plany operacyjne województwa świętokrzyskiego, wojewódzkie plany doskonalenia obrony cywilnej, wojewódzki plan przygotowania i wykorzystania podmiotów leczniczych na potrzeby obronne państwa oraz plany organów samorządowych [Wywiad z K. Bartoszem Kierownikiem WCZK w Kielcach]. Centrum prowadzi również obsługę linii numeru 987, pod którym osoby potrzebujące i bezdomni mogą uzyskać informacje na temat noclegowni, ogrzewalni, schronisk różnych kategorii, stołówek, ośrodków pomocy, przytulisk.

Zakres działań służby dyżurnej

Praktyka zatrudnienia dyżurnych przez kierownika WCZK wskazuje na preferowanie osób będących byłymi funkcjonariuszami służb mundurowych. Przyczyn takiego stanu rzeczy należy szukać zarówno w kwestiach praktycznych, jak i ekonomicznych. Byli mundurowi dysponują wstępnym rozpoznaniem terenu, zasobów i środków województwa. Jest to wiedza szczególnie przydatna podczas szkoleń oraz w przypadku konieczności szybkiego reagowania w sytuacji kryzysowej. Dużą rolę odgrywa dyscyplina nabyta podczas służby. Zwłaszcza w sytuacjach nadzwyczajnych, kiedy następuje zmiana 12-godzinnej służby dyżurnej na 8- i 16-godzinny tryb pracy [Zarządzenie nr

3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 5]. Nie bez znaczenia pozostaje znajomość systemów łączności, a także fakt pobierania emerytur służbowych – które w pewien sposób rekompensują stosunkowo niewielkie wynagrodzenie dyżurnego [Wywiad z K. Bartoszem Kierownikiem WCZK w Kielcach].

Czas pracy zmiany służbowej wynosi 12 godzin: I zmiana: 7.30–19.30, II zmiana: 19.30–7.30. Zmiany dyżurów odbywają się zgodnie z harmonogramem dyżurów, który ustala kierownik. Osoba zdająca dyżur zobligowana jest do przekazania informacji z przebiegu pełnionego dyżuru osobie przyjmującej dyżur. Dodatkowo powinna poinformować ją o otrzymanych meldunkach, zgłoszeniach i zadaniach, a także wskazać sposób załatwienia spraw niezrealizowanych [Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, s. 5]. Służba dyżurna drugiej zamiany gromadzi i analizuje informacje dostarczane przez media, służby i administrację oraz opracowuje raport dobowy: przesyła informację dobową do Rządowego Centrum Bezpieczeństwa, sporządza papierową wersję dobowej informacji celem jej archiwizacji, przesyła meldunek bieżący do: wojewody, dyrektora WBiZK oraz kierownika WCZK [Sobolewski 2011, s. 63].

Raporty przesyłane są za pomocą CAR. Jeśli nie wystąpiły zjawiska konieczne do odnotowania, służba dyżurna wysyła „pusty" raport. Stanowi on zarówno informację o braku zagrożeń, jak również potwierdza drożność systemu. Raporty tworzy się na podstawie doniesień medialnych, raportów hydrologicznych i meteorologicznych oraz informacji otrzymywanych od służb. Ze względu na brak ustawowego obowiązku przesyłania informacji do WCZK przez służby, istotną rolę odgrywają kontakty personalne. Kierownik oraz dyżurni posiadają rozeznanie w osobach funkcyjnych województwa świętokrzyskiego [Wywiad z K. Bartoszem Kierownikiem WCZK w Kielcach]. W obliczu fiaska systemu SARNA (System Analizy i Raportów – Narzędzie Analityczne), stan wolnych łóżek w szpitalach dyżurni ustalają w wyniku bezpośredniego kontaktu ze szpitalną izbą przyjęć. Służba dyżurna pełni również funkcję obsługi kancelaryjnej wojewody oraz Świętokrzyskiego Urzędu Wojewódzkiego w dni wolne oraz po godzinach pracy. Dotyczy ona najczęściej przyjmowania korespondencji oraz spełniania funkcji komunikowania się z wojewodą w nagłych wypadkach [Wywiad z K. Bartoszem Kierownikiem WCZK w Kielcach].

Do stałych obowiązków dyżurnego należy przyjęcie zgłoszenia oraz uruchomienie właściwej procedury. Na polecenie osoby przełożonej, pracownicy centrum realizują standardowe procedury działania właściwe dla zaistniałej sytuacji kryzysowej. Ich kata-

log został określony w Wojewódzkim Planie Zarządzania Kryzysowego Województwa Świętokrzyskiego. Dokument klasyfikuje 13 rodzajowo różnych zagrożeń oraz 31 standardowych procedur operacyjnych [Wojewoda Świętokrzyski 2016, s. 37 i 116].

Zakończenie

Podsumowując ustalenia, należy stwierdzić, że WCZK w Kielcach działa przede wszystkim na podstawie ustawy o zarządzaniu kryzysowym oraz w oparciu o dwa zarządzenia Wojewody Świętokrzyskiego – nr 3/2011 i nr 62/2016 [Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym 2007, Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach 2011, Zarządzenie nr 62/2016 Wojewody Świętokrzyskiego z dnia 1 czerwca 2016 r. w sprawie ustalenia regulaminu Świętokrzyskiemu Urzędowi Wojewódzkiemu w Kielcach 2016]. Centrum posiada szerokie zaplecze techniczne i informatyczne oraz niezbyt rozbudowaną strukturę funkcyjną. Na podstawie Regulaminu WCZK w Kielcach należy wnioskować, że funkcjonowanie centrum opiera się przede wszystkim na działalności kierownika oraz służby dyżurnej. Obserwacja praktyki oraz wywiady wykazały, że infrastruktura techniczna – systemy łączności, gromadzenia oraz przetwarzania informacji – nie tylko usprawniają pracę centrum, lecz są konstytutywne dla jego funkcjonowania. CAR, Popiel, Opal, GIS, monitory hydrologiczne i meteorologiczne – oraz pozostałe programy opisane w artykule – to podstawowe narzędzia pracy WCZK w Kielcach. Należy zatem stwierdzić, że hipoteza badawcza została zweryfikowana pozytywnie.

W toku badań ustalono również inne wnioski, okazało się bowiem, że WCZK w Kielcach jest nierozerwalnie złączone z innymi komórkami Świętokrzyskiego Urzędu Wojewódzkiego. W sprawach wymagających wiedzy specjalistycznej, kierownik centrum korzysta z pomocy m.in. pracowników Wydziału Prawnego, Nadzoru i Kontroli Świętokrzyskiego Urzędu Wojewódzkiego czy komórki informatycznej. Owa relacja łącząca Świętokrzyski Urząd Wojewódzki z centrum jest funkcją zwrotną. WCZK w Kielcach wykonuje szereg prac – m.in. kancelaryjnych – wykraczających poza ramy zarządzania kryzysowego. Jest to obserwacja, która w zestawieniu z ustaleniami artykułu, uprawnia do konstatacji o zbyt małym składzie osobowym i funkcyjnym w stosunku do zakresu obowiązków WCZK w Kielcach. Wydaje się jednak, że wniosek ten można odnieść do wszystkich szczebli systemu zarządzania kryzysowego w Polsce.

Bibliografia

Baran P. (2014), *Awarie prądu w Świętokrzyskiem* [!]. *Trwają naprawy w wielu miejscowościach*, „Echo Dnia", 23 stycznia, [online] http://www.echodnia.eu/swietokrzyskie/wiadomosci/region/art/8020323,awarie-pradu-w-swietokrzyskiem-trwaja-naprawy-w-wielu-miejscowosciach,id,t.html, dostęp: 20.05.2017.

Centrum Hydrologicznej Osłony Kraju (2015), *Monitor IMGW-PIB. Instrukcja użytkownika* [online] http://www.imgw.pl/attachments/1829_3_Zalacznik_A_Dokumentacja_uzytkowa%20_Monitora_IMGW_PIB.doc, dostęp: 25.05.2017.

Domański P. (2016), *System wsparcia informatycznego w systemie zarządzania kryzysowego na szczeblu wojewódzkim*, „Rocznik Bezpieczeństwa Morskiego", R. X, Akademia Marynarki Wojennej, Gdynia.

Gminny Zespół Zarządzania Kryzysowego w Bodzentynie (2014), *Protokół z posiedzenia Gminnego Zespołu Zarządzania Kryzysowego w Bodzentynie* [18 grudnia 2014 r.], dokument dostępny w Urzędzie Miasta i Gminy Bodzentyn.

Instytut Meteorologii i Gospodarki Wodnej (2014a), *Komunikat hydrologiczny Instytutu Meteorologii i Gospodarki Wodnej Państwowego Instytutu Badawczego. Oddział w Krakowie* [17 listopada 2014 r.], dokument dostępny w Wojewódzkim Centrum Zarządzania Kryzysowego w Kielcach.

Instytut Meteorologii i Gospodarki Wodnej (2014b), *Komunikat opadowy Instytutu Meteorologii i Gospodarki Wodnej Państwowego Instytutu Badawczego. Oddział w Krakowie* [17 listopada 2014 r.], dokument dostępny w Wojewódzkim Centrum Zarządzania Kryzysowego w Kielcach.

Krynojewski F, Sienkiewicz-Małyjurek K. (2010), *Zarządzanie kryzysowe w administracji publicznej*, Difin, Warszawa.

Logistyka szczegółowa Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego, opracowanie dostępne w Wojewódzkim Centrum Zarządzania Kryzysowego w Kielcach.

Mazurek-Kucharska B., Wojciechowska-Filipek S. (2014), *Zarządzanie kryzysowe. Aspekty organizacyjne i psychologiczne*, CeDeWu, Warszawa.

Regionalny Zarząd Gospodarki Wodnej w Warszawie (2017), *Informacja z dnia 16 maja 2016 r. o aktualnej sytuacji na obszarze administrowanym przez RZGW w Warszawie stan na dzień 16.05.2017 na godz. 6.00*, dokument dostępny w Wojewódzkim Centrum Zarządzania Kryzysowego w Kielcach.

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 6 maja 2014 r. w sprawie zakresu i warunków korzystania z elektronicznej platformy usług administracji publicznej (2014), Dz.U. z 2014 r. poz. 584.

Rządowe Centrum Bezpieczeństwa (2013), *Komunikat z 10 września 2013 r.*, [online] http://rcb.gov.pl/centralna-aplikacja-raportujaca-dziala-od-1-wrzesnia-br, dostęp: 25.05. 2017.

Sobolewski G. (2011), *Organizacja i funkcjonowanie centrum zarządzania kryzysowego*, Akademia Obrony Narodowej, Warszawa.

Trybunał Konstytucyjny (2009), Wyrok z dnia 21 kwietnia 2009 r., Dz. U. z 2009 r. Nr 65 poz. 553.

Trybunał Konstytucyjny (2012), Wyrok z dnia 3 lipca 2012 r., Dz. U. z 2012 r. poz. 799.

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (2007), Dz. U. z 2017 r. poz. 209 i 1566.

Ustawa z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (2009), Dz. U. z 2017 r. poz. 935, 976, 1475 i 1566.

Wojewoda Świętokrzyski, Dyrektor OT TP SA (2008), *Porozumienie w zakresie współpracy podczas informowania ludności w sytuacjach kryzysowych* [14 maja 2008 r.], dokument dostępny w Wojewódzkim Centrum Zarządzania Kryzysowego w Kielcach.

Wojewoda Świętokrzyski, Zarząd Polskiego Radia Regionalnej Rozgłośni w Kielcach „Radio Kielce SA" (2013), *Porozumienie w sprawie nawiązania współpracy w zakresie obiegu i wymiany informacji w sytuacjach kryzysowych i zagrożenia bezpieczeństwa obywateli* [23 listopada 2013 r.], dokument dostępny w Wojewódzkim Centrum Zarządzania Kryzysowego w Kielcach.

Wojewoda Świętokrzyski (2016), *Wojewódzki Plan Zarządzania Kryzysowego Województwa Świętokrzyskiego* [28 kwietnia 2016 r.], [online] http://czkw.kielce.uw.gov.pl/czk/wojewodzkie-centrum-zarz/wojewodzki-plan-zarzadzania, dostęp: 12.08.2017.

Wojewódzkie Centrum Zarządzania Kryzysowego (2015), *Ocena zagrożeń województwa świętokrzyskiego w 2014 r.* [10 stycznia 2015 r.], znak: WBiZK.I.6332.2015, opracowanie dostępne w Wojewódzkim Centrum Zarządzania Kryzysowego w Kielcach.

Załącznik do Zarządzenia nr 152/2015 Starosty Kieleckiego z dnia 6 listopada 2015 r. Regulamin Organizacyjny Powiatowego Centrum Zarządzania Kryzysowego (2015), dokument dostępny w Starostwie Powiatowym w Kielcach.

Załącznik nr 1 do Zarządzenia nr 62/2016 Wojewody Świętokrzyskiego z dnia 1 czerwca 2016 r. w sprawie ustalenia regulaminu Świętokrzyskiemu Urzędowi Wojewódzkiemu w Kielcach (2016), [online] http://bip.kielce.uw.gov.pl/bip/urzad-wojewodzki, dostęp: 12.08.2017.

Załącznik nr 1 do Zarządzenia nr 9/2017 Wojewody Świętokrzyskiego z dnia 24 stycznia 2017 r. w sprawie powołania Wojewódzkiego Zespołu Zarządzania Kryzysowego (2017), dokument dostępny w Wojewódzkim Centrum Zrządzania Kryzysowego w Kielcach.

Zarządzenie nr 3/2011 Wojewody Świętokrzyskiego z dnia 20 stycznia 2011 r. w sprawie ustalenia regulaminu Wojewódzkiego Centrum Zarządzania Kryzysowego Świętokrzyskiego Urzędu Wojewódzkiego w Kielcach, [online] bip.kielce.uw.gov.pl/download/2/5996/z32011regulamin.pdf, dostęp: 12.08.2017].

Zarządzenie nr 62/2016 Wojewody Świętokrzyskiego z dnia 1 czerwca 2016 r. w sprawie ustalenia regulaminu Świętokrzyskiemu Urzędowi Wojewódzkiemu w Kielcach (2016), [online] http://bip.kielce.uw.gov.pl/bip/urzad-wojewodzki, dostęp: 12.08.2017.

Ziembiński Z. (2015), *Logika praktyczna*, Wydawnictwo Naukowe PWN, Warszawa.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **53–65**

Zofia Wilk-Woś[1], **Ewa Stroińska**[2]
Przemysław Kornacki[3], **Włodzimierz Zawisza**[4]
Społeczna Akademia Nauk

Współdziałanie służb i podmiotów ratowniczych w oparciu o system powiadamiania ratunkowego – rola i znaczenie operatorów numerów alarmowych w przekazie informacji o zdarzeniach

Cooperation of Emergency Services and Emergency Subjects Based on the Emergency Information System – Role and Significance of Emergency Phone Numbers Operators in Conveying Information about Emergencies

Abstract: Emergency information system is an important element of security management of the state and its citizens. A link of this system are emergency information centers. The aim of this article is an attempt to assess a current emergency information system pursuant to qualitative research with the application of focus group interview and free interview. The article attempts to assess emergency information system and to determine the role of emergency information centers in this system based on a systemic organization model identified by Harold Leavitt.
Key words: emergency information system, Emergency Information Centers, emergency phone numbers operators, police.

[1] zwilk@spoleczna.pl
[2] estroinska@spoleczna.pl
[3] przemyslawkornacki@interia.pl
[4] wierzbica@poczta.fm

Wstęp

Jednym z istotnych elementów zarządzania bezpieczeństwem państwa i jego obywateli jest system powiadamiania ratunkowego. Ogniwem tego sytemu są Centra Powiadamiania Ratunkowego. Na pracujących w nich operatorach numerów alarmowych spoczywa obowiązek sprawnej i rzeczowej obsługi zgłoszeń, gdyż w ratownictwie kluczowy jest przecież czas i informacja. Umiejętności i kompetencje operatorów mogą okazać się jednak niewystarczające przy braku odpowiedniej współpracy i współdziałania ze służbami i pozostałymi podmiotami ratowniczymi.

Celem artykułu jest próba oceny funkcjonującego obecnie systemu powiadamiania ratunkowego w oparciu o badania jakościowe z zastosowaniem metody zogniskowanego wywiadu grupowego FGI (Focus Group Interview) oraz wywiadu swobodnego. Grupy fokusowe tworzyli operatorzy numerów alarmowych z Centrum Powiadamiania Ratunkowego w Łodzi oraz policjanci z Komendy Powiatowej Policji w Pabianicach i Ośrodka Szkolenia Policji w Sieradzu, uczestniczący w zorganizowanych przez Łódzki Urząd Wojewódzki oraz Społeczną Akademię Nauk w Łodzi warsztatach, przeprowadzonych w dniach 13–14 listopada 2017 r. w Uniejowie. Roli ekspertów i moderatorów podjęli się wykładowcy wspomnianej uczelni. Dzięki metodzie FGI udało się poznać opinie uczestników warsztatów na temat jakości funkcjonowania sytemu powiadamiania ratunkowego. Przedstawione wyniki badań wymagają jednak dalszych pogłębionych prac badawczych w celu wskazania pełnych związków przyczynowo-skutkowego działania systemu.

Chcąc zbadać i ocenić system powiadamiania ratunkowego oraz określić rolę Centrów Powiadamiania Ratunkowego w tym systemie, można się odwołać do systemowego modelu organizacji zaproponowanego przez Harolda Leavitta. Jest to czteroczłonowy model, w którym wyróżniamy dwa współzależne podsystemy: społeczny, do którego można zaliczyć ludzi oraz cele i zadania oraz techniczny, złożony z dwóch elementów technologii i struktury formalnej. Model ten pokazuje, że zmiana dokonana lub wymuszona przez otoczenie w jednym elemencie pociąga za sobą zmiany w trzech pozostałych. Jakość działania organizacji będzie więc wynikową podsystemu społecznego i technicznego [Bielski 2004, ss. 43–44].

W Polsce funkcjonuje 17 Centrów Powiadamiania Ratunkowego, 16 zlokalizowanych jest w województwach, ostatnie swym obszarem działania obejmuje miasto stołeczne Warszawę. Pierwsze centra zaczęły odbierać zgłoszenia już w 2012 r., wśród nich było CPR w Łodzi [szerzej zob. Sikora-Wojtarowicz, Nienartowicz 2015, s. 224]. Operatorzy numerów alarmowych łódzkiego Centrum Powiadamiania Ratunkowego rozpoczęli swoją pracę 31 maja 2012 r. od przyjmowania zgłoszeń na nr 112 na tere-

nie Komendy Policji Miejskiej w Łodzi. Decyzja o tymczasowym umieszczeniu CPR w komendzie była autorskim rozwiązaniem Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Urzędu Wojewódzkiego w Łodzi, która pierwszym operatorom dała możliwość zdobycia doświadczenia u boku dyżurnych policjantów oraz zapoznania się z zagadnieniami będącymi w gestii merytorycznej Policji. Między 8.10 a 27.11.2013 r. operatorzy rozpoczęli odbieranie wszystkich zgłoszeń z numeru 112 z terenu województwa łódzkiego w nowej siedzibie CPR przy ulicy Pienistej, a od dnia 29.11.2015 r. rozpoczęli przekazywanie informacji o zdarzeniach za pomocą formularza elektronicznego tzw. formatki[5].

Organizacja w ujęciu systemowym

Podsystem społeczny

Czynnik ludzki stanowi istotny element każdej organizacji. We współczesnym podejściu do zarządzania zasobami ludzkimi coraz częściej podkreśla się, iż „zdobycie oraz utrzymanie jak najlepszych pracowników jest priorytetem pracodawcy, który chce odnieść sukces w strategii konkurowania na rynku" [Kowalczewski, Matwiejczuk 2008, s. 143]. W ostatnich latach obserwowane zmiany zachodzące na rynku pracy wymusiły nowe spojrzenie na znaczenie kapitału ludzkiego dla budowania różnie ujmowanego sukcesu organizacyjnego zdeterminowanego specyfiką świadczonej działalności. Pracodawcy w coraz większym stopniu rozumieją znaczenie i rolę swoich pracowników w procesie wzrostu i rozwoju. P. Borowski słusznie zauważa, że „nie tylko małe, ale i duże przedsiębiorstwa dostrzegają, że ludzie posiadają kluczowe znaczenie w działalności organizacji i przyczyniają się do odnoszenia sukcesów" [Borowski 2008, s. 20].

J. Penc stwierdza, że „w obecnych warunkach liczą się przede wszystkim wiedza i postawy pracowników oraz ich motywy, jakimi kierują się w dążeniu do lepszej pracy, zmian i postępu. Uważa się bowiem, że intelekt staje się krytycznym czynnikiem produkcji i że przedsiębiorstwa odnoszące sukcesy różnią się od mniej skutecznych przede wszystkim sposobem traktowania pracowników. Wyrażają one uznanie i przyznają premie za umiejętności współdziałania z innymi, zaangażowanie, umiejętności fachowe, uczciwość i inne postawy, a jednocześnie tworzą warunki, w których pracownicy mogą się rozwijać i zdobywać nowe umiejętności zawodowe oraz zwiększać wartość swej pracy" [Penc 2007, s. 65].

[5] Autorzy dziękują Krzysztofowi Janeckiemu, dyrektorowi Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Urzędu Wojewódzkiego w Łodzi oraz Agnieszce Łukomskiej-Dulaj, kierownik Centrum Powiadamiania Ratunkowego w Łodzi za informacje na temat działań CPR w Łodzi.

Dbałość o kapitał ludzki stanowi zatem ważny element budowania strategii zarządzania organizacją, a w szczególności zatrudnionym w niej personelem. Istotą organizacji jest to, że jest ona formą współdziałania ludzi, zmierzającego do realizacji określonego celu. W przypadku CPR elementami, od których zależna będzie jakość działania organizacji, są zarówno poziom aspiracji i oczekiwań danego operatora, jak i jego identyfikacja z nadrzędnym celem organizacji, czyli skuteczną obsługą zgłoszeń alarmowych.

Zadania CPR określa obecnie Ustawa z 22 listopada 2013 r. o systemie powiadamiania ratunkowego oraz Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 28 kwietnia 2014 r. w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego[6]. Do zadań CPR należy:

- obsługa zgłoszeń alarmowych, z wyłączeniem systemów sygnalizacji pożarowej;
- przetwarzanie, w zakresie nadanych upoważnień, w systemie teleinformatycznym danych dotyczących treści zgłoszeń alarmowych;
- wykonywanie analiz związanych z funkcjonowaniem systemu powiadamiania ratunkowego oraz tworzenie statystyk w zakresie liczby, rodzaju oraz czasów realizacji zgłoszeń alarmowych;
- współpraca oraz wymiana informacji z centrami zarządzania kryzysowego;
- wymiana informacji i danych, z wyłączeniem danych osobowych, na potrzeby analiz z Policją, Państwową Strażą Pożarną, dysponentami zespołów ratownictwa medycznego oraz podmiotami, których numery telefoniczne są obsługiwane w ramach systemu powiadamiania ratunkowego;
- podejmowanie działań mających na celu przekazanie informacji o zgłoszeniu alarmowym do podmiotów, do których zadań należy ochrona życia, zdrowia, bezpieczeństwa i porządku publicznego, mienia lub środowiska, których numery telefoniczne nie są obsługiwane w ramach systemu powiadamiania ratunkowego;
- prowadzenie działalności popularyzatorskiej w zakresie systemu powiadamiania ratunkowego.

Człon zadania (cele) jasno wskazuje, że nadrzędnym celem skutecznie działającego systemu powiadamiania ratunkowego jest poprawa bezpieczeństwa obywateli przez sprawną i właściwą obsługę zgłoszeń alarmowych. W kwestii zaspokojenia tej społecznej potrzeby istnieje zgodność zarówno po stronie organizacji, jak i jej otoczenia.

Badania jakościowe pokazały jednak, że w podsystemie społecznym występuje zjawisko fluktuacji, wpływające na poziom jakości działań CPR. Stawianym operato-

[6] Zadania te są szczegółowo opisane w następujących dokumentach: Ustawa z 22 listopada 2013 r. o systemie powiadamiania ratunkowego, Dz. U. z 2013 r. poz. 1635 z późń. zm. (tekst ujednolicony); Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 28 kwietnia 2014 r. w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego, Dz. U. z 2014 r. poz. 574.

rom wysokim wymaganiom nie towarzyszą adekwatne do tych oczekiwań wynagrodzenia, co powoduje duże zmiany w obsadzie kadrowej CPR. Rotacje pracowników, zwłaszcza odejścia doświadczonych operatorów, wpływają okresowo na zwiększenie obciążenia pozostałych liczbą przyjmowanych zgłoszeń, przyczyniając się do obniżenia jakości systemu.

Według danych dla wszystkich Centrów Powiadamiania Ratunkowego w roku 2017, w porównaniu z rokiem poprzednim faktyczny stan zatrudnienia na stanowisku operatora numeru alarmowego zmniejszył się o 57 osób. W 2016 r. zostały rozwiązane umowy o pracę z 216 operatorami, zaś w 2015 z 152 osobami. Kolejne raporty podkreślają, że główną przyczyną rotacji pracowników jest niskie wynagrodzenie [Raporty z funkcjonowania SPR 2015, 2016, 2017]. W Centrum Powiadamiania Ratunkowego w Łodzi rotacja pracowników jest również spora. 1 stycznia 2015 r. pracowało w nim 50 osób. Do 31 grudnia 2015 r. stan osobowy CPR w Łodzi wzrósł do 61 osób, przy czym w ciągu roku odeszło z pracy 11 osób, a zatrudniono 22 nowych operatorów. Obecnie stan zatrudnienia (31.12.2017) wynosi 78 osób. W ciągu 2017 r. odeszło z pracy 12 osób, zatrudniono 9 nowych[7].

Dla Centrum Powiadamiania Ratunkowego w Łodzi niezwykle istotne byłoby zmniejszenie zjawiska rotacji pracowników, zwłaszcza powstrzymanie od odejścia doświadczonych operatorów numerów alarmowych. Potrzebne jest więc wypracowanie odpowiedniego systemu motywacyjnego. Jednym ze skutecznych narzędzi budowania zaangażowania i zwiększania efektywności pracowników, prowadzącym ich do osiągnięcia celów organizacji, jak i ich własnych, jest funkcjonujący w organizacji system motywacyjny. Można go rozumieć jako „(…) układ logicznie spójnych i wzajemnie się wspierających środków motywacji, a także ich zespołów działających na zasadzie wzmocnienia i dających efekt synergetyczny, służących do kształtowania wynagrodzeń pracowników w zależności od ich wartości dla firmy, zgodnie z przyjętą strategią motywowania" [Juchnowicz 2012, s. 135]

Centrum Powiadamiania Ratunkowego należy do tych rodzajów organizacji, w których rodzaj pracy, przedmiot działań i specyfika organizacji procesów pracy wymaga zastosowania szczególnych metod i technik zarządzania zespołem pracowniczym. Odpowiedzialność za ludzi, procesy, zdarzenia, które stanowią podstawę pracy, prowadzi do zastanowienia się nad kwestią budowania odpowiedniego zaplecza realizacji pracy, dającego odpowiedni komfort psychologiczny, ale też i budujący poczucie zadowolenia z kwestii wynagradzania.

[7] Informacje uzyskane od Krzysztofa Janeckiego, dyrektora Wydziału Bezpieczeństwa i Zarządzania Kryzysowego Urzędu Wojewódzkiego w Łodzi oraz Agnieszki Łukomskiej-Dulaj, kierownik Centrum Powiadamiania Ratunkowego w Łodzi.

Od pracowników CPR wymaga się między innymi odpowiedniego poziomu:
- kwalifikacji technicznych,
- kompetencji społecznych,
- diagnozowania poziomu zdarzeń krytycznych,
- rzetelności w udzielaniu pomocy czy porad w zdarzeniach krytycznych,
- określonego stopnia autonomii w podejmowaniu decyzji.

Specyfika stanowiska operatora numerów alarmowych wymaga dbania o komfort pracownika poprzez dobrą organizację pracy i możliwość wsparcia w systemie kooperacji współpracowniczej. Ważną rolę odgrywa też aspekt budowania odpowiedniego klimatu pracy, dającego wsparcie w postaci elementów kultury organizacyjnej, np. w ramach określonych norm czy wartości pracowniczych zachęcających do większej kooperacji mimo indywidualizacji procesów pracy (np. podkreślenie roli współodpowiedzialności zespołowej za pomoc w pracy innym pracownikom poprzez system wsparcia, wymiany pomysłów rozwiązań w sytuacjach kryzysowych, zapobiegania wypaleniu zawodowemu z racji zdarzeń, z jakimi spotykają się w swojej pracy).

Indywidualizacja procesów pracy powoduje konieczność wypracowania odpowiednich systemów docenienia pracowników CPR, dających im przeświadczenie, że określony wysiłek włożony w pracę zostanie dostrzeżony i doceniony. Ważne jest, aby stwarzać możliwość realnego awansu pracowniczego będącego rezultatem włożonego w pracę własnego wysiłku. Pracownicy winni mieć możliwość własnego rozwoju w zakresie wzrostu poziomu wiedzy i doświadczenia zawodowego nie tylko w ramach recertyfikacji, ale też organizacji różnych warsztatów dotyczących budowania wiedzy na temat siebie, własnych możliwości, radzenia sobie z sytuacjami trudnymi. Daje to realne szanse na możliwość osiągnięcia poczucia zadowolenia i komfortu psychologicznego utylitarności realizowanych działań. Według Herzberga, właśnie te czynniki, nazwane przez niego motywacyjnymi, warunkują wejście w odpowiedni system motywacji, dający większe szanse na budowanie zaangażowania w proces pracy oraz zmniejszający fluktuację kadry pracowniczej – co w przypadku pracowników CPR jest również ważnym problemem [Michalik 2009, s. 378].

Drugim ważnym obszarem jest utrzymanie na odpowiednim poziomie czynników higieny. Do nich Herzberg zaliczył w głównej mierze wynagrodzenie oraz inne czynniki wsparcia finansowego skierowanego do pracowników [Michalik 2009, ss. 378–379]. Sytuacja pracowników CPR i w tym obszarze wymaga zmian. Wysokość wynagrodzenia otrzymywanego za pracę nie należy do motywujących, a w szczególności do dłuższego pozostania na stanowisku pracy. Braki w tym obszarze są widoczne i chyba o wiele pilniejsze do zmiany niż w poprzednim aspekcie.

Rzetelność, fachowość, efektywność i skuteczność pracy pracowników CPR w sytuacjach kryzysowych zależy w głównej mierze od bystrości ich umysłu, odpowiednich reakcji, wypracowania własnych sposobów radzenia w określonych zdarzeniach. Kursy, szkolenia i warsztaty będą bardzo pomocne, ale najskuteczniejszym sposobem budowania ich wiedzy i zaplecza technicznego jest ich własna praca. Doświadczenie, jakie zdobywają w realnym świecie pracy, nie jest do nauczenia w systemach kształcenia. Biografia zawodowa staje się wyznacznikiem skuteczności ich działania, a pamiętać należy, że przedmiotem i podmiotem ich pracy jest w większości przypadków życie innych. Dlatego też zmianie winien ulec sposób budowania systemu wynagrodzeń za pracę. To właśnie wysokość wynagrodzenia jest jednym z podstawowych czynników destabilizujących stałość zatrudnienia.

Rotacja pracownicza wywołana niekorzystnymi wynagrodzeniami nie wpływa pozytywnie na budowanie wysokiej klasy pracowników – merytorycznych specjalistów oczywiście w zdecydowanie większej niż obecnie liczbie. Warto wspomnieć, iż służby te w wielu wypadkach warunkują pracę i skuteczność realizacji działań przedstawicieli innych jednostek np. Policji, PSP czy ratownictwa medycznego. System wynagradzania finansowego pracowników winien być kształtowany podobnie jak w służbach zhierarchizowanych. Stałość i atrakcyjność adekwatnego wynagrodzenia oraz rozwinięty system wsparcia w postaci innych form motywacji płacowej mógłby przyczynić się do budowania stałej sieci współpracowników.

Wielość i złożoność problemów pracy pracowników CPR wpływa na konieczność ulokowania ich w systemach służb zhierarchizowanych, uwzględniając zarówno kwestię wynagrodzeń, jak i możliwość rozwoju ścieżki zawodowej ściśle określonej nawet w kwestiach proceduralnych.

Dodatkowo, mimo że zarówno operatorzy, jak i raporty z funkcjonowania SPR, wskazują jako główną przyczynę rotacji pracowników problem niskiego wynagrodzenia, warto rozważyć – jeśli taka procedura nie jest obecnie stosowana – monitoring osób odchodzących. Może pozwoli on na wychwycenie również błędów w innych obszarach, np. w systemie selekcji pracowników. Problemem może okazać się nie tylko system motywacji, ale również struktura organizacyjna lub jakieś ograniczenie technologiczne.

Relacje z otoczeniem

Równie istotne jak relacje wewnątrz organizacji, są relacje uczestników organizacji z otoczeniem, w przypadku CPR ze służbami i podmiotami ratowniczymi, a więc organizacjami silniej zhierarchizowanymi, scentralizowanymi i sformalizowanymi oraz społeczeństwem.

Podczas szkolenia operatorzy numerów alarmowych stwierdzili, że nie są traktowani jako równorzędny partner dla służb i podmiotów ratunkowych, choć to oni stanowią najistotniejszy element obecnie funkcjonującego systemu powiadamiania ratunkowego, a ich niezwykle trudna i stresująca praca nie jest doceniana przez zarówno przez służby, jak i zgłaszających zdarzenia obywateli. Najistotniejszym problemem podnoszonym na warsztatach była jakość współpracy między poszczególnymi służbami: Policja, PSP, Pogotowie Ratunkowe a pracownikami CPR. Podczas szkolenia można było zauważyć, że współpraca między operatorami numeru 112 i dyżurnymi stanowisk kierowania Policji nie jest doskonała i wymaga istotnej poprawy. Prawdopodobnie taki sam problem występuje w przypadku pozostałych służb ratowniczych (wynikało to z uwag uczestników szkolenia, podkreślali oni zwłaszcza słabą współpracę z niektórymi dysponentami ratownictwa medycznego).

Podczas szkolenia zaobserwowano również zbyt duże oczekiwania ze strony Policji wobec pracowników CPR. Funkcjonariusze Policji uważali, że operatorzy numerów alarmowych powinni wypełnić formatkę w taki sposób, aby mogła ona stanowić materiał w sprawie. Podkreślić również należy, że w ocenie samych policjantów ta sama formatka mogła być uznana za prawidłowo wypełnioną lub nieprecyzyjną (dwa zespoły policyjne omawiały tę samą formatkę dotyczącą awantury domowej, jeden z zespołów uznał przekazane przez operatora dane za wystarczające, drugi skrytykował sposób przekazu informacji o tym, że w mieszkaniu, w którym doszło do zajścia, przebywa dziecko). W trakcie dyskusji między policjantami i operatorami zauważano także pewne nieścisłości w zrozumieniu niektórych pojęć np. osoba poszkodowana, pokrzywdzona, ranna. Konieczne staje się więc wypracowanie wspólnych kodów językowych zrozumiałych przez wszystkie podmioty uczestniczące w systemie powiadamiania ratunkowego.

Powyższe uwagi skłaniają do zalecenia wprowadzenia pewnych zmian w systemie przygotowania zawodowego operatorów numeru 112. Każdy z operatorów powinien odbyć praktykę w stanowiskach kierowania poszczególnych służb ratowniczych, żeby poznać specyfikę danej służby i mieć świadomość, na co zwracać uwagę przy przyjmowaniu zgłoszenia o zdarzeniu. Podobnie obsada dyżurna stanowisk kierowania poszczególnych służb ratowniczych powinna odbyć praktyki w CPR. Taki system do-

skonalenia współpracy spowoduje większe zrozumienie i udoskonali współdziałanie między służbami. Idealnym rozwiązaniem byłoby, aby operatorami numeru 112 zostawali doświadczeni funkcjonariusze poszczególnych służb ratowniczych. Jest to bardzo ważne z uwagi na zapowiedź, że w niedługim czasie CPR przejmą pozostałe numery alarmowe. Jak istotna i przydatna jest obecność byłego funkcjonariusza Komendy Wojewódzkiej Policji w Łodzi w zespole operatorów numerów alarmowych, pokazuje przykład łódzkiego CPR. Doświadczenie oraz znajomość merytoryczna zadań i działań Policji w systemie ratownictwa Bogumiła Marony jest niezwykle pomocna i z pewnością ułatwia koordynację działań na linii CPR – Policja.

Nie tylko zbyt duże oczekiwania ze strony Policji od operatorów numerów alarmowych są przyczyną problemów komunikacyjnych. Po stronie funkcjonariuszy Policji zaobserwowano również brak odpowiedniego docenienia i szacunku do pracy wykonywanej przez operatorów numerów alarmowych. Na początku szkolenia wielu funkcjonariuszy o pracownikach CPR mówiło „oni", nie traktując ich jako partnera.

Brak odpowiedniego statusu społecznego operatorów numerów alarmowych może wynikać z niskiej świadomości społecznej o zakresie działań Centrów Powiadamiania Ratunkowego. Z dyskusji wynikało, że wiedza społeczeństwa o znaczeniu numerów alarmowych, w tym numeru 112 jest dość niska. Społeczeństwo w większości przypadków, oprócz chwili komunikacji z numerem 112, nie widzi strategicznego znaczenia tych pracowników, w wielu wypadkach nie jest świadome roli, jaką odgrywają oni w systemie zapewnienia bezpieczeństwa państwa.

O niskiej świadomości społecznej świadczy utrzymująca się wciąż na wysokim poziomie liczba zgłoszeń fałszywych, złośliwych lub niezasadnych (47% ogółu zgłoszeń w roku 2015 i 2016, a 44,6% w roku 2017) [Raporty z funkcjonowania SPR 2015, 2016, 2017]. Zgłoszenia te zostają obsłużone na poziomie CPRów i nie trafiają do służb i podmiotów ratowniczych. Warto podkreślić, że zatrzymanie takich zgłoszeń na poziomie CPR powoduje duże odciążenie służb ratowniczych, które mogą skupić się na obsłudze zgłoszeń zasadnych. Wpływ na zmniejszenie liczby zgłoszeń fałszywych może mieć przyjęta we wrześniu 2017 r. nowelizacja przepisów kodeksu wykroczeń wprowadzająca karę aresztu, ograniczenia wolności albo grzywny do 1,5 tys. zł za umyślnie i nieuzasadnione blokowanie telefonicznych numerów alarmowych[8].

Liczby wskazują, że zachodzi potrzeba uświadamiania społeczeństwa w tym zakresie. Warto podkreślić, że pracownicy Centrum Powiadamiania Ratunkowego w Łodzi

[8] Precyzuje to Ustawa z dnia 15 września 2017 r. o zmianie ustawy – Kodeks wykroczeń, Dz. U. z 2017 r. poz. 1941.

sami podejmują działania edukacyjne promujące numer 112 oraz swoją pracę w systemie powiadamiania ratunkowego[9].

Podsystem techniczny

Podsystem techniczny i związane z nim wyposażenie techniczne oraz metody i techniki postępowania wpływają na kształt struktury organizacyjnej. Technologia w znacznym stopniu determinowana jest celami organizacji, stawia też określone wymagania ludziom, wymuszając odpowiedni dobór pracowników.

W trakcie szkolenia pracownicy Centrum Powiadamiania Ratunkowego w Łodzi oraz funkcjonariusz Powiatowej Komendy Policji w Pabianicach wskazali szereg problemów utrudniających ich współpracę, wynikających z technicznych ograniczeń systemu teleinformatycznego. Podstawową kwestią są nadal występujące problemy związane z wymianą informacji między System Informatycznym Powiadamiania Ratunkowego (SI PR) a systemami SWD służb: Policji, PSP i ratownictwa medycznego.

Operatorzy zwracali uwagę na fakt trudności w przypadku potrzeby uzupełnienia formatki o dodatkowe dane. Zgłaszający zdarzenie do CPR dzwoni na numer 112, jednak w przypadku potrzeby uzyskania dodatkowych informacji od zgłaszającego już po przyjęciu zgłoszenia i rozłączenia się z numerem 112, gdy operator oddzwania na numer zgłaszającego, temu ostatniemu wyświetla się numer stacjonarny CPR, który jest 9-cyfrowy, a nie 112, na który było zgłoszenie. Nie każdy odbiera wtedy telefon, jeżeli numer jest nieznany. Ten problem powinien być rozwiązany w taki sposób, aby zgłaszającemu wyświetlał się numer 112.

Poważnym problemem dla pracowników CPR jest brak wiedzy o efektach podejmowanych interwencji. Operatorzy numeru alarmowego podkreślali, że nie są informowani, w jaki sposób zakończyło się zdarzenie zgłoszone do Policji. Dla nich wiedza o tym jest niezwykle istotna z kilku powodów. Po pierwsze, staje się szczególnie ważna w przypadku poważnego zdarzenia, o zaistnieniu którego informują CPR liczni zgłaszający, w celu uniknięcia sporządzania kolejnej formatki i przesłania jej ponownie do Policji. Rozwiązaniem powinna być modyfikacja formatki w taki sposób, aby operator CPR miał pogląd, jakie działania podjęto lub też dyżurny Policji powinien informować CPR o podjętych działaniach. Ułatwiłoby to operatorom CPR pracę. Przy kolejnych zgłoszeniach w tej samej sprawie zgłaszający byłby informowany, że Policja podjęła już działania. Kwestia wiedzy na temat podjętych przez służbę działań jest

[9] Łódzki CPR co roku organizuje obchody Europejskiego Dnia Numeru Alarmowego 112 oraz spotkania z dziećmi i młodzieżą, zapraszając do swojej siedziby przedszkola, szkoły podstawowe, gimnazja i licea, http://lodzkie.eu/page/4070,centrum-powiadamiania-ratunkowego.html.

również ważna dla samych operatorów, którzy nie pozostają obojętni wobec zdarzeń, które są im zgłaszane i chcieliby wiedzieć, czy dzięki ich pracy akcja ratownicza zakończyła się sukcesem. Informacja zwrotna o podjętych np. przez Policję działaniach jest także istotna przy analizowaniu przebiegu rozmów operatorów ze zgłaszającymi podczas szkoleń i oceny wewnętrznej operatorów oraz pozwala na lepszą ocenę skuteczności podejmowanych przez pracowników CPR działań. W wielu przypadkach komunikat zwrotny ze strony Policji lub innej służby mógłby stanowić swoisty motywator do dalszej pracy dla operatorów.

Jednym z elementów szkolenia było omawianie formatek przesyłanych przez operatorów numerów alarmowych do dyżurnych Policji. Problem stanowiło już źródło niektórych formatek. Funkcjonariusze Policji nie wiedzieli, że w przypadku części przesłanych im zgłoszeń osobą odpowiedzialną za sporządzenie formatki nie był operator numeru alarmowego, ale dyspozytor ratownictwa medycznego lub dyżurny stanowiska kierowania PSP. Wynikało to z niezwracania uwagi na identyfikator formatki, zawierający informację o sporządzającym. Na marginesie, podmiotom uczestniczącym w systemie powiadamiania ratunkowego powinien zostać zagwarantowany spójny i dobrze zintegrowany system informatyczny, przekaz i uzupełnianie informacji ułatwiłby z pewnością identyczny wygląd formatki – obecnie różnice w rozmieszczeniu danych na formularzach widocznych na ekranie operatora i dyżurnego Policji powodują niepotrzebną stratę cennego czasu. Odwołując się do modelu Leavitta, w podsystemie technicznym można zaobserwować wyraźną interakcję podsystemu z otoczeniem. Pojawiające się niespójności w interfejsie komunikacyjnym, którego zadaniem jest zintegrowanie SIPR z SWD służb, na bieżąco wymuszą pewne zmiany, mające wpływ na pozostałe człony systemu. Przy zakładanej większej liczbie zadań po stronie CPR nie jest to rozwiązanie zbyt korzystne.

Podsumowanie

Podsumowując, zaznaczyć należy, że sama organizacja – CPR – jest organizacją w procesie zmiany. Liczne przekształcenia w koncepcji budowy systemu powiadamiania ratunkowego w ostatnich latach – odejście od systemu operatorsko-dyspozytorskiego, opartego na powiatowych strukturach Państwowej Straży Pożarnej i wprowadzenie systemu operatorskiego opóźniły wprowadzenie jednolitego dla całego kraju systemu powiadamiania ratunkowego [Soloch 2015, s. 3n]. Dodatkowo, obecnie CPR nadal obsługują tylko część zgłoszeń alarmowych – te, które wpływają na numer 112. Wyjątek stanowi jedynie CPR w Katowicach, który w listopadzie 2017 r. przejął także obsługę numeru 997. Docelowo jednak operatorzy numerów alarmowych mają

przejąć obsługę wszystkich zgłoszeń. Zasadne jest więc ograniczenie występującego w CPR zjawiska fluktuacji oraz poprawienie współpracy organizacji z otoczeniem.

Odnosząc się do dyskusji i uwag uczestników warsztatów, za istotną kwestię, konieczną do rozwiązania, należy uznać problem systemu motywacyjnego, zwłaszcza wynagrodzeń oraz sprawę statusu – pozycji społecznej operatorów numerów alarmowych. Pracownicy Centrum Powiadamiania Ratunkowego chcą i muszą być traktowani jako równorzędny element systemowy, a nie jedynie jako „gorsze" ogniwo, bo tylko zbierające i przekazujące informacje o zdarzeniu, nieuczestniczące w działaniach ratowniczych. Istotne jest więc, aby ich wysiłek włożony w pracę – w zdobycie istotnych dla przebiegu akcji ratunkowej informacji często od osoby, z którą z różnych przyczyn komunikacja jest utrudniona (osoba ranna, w szoku, dziecko, osoba nietrzeźwa lub pod wpływem środków odurzających, cudzoziemiec) – został doceniona przez innych uczestników systemu.

Jednocześnie należy stwierdzić, że idea warsztatów się sprawdziła i powinno się je kontynuować w kolejnych latach, włączając w nie także pozostałe służby i podmioty ratownictwa. Na warsztatach obie strony dokonały wspólnej oceny technicznych narzędzi komunikacji (ograniczenia wynikające z wad technicznych formatki), wskazały obszary problemowe, nad którymi muszą wspólnie popracować, a co najistotniejsze spotkanie warsztatowe pozwoliło na nawiązanie osobistych relacji między dwoma kluczowymi „trybami" w systemie powiadamiania ratunkowego.

Obecnie operatorzy łódzkiego CPR obsługują zgłoszenia z numeru 112, jednak już niedługo przejmą zgłoszenia wpływające na numer alarmowy Policji 997, a docelowo mają przyjmować zgłoszenia z pozostałych numerów alarmowych, w tym 998 i 999. Przyjęta w systemie powiadamiania ratunkowego zasada wzajemnej zastępowalności centrów w razie miejscowej awarii systemu teleinformatycznego bądź jego przeciążenia sprawia, że zasięg działań CPR, zwłaszcza w przypadkach wystąpienia sytuacji kryzysowej, nie ogranicza się tylko do jednego województwa. Planowane przejmowanie kolejnych numerów alarmowych wymaga już teraz odpowiedniego przygotowania samych operatorów oraz usprawnienia współpracy w ramach systemu powiadamiania ratunkowego.

Służby – Policja i PSP powinny też dostrzec pewne korzyści z odciążenia dyżurnego dzięki zatrzymaniu na poziomie CPR zgłoszeń fałszywych bądź niezasadnych. Korzyścią dla służb może być również obsługa zgłoszeń obcojęzycznych oraz kojarzenie zgłoszeń podobnych.

Bibliografia

Bielski M. (2004), *Podstawy teorii organizacji i zarządzania*, Wydawnictwo C. H. Beck, wyd. 2 rozszerzone, Warszawa.

Borowski P. (2008), *Funkcja personalna w przedsiębiorstwach należących do sektorów silnie regulowanych,* [w:] E. Jędrych, A. Pietras, A. Stankiewicz (red.) *Funkcja personalna w zmieniającej się organizacji,* Media Press, Łódź.

Juchnowicz M. (2012), *Zaangażowanie pracowników: sposoby oceny i motywowania*, PWE, Warszawa.

Kowalczewski W., Matwiejczuk W. (2008), *Zarządzanie organizacjami w teorii i praktyce*, Difin, Warszawa.

Michalik K. (2009), *Typologia czynników motywacji,* „Zeszyty Naukowe Małopolskiej Wyższej Szkoły Ekonomicznej w Tarnowie", Tarnów, t. 2., nr 2 (13); cyt. za: http://zn.mwse.edu.pl/ebooki/13-2/373-387.pdf, s. 6, dostęp: 10 marca 2017.

Penc J., (2007), *Nowoczesne kierowanie ludźmi*, Difin, Warszawa.

Sikora-Wojtarowicz K., Nienartowicz A. (2015), *Funkcjonowanie systemu powiadamiania ratunkowego w Polsce. Założenia i praktyka*, „Rocznik Bezpieczeństwa Międzynarodowego", vol. 9, nr 2.

Soloch P. (2015), *O systemie powiadamiania ratunkowego w 16 miesięcy po uchwaleniu ustawy*, Analiza Instytutu Sobieskiego nr 75, kwiecień.

Akty prawne:

Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 28 kwietnia 2014 r. w sprawie organizacji i funkcjonowania centrów powiadamiania ratunkowego, Dz. U. z 2014 r. poz. 574.

Ustawa z 22 listopada 2013 r. o systemie powiadamiania ratunkowego, Dz. U. z 2013 r. poz. 1635 z późn. zm. (tekst ujednolicony).

Ustawa z dnia 15 września 2017 r. o zmianie ustawy – Kodeks wykroczeń, Dz. U. z 2017 r. poz. 1941.

Raporty:

Raport z funkcjonowania systemu powiadamiania ratunkowego w 2015 r.

Raport z funkcjonowania systemu powiadamiania ratunkowego w 2016 r.

Raport z funkcjonowania systemu powiadamiania ratunkowego w 2017 r.

Wszystkie raporty dostępne na stronie Ministerstwa Spraw Wewnętrznych i Administracji https://bip.mswia.gov.pl/bip/system-powiadamiania-ra.

Strony internetowe:

Centrum Powiadamiania Ratunkowego w Łodzi: http://lodzkie.eu/page/4070,centrum-powiadamiania-ratunkowego.html.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **67–80**

Michał Stępiński[1]
Społeczna Akademia Nauk

System budowania kompetencji dowódczych w Policji jako istotny czynnik wpływający na gotowość formacji do zapewnienia bezpieczeństwa obywateli w przypadku wystąpienia zdarzenia kryzysowego

A system of Building Commanding Capacity in the Police as an Important Factor Influencing the Readiness of the Formation to Ensure the Security of Citizens in the Event of a Crisis

Abstract: Police as the formation responsible for the security of the citizen maintain the system of building the competence of commanders in crisis situations. The most important competence is decision-making in crisis situations. The training system is tailored to your needs and allows you to acquire and maintain the necessary specialist skills in the command area.
Key words: commander, training, competence, emergency response activities, Police.

Wstęp

Policja jako największa formacja mundurowa w Polsce[2] realizuje bardzo szeroki zakres zadań w obszarze bezpieczeństwa, wynikających z Ustawy o Policji [Dz.U. 1990 Nr 30 poz. 179 z późniejszymi zmianami], takich jak:

[1] michstepinski@gmail.com

- ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra;
- ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania;
- inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi;
- prowadzenie działań kontrterrorystycznych w rozumieniu Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych [Dz. U. 2016r., poz. 904];
- wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców;
- nadzór nad specjalistycznymi uzbrojonymi formacjami ochronnymi w zakresie określonym w odrębnych przepisach;
- kontrola przestrzegania przepisów porządkowych i administracyjnych związanych z działalnością publiczną lub obowiązujących w miejscach publicznych;
- współdziałanie z policjami innych państw oraz ich organizacjami międzynarodowymi, a także z organami i instytucjami Unii Europejskiej na podstawie umów i porozumień międzynarodowych oraz odrębnych przepisów;
- gromadzenie, przetwarzanie i przekazywanie informacji kryminalnych;
- prowadzenie zbiorów danych zawierających informacje gromadzone przez uprawnione organy o odciskach linii papilarnych osób, niezidentyfikowanych śladach linii papilarnych z miejsc przestępstw oraz o wynikach analizy kwasu deoksyrybonukleinowego (DNA).

Powyższy katalog obejmuje w szczególności zadania, w przypadku których sprawność i skuteczność działania ma bezpośredni wpływ nie tylko na bezpieczeństwo publiczne, ale przede wszystkim na fizyczne bezpieczeństwo ludzi. Świadomość profesjonalnej pomocy, jaką obywatele mogą uzyskać w sytuacji zagrożenia życia lub zdrowia, jest znaczącym czynnikiem wpływającym na ich poczucie bezpieczeństwa. Obszar ten dotyczy działań Policji związanych z wystąpieniem zdarzeń kryzysowych. Zgonie z zapisami Zarządzenia nr 23 Komendanta Głównego Policji z dnia 24 września 2014 r. w sprawie metod i form przygotowania i realizacji działań Policji w związku ze zdarzeniami kryzysowymi [Dz.Urz. KGP z 2014r. poz. 65] zdarzenie kryzysowe to zda-

[2] Stan na 1 stycznia 2017 r. – Policjanci: Stan etatowy – 102 309, Stan zatrudnienia – 99 924 (oraz 49 na stanowiskach finansowanych przez samorządy lokalne), Korpus Służby Cywilnej: stan etatowy – 12 173,5 liczba zatrudnionych osób – 11 902, pozostali pracownicy cywilni: stan etatowy – 12 540,61 liczba zatrudnionych osób – 13 153, http://www.info.policja.pl/inf/organizacja/stan-zatrudnienia/81505,Stan-zatrudnienia-na-dzien-1-stycznia-2017-roku.html, dostęp: 04.10.2017 r.

rzenie spowodowane bezprawnymi zamachami mogącymi sprowadzić niebezpieczeństwo dla życia lub zdrowia ludzi albo mienia, charakteryzujące się możliwością utraty kontroli przez podmiot odpowiedzialny za stan bezpieczeństwa i porządku publicznego w miejscu zdarzenia albo eskalacji zagrożenia w stopniu wymagającym użycia do ochrony bezpieczeństwa i porządku publicznego policjantów zorganizowanych w oddziały lub pododdziały zwarte. Przytoczona definicja wskazuje, że działania Policji, związane z zaistnieniem zdarzenia kryzysowego, są pewnym szczególnym rodzajem działań, wymagającym od osób odpowiedzialnych za ich prowadzenie szczególnych kompetencji. M. Wojakowska przywołuje kompetencje menedżerów bezpieczeństwa [2017, s. 37], uznając, że są one niezbędne w następujących obszarach:

- umiejętności techniczne (zawodowe) – określające zdolność posługiwania się narzędziami, technologią. Są one niezbędne do wykonywania i rozumienia zadań, za które się odpowiada;
- umiejętności społeczne (interpersonalne) – przejawiające się jako zdolność do współpracy i nawiązywania kontaktów z innymi ludźmi, rozumienia ich i motywowania do pracy;
- umiejętności koncepcyjne – określane jako zdolność do abstrakcyjnego myślenia; intelektualną zdolność do koordynowania i integrowania wszystkich interesów firmy i działalności organizacji.

Wskazuje ona jednocześnie, ze w przypadku menedżerów bezpieczeństwa cechy te powinny oscylować wokół odporności na stres i krytykę oraz wytrwałości i determinacji. Wydaje się jednak, że dla potrzeb niniejszych rozważań bardziej właściwe jest stanowisko, zgodnie z którym kluczową kompetencją dowódczą jest umiejętność podejmowania decyzji [Stępiński 2015, s. 102]. Biorąc pod uwagę powyższe, celem niniejszej publikacji jest ocena istniejącego w Policji systemu szkolenia i doskonalenia zawodowego pod kontem możliwości budowania i utrzymania przez policjantów kompetencji dowódczych, umożliwiających sprawne i skuteczne realizowanie działań w przypadku wystąpienia zdarzenia kryzysowego. Wobec tego we wskazanym zakresie analizie poddane zostaną programy kursów oferowanych przez szkoły policji. W oparciu o przeprowadzoną analizę, autor spróbuje ocenić, czy powyższe rozwiązanie można określić mianem systemu budowania kompetencji dowódczych. Na potrzeby kompletności rozważań w przedmiotowym obszarze w pierwszej części przedstawiona zostanie występująca w Policji zależność pomiędzy kierowaniem i dowodzeniem, źródła kompetencji oraz różnice w uwarunkowaniu podejmowania decyzji w tych dwóch obszarach. W drugiej części przeanalizowane zostaną programy szkoleń, kursów i warsztatów realizowanych w obszarze dowodzenia w Policji, pod kątem ich kompletności i wystarczalności dla zbudowania kompetencji dowódczych.

Kompetencje w obszarze kierowania i dowodzenia w Policji

W literaturze wielu dziedzin nauki można znaleźć definicje kompetencji. Nie ma jednej uznanej za uniwersalną. Z tego powodu na potrzeby niniejszych rozważań przyjęto definicje kompetencji, z której wynika, że są to:

- zakres uprawnień urzędu lub urzędnika do zajmowania się określonymi sprawami i podejmowania decyzji z nimi związanych;
- zakres czyjejś wiedzy, umiejętności i doświadczenia;
- zdolność komórek do reagowania na określone bodźce[3].

Pozwoli to wykazać zależności zachodzące pomiędzy kierowaniem a dowodzeniem w Policji. Jak wskazano we wstępie, dowodzenie w przypadku Policji realizowane jest jedynie w warunkach określanych mianem kryzysowych. Codzienna działalność tej formacji podlega kierowaniu zgodnie z zapisami Zarządzenia nr 1041 Komendanta Głównego Policji z dnia 28 września 2007 r. w sprawie szczegółowych zasad organizacji i zakresu działania komend, komisariatów i innych jednostek organizacyjnych Policji [Dz.Urz KGP z 2013 r., poz. 50, tekst jednolity], na postawie którego w organizacji Policji wyróżnione zostały stanowiska kierownicze, którymi są:

- kierownik jednostki Policji i jego zastępcy;
- kierownik komórki i jego zastępcy.

Osoby zajmujące te stanowiska odpowiedzialne są za funkcjonowanie podlegających im jednostek i komórek, odgrywając rolę przełożonych w rozumieniu Zarządzenia nr 30 Komendanta Głównego Policji z dnia 16 grudnia 2013 r. w sprawie funkcjonowania organizacji hierarchicznej w Policji [Dz.Urz. z 2013 r., poz. 99]. Zgodnie z tym przepisem przełożony to policjant lub pracownik Policji uprawniony z racji zajmowanego stanowiska albo na podstawie odrębnego przepisu lub upoważnienia do kierowania przebiegiem służby lub pracy innego policjanta lub pracownika Policji. W przytoczonych regulacjach prawnych, wpływających na organizację Policji, nie ma mowy o dowódcy czy dowodzeniu. Występują natomiast kierownik i kierowanie. Taki stan rzeczy doprowadził do sytuacji, w której kierowanie w Policji jest obszarem jedynie bardzo luźno związanym z dowodzeniem. Wynika to między innymi z faktu, że kierownik jednostki Policji to niejednokrotnie organ administracji, odpowiedzialny również za cały obszar funkcjonowania podległego mu urzędu, jakim jest Komenda (Główna, Wojewódzka, Powiatowa lub Rejonowa) Policji, w tym za zarządzanie środkami publicznymi, niezbędnymi do funkcjonowania podległej mu jednostki. Środki te otrzymywane są z budżetu centralnego, jak również w coraz większym zakresie pozyskiwane od samorządów terytorialnych. Taki stan rzeczy spowodował, że osoby te

[3] Definicja podana za: http://sjp.pwn.pl/slowniki/kompetencje.html, dostęp 04.10.2017 r.

skoncentrowały się na działaniach w tym obszarze i w efekcie bardziej utożsamiają się z rolą menedżera niż dowódcy. W codziennej działalności Policji efekt ten pogłębia jeszcze wymaganie ze strony wyższych przełożonych, radzenia sobie z działalnością jednostek przy coraz mniejszych środkach finansowych oraz oczekiwanie pozyskiwania coraz większych kwot spoza budżetu centralnego. Z powyższego wynika, że decyzje podejmowane w zakresie kierowania w Policji dotyczą odmiennego obszaru decyzyjnego niż decyzje dowódcze, a co za tym idzie, posiadanie kompetencji kierowniczych nie zawsze jest równoznaczne z posiadaniem kompetencji dowódczych. Poza wymienionymi uwarunkowaniami wskazać należy na całkowicie odmienną sytuację operacyjną, w której przychodzi podejmować decyzje kierownikom i dowódcom. Kierownik działa w warunkach normalnego funkcjonowania organizacji, dowódca w warunkach kryzysowych. Do najważniejszych cech sytuacji kryzysowej w przypadku Policji zaliczyć należy:

- bezpośrednie zagrożenie życia i zdrowia ludzi,
- nieprzewidywalność,
- presję czasu,
- utratę lub groźbę utraty kontroli nad sytuacją operacyjną,
- poważne zaburzenia funkcjonowania systemu informacji [Stępiński 2015, s. 99].

W oparciu na tym założeniu opracowany został model dowódcy idealnego, na który składają się kluczowa kompetencja, którą jest podejmowanie decyzji oraz jej źródła, co daje następujący obraz:

- potrafi podejmować decyzje nawet w najtrudniejszych warunkach;
- posiada doświadczenie w działaniach w sytuacjach kryzysowych;
- posiada wiedzę specjalistyczną związaną z działaniami w warunkach kryzysowych, w tym znajomość przepisów regulujących tę materię;
- jest odporny na stres;
- posiada zaufanie do podwładnych;
- jest odważny[4].

Działania Policji w związku ze zdarzeniem kryzysowym mogą być prowadzone w ramach interwencji, akcji lub operacji policyjnej. Operacja jako najwyższa forma zorganizowania działań może być dzielona na podoperacje o różnym profilu działań. Szczególnym rodzajem podoperacji jest podoperacja antyterrorystyczna, w ramach której prowadzone będą bojowe działania kontrterrorystyczne. Pomimo znacznej odmienności warunków, w jakich przychodzi działać dowódcy, od warunków, w ja-

[4] Badania przeprowadzone przez autora wśród dowódców Policji w latach 2011–2012 w ramach rozprawy doktorskiej nt. „Uwarunkowania podejmowania decyzji w sytuacjach kryzysowych na przykładzie Policji" Politechnika Łódzka.

kich działa kierownik, katalog osób mogących pełnić najważniejsze funkcje dowódców, w zasadzie wypełniają osoby nabywające takie uprawnienie jedynie w oparciu na pełnionej przez siebie funkcji kierownika jednostki organizacyjnej Policji. Są to odpowiednio:

1. W przypadku operacji policyjnej:
– Komendant Główny Policji,
– Zastępca Komendanta Głównego Policji,
– Komendant Wojewódzki Policji,
– Zastępca Komendanta Wojewódzkiego Policji,
2. W przypadku zastępcy dowódcy operacji:
– zastępcy Komendanta Głównego Policji,
– Komendant Wojewódzki Policji,
– Zastępca Komendanta Wojewódzkiego Policji
3. W przypadku podoperacji antyterrorystycznej:
– dowódca jednostki antyterrorystycznej Policji,
– zastępca dowódcy jednostki antyterrorystycznej Policji

Rozwiązanie takie daje wymienionym policjantom podstawę formalną do odgrywania roli dowódcy działań. Wydaje się, że w wielu przypadkach do sprawnej i skutecznej realizacji procesu dowodzenia może się to jednak okazać niewystarczające. Do pełnienia funkcji dowódcy prawo mają również oficerowie Policji niebędący kierownikami jednostek organizacyjnych Policji, muszą spełniać oni jednak ściśle określone wymagania formalne, którymi są:

– odbycie przeszkolenia w zakresie dowodzenia,
– posiadanie predyspozycji,
– posiadanie doświadczenia w zakresie dowodzenia (w przypadku podoperacji antyterrorystycznej w zakresie dowodzenia bojowymi działaniami kontrterrorystycznymi).

Tylko w przypadku tej grupy policjantów określone zostały konkretne cechy, jakie muszą charakteryzować dowódcę. W przypadku pierwszej grupy założono *a priori,* że sam fakt bycia kierownikiem jednostki organizacyjnej Policji jest wystarczającą przesłanką, aby być dobrym dowódcą. Błędność takiego założenia wielokrotnie pokazały analizy prowadzonych działań. Zapis mówiący o potrzebie posiadania przeszkolenia przez funkcjonariuszy niepełniących funkcji kierowników jednostki stworzył potrzebę wprowadzenia oferty szkoleniowej w zakresie dowodzenia działaniami Policji, prowadzonymi w związku ze zdarzeniami kryzysowymi. W efekcie w 2008 roku rozpoczęto realizację kursów dla dowódców, w których z założenia mieli uczestniczyć jedynie funkcjonariusze niezajmujący stanowisk kierowniczych. Już pierwsze edycje pokazały

jednak, że zainteresowanie tą ofertą jest znacznie większe, a potrzeby szkoleniowe zgłaszane były również przez policjantów, którzy mogli pełnić funkcję dowódców bez tego przeszkolenia. Taki stan rzeczy dał impuls do ewolucyjnego rozwoju tego rozwiązania i oferty dydaktycznej w tym zakresie.

System budowania kompetencji dowódczych w Policji

Nie wszystkie wymienione wcześniej źródła kompetencji są w równej mierze możliwe do wykształcenia w procesie szkolenia lub doskonalenia zawodowego. Cechy takie jak odporność na stres czy odwaga mogą być jednak wzmacniane dzięki właściwie skonstruowanemu procesowi dydaktycznemu. Doświadczenie w dziedzinie, w której dowódcy przychodzi podejmować decyzje, może być uzupełniane na bazie przeżyć własnych, analizy i wyciągania wniosków z działań innych oraz udziału w grach decyzyjnych, prowadzonych w oparciu o scenariusze konstruowane na podstawie przeprowadzonych działań. Wiedza specjalistyczna związana z działaniami w warunkach kryzysowych, w tym znajomość przepisów regulujących te materię, może zostać nabyta i utrwalona podczas udziału w różnych formach kształcenia. Wskazuje to na znaczenie właściwie skonstruowanego procesu dydaktycznego dla nabywania i utrwalania źródeł kompetencji dowódczych. Szkolenie zawodowe i doskonalenie zawodowe w Policji reguluje Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 19 czerwca 2007 r., w sprawie szczegółowych warunków odbywania szkoleń zawodowych oraz doskonalenia zawodowego [Dz.Urz. KGP z 2007 r. poz. 877]. Szkolenie zawodowe przybiera formę:

- szkolenia zawodowego podstawowego,
- szkolenia zawodowego dla absolwentów szkół wyższych.

Pierwsze z nich prowadzi się w celu przygotowania policjantów do wykonywania podstawowych zadań służbowych na stanowiskach, na których są wymagane kwalifikacje zawodowe podstawowe. Drugie prowadzone jest w celu przygotowania policjantów do wykonywania zadań służbowych na stanowiskach, na których są wymagane kwalifikacje zawodowe wyższe i w efekcie umożliwia ono uzyskanie stopnia oficerskiego. Ze względu na swój ogólny charakter te formy kształcenia nie zakładają nabycia specjalistycznych kompetencji dowódczych. Z tego powodu analizowany system realizowany jest w ramach doskonalenia zawodowego, które w Policji prowadzone jest w celu nabywania, aktualizowania, rozszerzania oraz pogłębiania wiedzy i umiejętności zawodowych policjanta, wymaganych przy wykonywaniu przez niego zadań i czynności służbowych, a także uzyskaniu przez niego dodatkowych upraw-

nień, w tym uprawnień instruktorskich. Doskonalenie zawodowe może być prowadzone w formie:

- doskonalenia centralnego – przez szkoły policyjne i Wyższą Szkołę Policji;
- doskonalenia lokalnego – przez jednostki organizacyjne Policji lub komórki organizacyjne tych jednostek;
- doskonalenia zewnętrznego – przez podmioty pozapolicyjne.

Doskonalenie centralne z kolei może być realizowane w formie:

- kursów specjalistycznych;
- innych niż kursy przedsięwzięć.

Umiejętności w obszarze dowodzenia uznane zostały za tak ważne dla Policji, że podstawową formą ich nabywania są kursy specjalistyczne realizowane w ramach doskonalenia centralnego, przez wskazaną komórkę Wyższej Szkoły Policji. Zajęcia prowadzą wykładowcy WSPol, posiadający – poza wiedzą teoretyczną – niezbędne doświadczenie w zakresie dowodzenia oraz nauczyciele stowarzyszeni, którymi są najbardziej doświadczeni funkcjonariusze, realizujący w ramach swoich obowiązków służbowych na co dzień zadania związane z dowodzeniem działaniami w jednostkach terenowych Policji. W 2017 roku zakończył się etap tworzenia całego systemu kursów specjalistycznych w zakresie dowodzenia działaniami Policji, prowadzonymi w związku ze zdarzeniami kryzysowymi, w tym działaniami antyterrorystycznymi i działaniami kontrterrorystycznymi. System ten obejmuje następującą ofertę dydaktyczną:

1) Kurs specjalistyczny dla policjantów komórek organizacyjnych policji właściwych w sprawach sztabowych [Decyzja nr 399 Komendanta Głównego Policji z dnia 19 czerwca 2008 r. w sprawie programu kursu specjalistycznego dla policjantów komórek organizacyjnych Policji właściwych w sprawach sztabowych (Dz.Urz. KGP z 2008 r., poz. 79)];
2) Kurs specjalistyczny dla dowódców akcji i operacji policyjnych [Decyzja nr 882 Komendanta Głównego Policji z dnia 5 grudnia 2007 r. w sprawie programu kursu specjalistycznego dla dowódców operacji policyjnych (Dz. Urz. KGP z 2008 r., poz. 195), uchylona Decyzją Nr 173 Komendanta Głównego Policji z dnia 22 maja 2015 r. w sprawie programu nauczania na kursie specjalistycznym dla dowódców akcji i operacji policyjnych (Dz.Urz. KGP z 2015 r., poz. 35)];
3) Kurs specjalistyczny dla dowódców podoperacji antyterrorystycznych prowadzonych w ramach operacji policyjnych [Decyzja nr 301 Komendanta Głównego Policji z dnia 23 września 2015 r. programu kursu specjalistyczny dla dowódców podoperacji antyterrorystycznych prowadzonych w ramach operacji policyjnych (Dz.Urz. KGP z 2015r., poz. 73)];

4) Kurs specjalistyczny dla kierujących działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym [Decyzja Nr 125 Komendanta Głównego Policji z dnia 30 maja 2017 r. w sprawie programu nauczania na kursie specjalistycznym dla kierujących działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym (Dz.Urz. KGP z 2017r., poz. 35)].

Powyższe kursy zapewniają możliwości kształcenia dla dowódców wszystkich szczebli dowodzenia w Policji oraz funkcjonariuszy odpowiedzialnych za funkcjonowanie komórek sztabowych. Uznając, że właściwy proces dowodzenia możliwy jest do przeprowadzenia jedynie dzięki wykwalifikowanej komórce analityczno-doradczej, jaką jest sztab dowódcy działań [Struniawski 2017, s. 181] pierwszy element systemu stanowi kurs specjalistyczny dla policjantów komórek organizacyjnych policji właściwych w sprawach sztabowych. Przeznaczony jest on dla policjantów, którzy są odpowiedzialni za działanie sztabu dowódcy operacji. Trwa 10 dni szkoleniowych, w trakcie których realizowane są zajęcia z pracy sztabowej, dzięki czemu kursanci nabywają podstawową wiedzę z zakresu:

- przygotowania i planowania działań sztabowych;
- realizacji działań sztabowych;
- analizy i oceny działań sztabowych.

W efekcie budowane są kompetencje kadry wspierającej proces dowodzenia. Dla oficerów niezajmujących stanowisk kierowniczych ukończenie tego kursu jest warunkiem niezbędnym dla ubiegania się o skierowanie na kurs drugiego stopnia, czyli dla dowódców akcji i operacji policyjnych. Kurs ten przeznaczony jest dla oficerów Policji, przewidzianych do pełnienia funkcji dowódcy lub zastępcy dowódcy akcji lub operacji (podoperacji) policyjnej, którzy ukończyli kurs specjalistyczny dla policjantów komórek organizacyjnych Policji właściwych w sprawach sztabowych lub oficerów Policji zajmujących stanowiska kierowników jednostek organizacyjnych Policji i komórek organizacyjnych KGP, KWP, KSP oraz ich zastępców. Trwa on 10 dni szkoleniowych, w trakcie których realizowane są takie zagadnienia, jak:

1) Wybrane zagadnienia dowodzenia w Policji;
2) Przygotowanie akcji lub operacji policyjnej;
3) Realizacja akcji lub operacji policyjnej;
4) Podsumowanie i ocena akcji lub operacji policyjnej.

Poza częścią wykładową, na kursie prowadzone są gry decyzyjne, pomagające nabywać umiejętności podejmowania decyzji w sytuacjach kryzysowych. Do tego celu wykorzystywany jest symulator działań policji w sytuacjach kryzysowych, działający w WSPol w Szczytnie. Jest to zaawansowane narzędzie dydaktyczne, pozwalające wiernie odtworzyć warunki prowadzenia operacji policyjnej na terenie Warszawy.

Trzeci etap, kurs specjalistyczny dla dowódców podoperacji antyterrorystycznych prowadzonych w ramach operacji policyjnych, został wprowadzony w 2015 roku. Powodem wprowadzenia go w życie było uregulowanie przepisów w zakresie dowodzenie działaniami bojowymi w Policji. Zgodnie z ogólnymi regulacjami dowódca podoperacji antyterrorystycznej powinien, poza predyspozycjami i doświadczeniem w zakresie dowodzenia działaniami antyterrorystycznymi, posiadać również przeszkolenie w zakresie dowodzenia działaniami kontrterrorystycznymi. Kurs przeznaczony jest dla oficerów Policji z jednostek i komórek antyterrorystycznych Policji, przewidzianych do pełnienia funkcji dowódcy lub zastępcy dowódcy podoperacji antyterrorystycznej lub funkcjonariuszy zajmujących stanowiska dyrektorów Biura Operacji Antyterrorystycznych Komendy Głównej Policji, dowódców i kierowników jednostek i komórek antyterrorystycznych Policji oraz ich zastępców. Trwa on 5 dni szkoleniowych, z czego dwa pierwsze przeznaczone są na zajęcia teoretyczne, a trzy kolejne na ćwiczenia. W ramach zajęć teoretycznych omawiane są następujące tematy:

- Psychologiczne aspekty podejmowania decyzji;
- Dowodzenie w Policji;
- Specyfika działań jednostek i komórek antyterrorystycznych Policji w związku z akcjami lub operacjami policyjnymi;
- Przepisy regulujące funkcjonowanie jednostek i komórek antyterrorystycznych Policji;
- Organizacja podoperacji AT;
- Współdziałanie z innymi podmiotami policyjnymi i pozapolicyjnymi;
- Planowanie podoperacji AT;
- Dokumentacja działań.

W ramach ćwiczeń prowadzona jest gra decyzyjna, zgodnie ze scenariuszem przygotowanym w oparciu o realizowane działania bojowe. Scenariusz gry przedstawiany jest w czasie rzeczywistym, tak samo rozpatrywany jest czas działań planowanych i podejmowanych przez uczestników kursu. Na potrzeby utrwalania i doskonalenia wiedzy nabytej w ramach kursu od 2017 roku w WSPol w Szczytnie realizowane są warsztaty dowodzenia działaniami bojowymi w ramach innych przedsięwzięć doskonalenia centralnego. W warsztatach tych biorą udział absolwenci kursu specjalistycznego dla dowódców podoperacji antyterrorystycznych prowadzonych w ramach operacji policyjnych. W ramach warsztatów policjanci biorą udział w całodobowej grze decyzyjnej, wymagającej zaplanowania, przygotowania, przeprowadzenia i oceny działań antyterrorystycznych. Ostatnim etapem skierowanym dla dowódców najwyższego szczebla dowodzenia w Policji, jest kurs specjalistyczny dla kierujących działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym.

Został on wprowadzony w 2017 roku. Przepisy ustawy antyterrorystycznej nałożyły na Policję odpowiedzialność za kierowanie całością działań prowadzonych na miejscu zdarzenia o charakterze terrorystycznym. Zwrot „kierowanie" został użyty przez ustawodawcę z pełną świadomością, ponieważ dotyczy on odpowiedzialności za działanie wszystkich służb i podmiotów biorących udział w działaniach, w tym cywilnych, których nie obejmuje dowodzenie. *De facto* funkcja kierującego działaniami pełniona będzie przez wskazanego dowódcę działań Policji. Uznając wagę tego przedsięwzięcia, Komendant Główny Policji zgłosił realizację kursu specjalistycznego dla kierujących działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym jako wkład Policji w realizację założeń „Narodowego Programu Antyterrorystycznego na lata 2014–2019". Kurs jest kierowany do funkcjonariuszy Policji, spełniających wymagania do pełnienia funkcji dowódcy operacji policyjnej, zastępcy dowódcy operacji policyjnej lub podoperacji antyterrorystycznej realizowanej w ramach operacji policyjnej na podstawie przepisów w sprawie metod i form przygotowania i realizacji działań Policji w związku ze zdarzeniami kryzysowymi, którzy będą mogli pełnić funkcję kierującego działaniami antyterrorystycznymi. Kurs trwa 5 dni szkoleniowych, z czego dwa pierwsze są przeznaczone na zajęcia teoretyczne, trzy kolejne na ćwiczenia. W ramach zajęć teoretycznych omawiane są następujące tematy:

- Psychologiczne aspekty podejmowania decyzji;
- Dowodzenie w Policji;
- Przepisy regulujące prowadzenie działań antyterrorystycznych na miejscu zdarzenia o charakterze terrorystycznym;
- Przepisy regulujące działanie oraz specyfikę działań pododdziałów antyterrorystycznych Policji realizujących działania kontrterrorystyczne;
- Wykorzystanie negocjacji policyjnych w działaniach antyterrorystycznych;
- Organizacja działań antyterrorystycznych na miejscu zdarzenia o charakterze terrorystycznym;
- Kierowanie podmiotami pozapolicyjnymi, biorącymi udział w działaniach antyterrorystycznych na miejscu zdarzenia o charakterze terrorystycznym;
- Siły Zbrojne Rzeczypospolitej Polskiej w działaniach kontrterrorystycznych;
- Specjalne użycie broni w działaniach kontrterrorystycznych;
- Analiza ryzyka w działaniach antyterrorystycznych;
- Planowanie działań antyterrorystycznych na miejscu zdarzenia o charakterze terrorystycznym, w tym działań kontrterrorystycznych;

W ramach ćwiczeń realizowane są dwa moduły:

- Kierowanie działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym;
- Analiza i ocena działań antyterrorystycznych na miejscu zdarzenia o charakterze terrorystycznym, w tym działań kontrterrorystycznych.

W 2017 roku odbyły się dwie edycje przedmiotowego kursu, w których wzięli udział Komendanci i Zastępcy Komendantów Wojewódzkich Policji z wszystkich garnizonów. Kurs ten ma być realizowany cyklicznie i ma objąć wszystkich funkcjonariuszy przewidzianych do pełnienia funkcji kierującego działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym.

Podsumowanie

Wyniki przeprowadzonych w Policji badań wskazują, że policjanci oczekują od swoich dowódców autorytetu opartego na kompetencjach, zamiast tradycyjnego autorytaryzmu wynikającego z uprawnień formalnych [por. Olszewski 2010 r., ss. 142–153]. Uznając słuszność takiego stanowiska, podkreślić należy, że przeanalizowane programy kursów specjalistycznych pozwalają przyjąć, że dowodzenie w Policji uznane zostało za umiejętność ekspercką, która stanowi znaczącą wartość dla organizacji. Stworzony system centralnego doskonalenia zawodowego nastawiony jest na wykształcenie kluczowej kompetencji dowódczej, czyli umiejętności podejmowania decyzji, umożliwia zdobycie atrybutów stanowiących źródła tej kompetencji oraz minimalizuje groźbę dezaktualizacji kompetencji osób objętych tym systemem. Potwierdzeniem tych wniosków są wyniki badań ankietowych, przeprowadzonych wśród uczestników kursów dla dowódców podoperacji antyterrorystycznych prowadzonych w ramach operacji policyjnych. Dobór treści programowych i ich logiczny układ zostały zaaprobowane przez wszystkich uczestników badania. Podobnie zgodzili się oni, że przedstawiana na zajęciach problematyka może być wysoce użyteczna przy wykonywaniu obowiązków służbowych. Również bardzo wysoko ocenili (w pięciostopniowej skali) zdobytą w trakcie kursu wiedzę – średnia ocen 4,83 oraz umiejętności zawodowe – średnia ocen 4,65[5]. Prowadzone kursy skierowane są do dowódców wszystkich szczebli dowodzenia oraz funkcjonariuszy struktur sztabowych. Cykliczność omawianych przedsięwzięć daje możliwość nabycia oraz utrzymania na niezbędnym poziomie specjalistycznej wiedzy i umiejętności przez całą grupę docelową. Biorąc pod uwagę

[5] Dane uzyskane na podstawie ankiet ewaluacyjnych wypełnianych przez 30 uczestników kursów dla dowódców podoperacji antyterrorystycznych, prowadzonych w ramach operacji policyjnych, zrealizowanych w WSPol w 2016 roku.

powyższe, przyjąć należy, że w Policji istnieje system pozwalający nabywać i utrzymać specjalistyczne kompetencje wymagane od dowódców. Jednocześnie pamiętać należy, że weryfikacja tych kompetencji następuje jedynie w prawdziwym działaniu i musi być to uwzględniane przez wszystkich uczestników przedstawionego procesu dydaktycznego, tak słuchaczy, jak i wykładowców.

Bibliografia

Olszewski G. (2010), *Obszary wykorzystania kompetencji w zarządzaniu zasobami ludzkimi w jednostce Policji*, „Przegląd Policyjny", 3(99), Szczytno.

Stępiński M. (2015), *Teoretyczne i prawno-organizacyjne uwarunkowania decyzji dowódczych w Policji,* WSPol w Szczytnie.

Struniawski J. (2017), *Sztaby w Policji, organizacja i funkcjonowanie,* WSPol Szczytno.

Wojakowska M. (2017), *Wpływ kompetencji menedżerskich na jakość zarządzania bezpieczeństwem,* [w:] J. Prońko, B. Wiśniewski (red.), *Zarządzanie instytucjami publicznymi i prywatnymi w kontekście niepewności zagrożeń kryzysów i ryzyka,* WSPol Szczytno.

Stępiński M. (2012), *Uwarunkowania podejmowania decyzji w sytuacjach kryzysowych, na przykładzie Policji,* rozprawa doktorska, Politechnika Łódzka.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 19 czerwca 2007 r., w sprawie szczegółowych warunków odbywania szkoleń zawodowych oraz doskonalenia zawodowego [Dz.Urz. KGP z 2007 r. poz. 877].

Zarządzenie nr 23 Komendanta Głównego Policji z dnia 24 września 2014 r. w sprawie metod i form przygotowania i realizacji działań Policji w związku ze zdarzeniami kryzysowymi [Dz.Urz. KGP z 2014 r. poz. 65].

Zarządzenie nr 1041 Komendanta Głównego Policji z dnia 28 września 2007 r. w sprawie szczegółowych zasad organizacji i zakresu działania komend, komisariatów i innych jednostek organizacyjnych Policji [Dz.Urz KGP z 2013 r., poz. 50, tekst jednolity].

Zarządzenie nr 30 Komendanta Głównego Policji z dnia 16 grudnia 2013 r. w sprawie funkcjonowania organizacji hierarchicznej w Policji [Dz.Urz. z 2013 r., poz. 99].

Decyzja nr 399 Komendanta Głównego Policji z dnia 19 czerwca 2008 r. w sprawie programu kursu specjalistycznego dla policjantów komórek organizacyjnych Policji właściwych w sprawach sztabowych [Dz.Urz. KGP z 2008 r., poz. 79].

Decyzja nr 882 Komendanta Głównego Policji z dnia 5 grudnia 2007 r. w sprawie programu kursu specjalistycznego dla dowódców operacji policyjnych [Dz. Urz. KGP z 2008 r., poz. 195], uchylona Decyzją Nr 173 Komendanta Głównego Policji z dnia 22 maja 2015 r. w sprawie programu nauczania na kursie specjalistycznym dla dowódców akcji i operacji policyjnych [Dz.Urz. KGP z 2015 r., poz. 35].

Decyzja nr 301 Komendanta Głównego Policji z dnia 23 września 2015 r. programu kursu specjalistyczny dla dowódców podoperacji antyterrorystycznych prowadzonych w ramach operacji policyjnych [Dz.Urz. KGP z 201r., poz. 73].

Decyzja Nr 125 Komendanta Głównego Policji z dnia 30 maja 2017 r. w sprawie programu nauczania na kursie specjalistycznym dla kierujących działaniami antyterrorystycznymi na miejscu zdarzenia o charakterze terrorystycznym [Dz.Urz. KGP z 2017 r., poz. 35].

http://www.info.policja.pl/inf/organizacja/stan-zatrudnienia/81505,Stan-zatrudnienia-na-dzien-1-stycznia-2017-roku.html, dostęp 04.10.2017 r.

http://sjp.pwn.pl/slowniki/kompetencje.html, dostęp 04.10.2017 r.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **81–92**

Tomasz Bąk[1]
Wyższa Szkoła Informatyki i Zarządzania w Rzeszowie

Ustawa antyterrorystyczna jako podstawa funkcjonowania systemu antyterrorystycznego Polski w systemie zarządzania kryzysowego

The Anti-terrorist Act as the Base of Functioning of the Anti-terrorist System of Poland in the System of the Crisis Management

Abstract: In the presented article basic elements of the anti-terrorist system of Poland were characterised. Special attention was paid to tasks which these elements are fulfilling. The Anti-terrorist Act which was introduced into the Polish legal system in 2016 was regarded as one of important components. A substantial role of this act was emphasized in the functioning of the anti-terrorist system of Poland and its contribution to the counteraction for terrorist threats.
Key words: anti-terrorist act, anti-terrorist system, system of crisis management, security.

Wstęp

Wydarzenia, które miały miejsce w ostatnich latach, a nastąpiły po 11 września 2001 r., sprawiły, że zaczęto mówić o współczesnym terroryzmie – współczesnym, bo zupełnie innym od tego, z którym mieliśmy do czynienia dotychczas – służącym głównie walce z cywilizacją Zachodu i będącym domeną organizacji o podłożu islamskim.
Nie ulega wątpliwości, że aby przeciwstawić się temu zjawisku, należy tworzyć efektywne systemy antyterrorystyczne. Ich budowa opiera się na czterech podstawowych elementach. Są to:

[1] tbak@wsiz.rzeszow.pl

- rozwiązania ustawowe,
- struktury i jednostki przeznaczone do walki z terroryzmem,
- współpraca międzynarodowa,
- formy i metody walki z terroryzmem.

Aby skutecznie walczyć z terroryzmem, należy przede wszystkim rozpoznać zjawisko i wytypować grupę, która zamierza przygotować zamach. Następnie trzeba określić jej potencjalne cele i możliwości wykonawcze. Jeśli dojdzie do zidentyfikowania takiej grupy lub do zdarzenia o charakterze terrorystycznym, muszą istnieć skuteczne środki prawne pozwalające odpowiednim służbom na sprawne działanie, a także efektywny system zwalczania terrorystów przez specjalistyczne formacje. Ważna jest likwidacja lub minimalizacja skutków dokonanego aktu terrorystycznego. Fundamentalną rolę odgrywa tu system zarządzania kryzysowego zorganizowany w oparciu o administrację rządową i samorządową, w tym system ratowniczy, obejmujący wszelkie służby ratownicze, obronę cywilną oraz Siły Zbrojne z nowo utworzonymi Wojskami Obrony Terytorialnej.

Głównym celem niniejszej publikacji jest przedstawienie założeń nowej ustawy antyterrorystycznej w aspekcie organizacji i funkcjonowania systemu antyterrorystycznego Polski [Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Przedstawione i omówione zostanie zastosowanie powyższej ustawy w całym systemie zarządzania kryzysowego RP.

Rozwiązania ustawowe

W Polsce po 2001 r., tak jak w innych państwach europejskich, pod wpływem szokujących zdarzeń z 11 września, zgodnie z polityką Unii Europejskiej, rozpoczęto budowę systemu antyterrorystycznego. Zaczęto wprowadzać do różnych aktów prawnych zapisy dotyczące reagowania na zagrożenia terrorystyczne, ale także już w tych wcześniej ustanowionych znaleźć można odniesienia dotyczące walki z terroryzmem.
Odniesienia takie zawierają m.in. następujące akty prawne:

- Ustawa z dnia 6 kwietnia1990 r. o Policji [1990],
- Ustawa z dnia 12 października 1990 r. o Straży Granicznej [1990],
- Ustawa z dnia 12 października 1990 r. o ochronie granicy państwowej [1990],
- Nowelizacja Ustawy z dnia 6 czerwca 1997 r. Kodeks karny,
- Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego [1997],
- Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe [1997],
- Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych [1999],
- Ustawa z dnia 16 marca 2001 r. o Biurze Ochrony Rządu [2001],

- Ustawa z dnia 6 lipca 2001 r. o gromadzeniu i przetwarzaniu informacji kryminalnych oraz o Krajowym Systemie Informacyjnym [2001],
- Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych [2001],
- Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej [2002],
- Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu [2002],
- Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym [2002],
- Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze [2002],
- Ustawa z dnia 29 lipca 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej [2002],
- Ustawa z dnia 27 września 2002 r. zmieniająca Ustawę z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu [2002],
- Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary [2002],
- Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym [2006],
- Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego [2006],
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym [2007],
- Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej [1967],
- Zarządzenie Komendanta Głównego Policji nr 3/96 z dnia 5 lutego 1996 r. w sprawie użycia pododdziałów antyterrorystycznych w przypadku zamachu terrorystycznego [1996].

Bardzo istotnym dokumentem w zakresie zabezpieczenia antyterrorystycznego stał się Narodowy Program Antyterrorystyczny Rzeczypospolitej Polskiej. Początkowo stworzono go na lata 2012–2016, ale nie został wprowadzony w życie. Wkrótce, bo na początku 2014 r., opracowano taki program na lata 2014–2019 i jest on obecnie wdrażany [Narodowy Program Antyterrorystyczny na lata 2014–2019 2014].

Należy jednak wyraźnie podkreślić, iż zapewnienie bezpieczeństwa antyterrorystycznego kraju jest rozumiane jako proces ciągły, niezmiennie istotny z punktu widzenia funkcjonowania Państwa, a zatem podejmowane w tym zakresie działania nie są ograniczone datą zakończenia programu, a zmieniające się uwarunkowania motywują do ciągłej dbałości o właściwą adaptację i doskonalenie wdrożonych rozwiązań.

Głównym celem Narodowego Programu Antyterrorystycznego jest wzmocnienie systemu antyterrorystycznego. Jego realizacji służą cztery, odpowiadające kolejnym fazom zarządzania kryzysowego, cele szczegółowe, a mianowicie:

- poprawa zdolności do zapobiegania zagrożeniom o charakterze terrorystycznym,
- wzmocnienie przygotowania służb i instytucji na wypadek wystąpienia zdarzeń o charakterze terrorystycznym,
- zwiększenie zdolności do reagowania w przypadku wystąpienia zdarzeń o charakterze terrorystycznym,
- poprawa skuteczności w zakresie odtwarzania wykorzystanych sił i środków oraz udoskonalania istniejących procedur postępowania w przypadku zagrożeń o charakterze terrorystycznym [Narodowy Program Antyterrorystyczny na lata 2014–2019 2014, ss. 33–35].

W polskim ustawodawstwie przepisy dotyczące terroryzmu znajdują się również w kodeksie karnym oraz wiążących Polskę konwencjach międzynarodowych.

Ustawa antyterrorystyczna

Przez ostatnie lata w Polsce podejmowano różnego rodzaju wysiłki w celu usprawnienia działań antyterrorystycznych. Dostrzeżono także potrzebę wzmocnienia narzędzi służących przeciwdziałaniu i zwalczaniu zagrożeń terrorystycznych, jak również reagowaniu na takie zagrożenia. Jedną z najważniejszych spraw stało się przygotowanie naczelnej ustawy dotyczącej walki z terroryzmem, dlatego też powołano specjalny zespół, który miał stworzyć ustawę antyterrorystyczną.

Jej głównym celem miała być przede wszystkim poprawa efektywności współdziałania służb odpowiedzialnych za bezpieczeństwo państwa i jego obywateli. Ustawa faktycznie zawiera wiele rozwiązań prawnych umożliwiających służbom nie tylko wzmocnienie mechanizmów koordynacji prowadzonych działań, ale też skuteczne i szybkie reagowanie już w przypadku zaistnienia samego podejrzenia o prowadzenie działalności terrorystycznej [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Po kilku latach wysiłków, 2 lipca 2016 r. weszła w życie ustawa o działaniach antyterrorystycznych, której zasadniczym celem – zgodnie z uzasadnieniem – jest zwiększenie efektywności polskiego systemu antyterrorystycznego, a tym samym zwiększenie bezpieczeństwa wszystkich obywateli RP wskutek: wzmocnienia koordynacji działań służb i doprecyzowania ich zadań, zapewnienia mechanizmów reagowania adekwatnych do rodzaju występujących zagrożeń, możliwości skuteczniejszego działania w przypadku podejrzenia przestępstwa o charakterze terrorystycznym, w tym w zakresie postępowania przygotowawczego, dostosowania przepisów karnych do

nowych typów zagrożeń o charakterze terrorystycznym [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Wiele rozwiązań, które wprowadza ustawa o działaniach antyterrorystycznych to zupełna nowość, nie były one bowiem stosowane do tej pory na terenie Rzeczypospolitej Polskiej przez organy ścigania oraz służby specjalne, natomiast zakres innych został rozszerzony i przystosowany do realnych potrzeb w zakresie poprawy bezpieczeństwa.

Ustawa z 10 czerwca 2016 r. wprowadza centralizację odpowiedzialności za zapobieganie i zwalczanie terroryzmu. Głównym ciężarem walki z terroryzmem w Polsce została obarczona Agencja Bezpieczeństwa Wewnętrznego (ABW) [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Ustawa spowodowała, że szef Agencji Bezpieczeństwa Wewnętrznego jest jedyną osobą w Rzeczypospolitej Polskiej, która może samodzielnie – bez konieczności uzyskiwania zgody jakiegokolwiek podmiotu – zdecydować o zastosowaniu środków operacyjno-rozpoznawczych (np. o założeniu podsłuchu, zainstalowaniu ukrytej kamery w domu czy zapoznawaniu się z treścią wiadomości mailowych). Pozostałe służby nadal są zobowiązane każdorazowo uzyskiwać zgodę sądu na dokonywanie działań operacyjno-rozpoznawczych. Ustawa wprowadziła jednak trzy ograniczenia wobec omawianego uprawnienia szefa ABW: podmiotowe (omawiane środki mogą być stosowane tylko wobec określonych kategorii cudzoziemców), przedmiotowe (środki te można stosować wyłącznie w przypadkach zapobiegania i zwalczania przestępstw o charakterze terrorystycznym) i temporalne (środki, o których mowa mogą być stosowane nie dłużej niż przez 3 miesiące, z możliwością przedłużenia) [Zubrzycki, Jałoszynski, Babiński 2016, ss. 262 i dalej].

Ustawa zdecydowanie rozszerzyła dotychczasowe uprawnienia Agencji Bezpieczeństwa Wewnętrznego. Agencja otrzymała m.in. szeroki dostęp do danych i informacji zgromadzonych w rejestrach i ewidencjach państwowych, prowadzonych przez inne organy, służby i podmioty, w tym także samorządy, a także dostęp do obrazu z monitoringu umieszczonego w miejscach publicznych (np. stadiony czy dworce i centra handlowe) [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Funkcjonariusze ABW będą mogli także zajrzeć do informacji i danych znajdujących się w rejestrach i ewidencjach prowadzonych przez służby specjalne (Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego i Centralne Biuro Antykorupcyjne), ministrów kierujących działaniami administracji rządowej, Urząd ds. Cudzoziemców, Urząd Komunikacji Elektronicznej, Urząd Lotnictwa Cywilnego, Państwową Agencję Atomistyki, Zakład Ubezpieczeń Społecznych, Kasę Rolniczego Ubezpieczenia Społecznego, Komisję Nadzoru Finansowego, Głównego

Geodetę Kraju, jednostki samorządu terytorialnego i Prokuratora Generalnego oraz jednostki organizacyjne podległe lub nadzorowane przez te podmioty. Zapisy ustawy spowodowały więc, że ABW posiadać będzie olbrzymią liczbę baz danych tworzonych przez: Policję, Straż Graniczną, Biuro Ochrony Rządu, Państwową Straż Pożarną, Służbę Celną, Generalnego Inspektora Informacji Finansowej, Generalnego Inspektora Kontroli Skarbowej, Żandarmerię Wojskową, Rządowe Centrum Bezpieczeństwa, jak również dostęp do baz: banków, SKOK-ów czy firm ubezpieczeniowych oraz innych baz danych [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Aby właściwie realizować zadania mające na celu zapobieganie zdarzeniom o charakterze terrorystycznym, ABW, zgodnie z nową ustawą, prowadzi wykaz informacji o wielu grupach osób, a mianowicie o:

1) osobach podejmujących działalność na rzecz organizacji terrorystycznych lub organizacji związanych z działalnością terrorystyczną lub członkach tych organizacji, a także poszukiwanych osobach prowadzących działalność o charakterze terrorystycznym, wobec których w Rzeczypospolitej Polskiej zostało wydane zarządzenie o zatrzymaniu, poszukiwaniu lub postanowienie o poszukiwaniu listem gończym oraz o poszukiwanych na podstawie europejskiego nakazu aresztowania;
2) osobach, wobec których istnieje uzasadnione podejrzenie, że mogą prowadzić działania zmierzające do popełnienia przestępstwa o charakterze terrorystycznym, w tym o osobach stanowiących zagrożenie dla bezpieczeństwa lotnictwa cywilnego;
3) osobach uczestniczących w szkoleniach terrorystycznych lub podejmujących podróż w celu popełnienia przestępstwa o charakterze terrorystycznym [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Oczywiście gromadzenie tych danych powinno odbywać się z zachowaniem wymogów dotyczących informacji niejawnych i ochrony danych osobowych.

Aby koordynacja reakcji na wszelkie zdarzenia o charakterze terrorystycznym lub możliwość ich wystąpienia była właściwa, ustawa przewiduje, że to właśnie szef ABW odpowiada za taką koordynację. Dotyczy to głównie:

- czynności operacyjno-rozpoznawczych podejmowanych przez Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego, Centralne Biuro Antykorupcyjne, a także: Policję, Straż Graniczną, Generalnego Inspektora Kontroli Skarbowej i Żandarmerię Wojskową;
- czynności obserwowania i rejestrowania obrazu zdarzeń w miejscach publicznych oraz dźwięku towarzyszącego tym zdarzeniom podejmowane, za pomocą środków technicznych, przez funkcjonariuszy celnych [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Zgodnie z nowymi uprawnieniami, szef ABW, w celu rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym, może zarządzić wobec osoby niebędącej obywatelem Rzeczypospolitej Polskiej, a w stosunku, do której istnieje obawa, że może ona zajmować się działalnością terrorystyczną, niejawne prowadzenie, nie dłużej niż przez 3 miesiące, czynności polegających na:

- uzyskiwaniu i utrwalaniu treści rozmów prowadzonych za pomocą środków technicznych, w tym za pomocą sieci telekomunikacyjnych;
- uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne;
- uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej;
- uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, a także w systemach informatycznych i teleinformatycznych;
- uzyskiwaniu dostępu do przesyłek i kontroli ich zawartości [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Jedną z najistotniejszych nowości jest fakt, że w celu ograniczenia skutków zamachów ustawa wprowadza powszechnie obowiązujący, czterostopniowy, system alarmowy na wypadek zagrożeń terrorystycznych oraz zagrożeń terrorystycznych w cyberprzestrzeni. Jest on dostosowany do wymogów obowiązujących w NATO [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

System alarmowy funkcjonował dotychczas w ramach polskiego prawa na poziomie kolejnych zarządzeń prezesa Rady Ministrów w sprawie przedsięwzięć i procedur systemu zarządzania kryzysowego, mających swoje umocowanie w ustawie o zarządzaniu kryzysowym [Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym 2007]. Umieszczenie systemu stopni alarmowych w przepisach prawa powszechnie obowiązującego umożliwiło jego powiązanie z procesem decyzyjnym i realizacją działań nie tylko w sferze administracji publicznej, lecz także w innych sferach życia społecznego.

W art. 16 ust. 1 ustawy o działaniach antyterrorystycznych, czytamy, że stopnie alarmowe mogą być wprowadzane, zmieniane i odwoływane w drodze zarządzenia, w zależności od rodzaju zagrożenia zdarzeniem terrorystycznym, przez prezesa Rady Ministrów, po zasięgnięciu opinii ministra właściwego do spraw wewnętrznych i szefa ABW. Z kolei w sytuacjach niecierpiących zwłoki stopnie alarmowe mogą być wprowadzane, po zasięgnięciu opinii szefa ABW, przez ministra właściwego do spraw wewnętrznych, który informuje o tym niezwłocznie prezesa Rady Ministrów [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. W efekcie, w porównaniu

do uprzednio obowiązującego porządku prawnego, na gruncie krajowym nastąpiło ograniczenie podmiotowe w zakresie kompetencji wprowadzania stopni alarmowych i jej przeniesienie wyłącznie na poziom odpowiedzialności prezesa Rady Ministrów, ministra właściwego do spraw wewnętrznych i szefa ABW (dotychczas, w ograniczonym podmiotowo i obszarowo zakresie, kompetencja ta przysługiwała również wojewodom, ministrom i kierownikom urzędów centralnych).

W sytuacji, gdy siły policyjne nie są wystarczające do prowadzenia działań antyterrorystycznych przewiduje się, że siły zbrojne RP mogą być wykorzystane do udzielenia wsparcia. W przypadku użycia takiego wsparcia nowa ustawa w art. 22 przewiduje, że oddziały i pododdziały Sił Zbrojnych Rzeczypospolitej Polskiej mogą użyć i wykorzystać środki przymusu bezpośredniego i broń palną na zasadach przewidzianych dla żołnierzy Żandarmerii Wojskowej [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Natomiast oddziały i pododdziały Wojsk Specjalnych mogą w tego rodzaju przypadkach użyć i wykorzystać w działaniach kontrterrorystycznych środki przymusu bezpośredniego i broń palną w sposób przewidziany w art. 3 ust. 2a ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej, tj. z uwzględnieniem konieczności i celu wykonania tych zadań, w sposób adekwatny do zagrożenia oraz w granicach zasad określonych w wiążących Rzeczypospolitą Polską ratyfikowanych umowach międzynarodowych oraz międzynarodowym prawie zwyczajowym [Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej 1967].

W przypadku użycia oddziałów lub pododdziałów Sił Zbrojnych RP w trybie art. 18 ustawy o Policji żołnierzom kierowanym do pomocy oddziałom i pododdziałom Policji przysługują, w zakresie niezbędnym do wykonywania ich zadań, wobec wszystkich osób, uprawnienia policjantów określone w art. 15 i art. 16 tej ustawy, a korzystanie z tych uprawnień następuje na zasadach i w trybie określonym dla policjantów [Ustawa z dnia 6 kwietnia 1990 r. o Policji 1990].

Dodatkowo ustawa antyterrorystyczna reguluje możliwość użycia broni palnej przeciwko osobie dokonującej zamachu nawet, jeśli skutkiem tego będzie śmierć lub bezpośrednie zagrożenie życia lub zdrowia zamachowca [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Kolejną i istotną nowością wprowadzoną przez ustawę jest obowiązek rejestracji posiadaczy prepaidowych kart SIM [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Obowiązkowa rejestracja danych właścicieli przedpłaconych kart SIM nie jest tak naprawdę niczym nowym. Zasadę taką stosuje się w wielu krajach Europy i świata. Ułatwia ona niewątpliwie pracę organom śledczym, nawet w przypadku rejestracji takiej karty przy pomocy podstawionych osób lub za pomocą podrobionych czy skradzionych dokumentów.

Biorąc pod uwagę fakt, że łatwy, obecnie, dostęp do bezzałogowych statków powietrznych (dronów), spowodował znaczny wzrost zagrożeń będących następstwem ich użycia przez terrorystów, w ustawie wprowadzono unormowania pozwalające na likwidację takich środków ataku terrorystycznego wskutek zestrzelenia czy też przejęcia nad nimi kontroli [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Ustawa o działaniach antyterrorystycznych przyznaje również ministrowi spraw wewnętrznych i administracji nowe kompetencje. Na wniosek szefa ABW albo SKW ma on możliwość wydawania decyzji o natychmiastowym wydaleniu z kraju cudzoziemca mogącego prowadzić działalność terrorystyczną lub szpiegowską lub podejrzewanego o popełnienie jednego z tych przestępstw [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Nowa ustawa wprowadza również zmiany, które pozwalają prokuratorowi na podjęcie decyzji o przeszukaniu pomieszczeń i innych miejsc na wskazanym obszarze. Ustawa umożliwia realizację czynności zatrzymania i przeszukania osób i miejsc o dowolnej porze [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Bardzo istotnym i usprawniającym możliwość stosowania sankcji karnych, jest zapis art. 26 tej ustawy, z którego wynika, że w przypadku podejrzenia popełnienia przestępstwa o charakterze terrorystycznym, jeżeli wymaga tego dobro postępowania przygotowawczego, postanowienie o przedstawieniu zarzutów można sporządzić na podstawie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Pozwala to odpowiednio wcześnie rozpocząć pracę z osobą, wobec której istnieją przesłanki pozaprocesowe świadczące o powiązaniach z terroryzmem (w charakterze osoby podejrzanej). W przypadku wydania i ogłoszenia postanowienia o przedstawieniu zarzutów sąd, na wniosek prokuratora, może zastosować tymczasowe aresztowanie na okres nieprzekraczający 14 dni. Samoistną przesłanką zastosowania tymczasowego aresztowania jest uprawdopodobnienie popełnienia, usiłowania popełnienia lub przygotowania do popełnienia przestępstwa o charakterze terrorystycznym.

Ważnym rozwiązaniem wprowadzonym przez ustawę o działaniach antyterrorystycznych jest obowiązek zapewnienia ochrony przez specjalistyczne uzbrojone formacje ochronne lub zapewnienia odpowiedniego zabezpieczenia technicznego w odniesieniu do obiektów infrastruktury krytycznej, w tym obiektów budowlanych, urządzeń, instalacji i usług kluczowych dla bezpieczeństwa państwa i jego obywateli oraz służących zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców [Ustawa z 10 czerwca 2016 r. o działa-

niach antyterrorystycznych 2016]. Co więcej, poszerzony został zakres obowiązkowych uzgodnień w odniesieniu do planów ochrony obiektów umieszczonych w prowadzonych przez wojewodów ewidencjach obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie, znajdujących się na terenie danego województwa. Kierownik jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami umieszczonymi w prowadzonych przez wojewodów ewidencjach obszarów, obiektów i urządzeń podlegających obowiązkowej ochronie (albo upoważniona przez niego osoba) jest obowiązany nie tylko, jak uprzednio, uzgadniać plan ich ochrony z właściwym terytorialnie komendantem wojewódzkim Policji, lecz również – w zakresie zagrożeń o charakterze terrorystycznym, z właściwym terytorialnie dyrektorem delegatury ABW. Wspomniane plany ochrony powinny posiadać tzw. załącznik antyterrorystyczny [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Zakończenie

Wprowadzona ustawa o działaniach antyterrorystycznych, w wyniku centralizacji odpowiedzialności za zapobieganie i zwalczanie terroryzmu, pozwala na właściwą realizację zadań mających na celu przeciwdziałanie współczesnym zagrożeniom terrorystycznym [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Zwiększa również możliwość współpracy między podmiotami zaangażowanymi w działania na rzecz zwalczania terroryzmu. Przyjęte w ustawie rozwiązania pozwalają na podejmowanie skutecznych działań już w przypadku podejrzenia przestępstwa o charakterze terrorystycznym oraz zapewniają odpowiednie mechanizmy reagowania. Pozwalają także na podjęcie służby w Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służbie Kontrwywiadu i Wywiadu Wojskowego, osobom posiadającym, oprócz polskiego obywatelstwa, również obywatelstwo innego kraju [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Z pewnością przyczyni się to do zwiększenia skuteczności rozpoznania środowisk radykalnych, w tym międzynarodowych organizacji terrorystycznych, działających poza terenem naszego kraju. W artykule przedstawiono najważniejsze i najistotniejsze rozwiązania, które wprowadzone zostały w nowej ustawie.

Należy z mocą podkreślić, że uchwalenie ustawy o działaniach antyterrorystycznych jest krokiem poczynionym we właściwym kierunku. Głównym założeniem ustawy o działaniach antyterrorystycznych jest wprowadzenie szczególnych rozwiązań w przypadku pojawienia się przesłanek świadczących o podejrzeniu planowania lub usiłowania dokonania aktu terrorystycznego, jak również monitorowania tego zjawiska [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016]. Ustawa o działaniach antyterrorystycznych z całą pewnością pozwala na doskonałą koordyna-

cję realizacji działań rozpoznawczych podejmowanych przez poszczególne organy, jak również w sposób oczywisty określa rolę szefa Agencji Bezpieczeństwa Wewnętrznego, który odpowiada za zapobieganie zdarzeniom o charakterze terrorystycznym oraz koordynuje czynności analityczno-informacyjne podejmowane przez służby specjalne [Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016].

Kształt ustawy jest niewątpliwie efektem wiedzy i doświadczeń ekspertów w zakresie działań antyterrorystycznych i kontrterrorystycznych oraz oczekiwań związanych z tym aktem prawnym.

Obecnie terroryzm jest jednym z głównych zagrożeń dla życia i zdrowia ludzkiego oraz elementów infrastruktury krytycznej, a ustawa o działaniach antyterrorystycznych uwzględnia rozwiązania istniejące m.in. w państwach Europy Zachodniej oraz wiedzę i doświadczenia polskich funkcjonariuszy, co czyni ją niewątpliwie cennym aktem prawnym, wpływającym na poprawę bezpieczeństwa Rzeczypospolitej Polskiej i jej obywateli.

Należy również zwrócić uwagę na fakt, że ustawa antyterrorystyczna może wzbudzać wiele kontrowersji, chociażby w związku z możliwością ograniczania niektórych praw i wolności obywateli. Trzeba jednak mieć świadomość, że chcąc żyć w bezpiecznym państwie, musimy zrezygnować, zwłaszcza w dzisiejszych czasach, z określonych praw i wolności na rzecz zwiększenia bezpieczeństwa.

Bardzo istotne jest powiązanie ustawy o działaniach antyterrorystycznych z ustawą z 2007 r. o zarządzaniu kryzysowym, co w założeniu zapewnić ma m.in. spójność wewnętrznych procedur reagowania, wynikających z obu regulacji, w przypadku zaistnienia przesłanek je uruchamiających [Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych 2016, Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym 2007].

Przedstawione w artykule fakty dowodzą, że w naszym kraju podjęto wiele działań mających na celu stworzenie dobrze działającego systemu antyterrorystycznego i zapewnienie jego odpowiedniego funkcjonowania w ramach systemu zarządzania kryzysowego. Jest to jednak wciąż zadanie otwarte, a działania te wymagają ciągłej ewolucji i doskonalenia.

Bibliografia

Narodowy Program Antyterrorystyczny na lata 2014–2019 (2014), M. P. z 2014 r. poz. 1218.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (2016), Dz. U. z 2016 r. poz. 904.

Ustawa z dnia 6 kwietnia1990 r. o Policji (1990), Dz. U. z 1990 r. Nr 30 poz. 179.

Ustawa z dnia 12 października 1990 r. o Straży Granicznej (1990), Dz. U. z 1990 r. Nr 78, poz. 462.
Ustawa z dnia 12 października 1990 r. o ochronie granicy państwowej (1990), Dz. U. z 1990 r. Nr 78 poz. 461.
Ustawa z dnia 6 czerwca 1997 r.- Kodeks postępowania karnego (1997), Dz. U z 1997 r. Nr 89 poz. 555.
Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (1997), Dz. U. z 1997 r. Nr 140 poz. 939.
Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (1999), Dz. U. z 1999 r. Nr 11 poz. 95.
Ustawa z dnia 16 marca 2001 r. o Biurze Ochrony Rządu (2001), Dz. U. z 2001 r. Nr 27 poz. 298.
Ustawa z dnia 6 lipca 2001 r. o gromadzeniu i przetwarzaniu informacji kryminalnych oraz o Krajowym Systemie Informacyjnym (2001), Dz. U. z 2001 r. Nr 110 poz. 1189.
Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (2001), Dz. U. z 2001 r. Nr 123 poz. 1353.
Ustawa z dnia 18 kwietnia 2002 r. o stanie klęski żywiołowej (2002), Dz. U. z 2002 r. Nr 62 poz. 558.
Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (2002), Dz. U. z 2002 r. Nr 74 poz. 1929.
Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym (2002), Dz. U. z 2002 r. Nr 113 poz. 985.
Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (2002), Dz. U. z 2002 r. Nr 130 poz. 1112.
Ustawa z dnia 29 lipca 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (2002), Dz. U. z 2002 r. Nr 156 poz. 1301.
Ustawa z dnia 27 września 2002 r. zmieniająca Ustawę z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (2002), Dz. U. z 2002 r. Nr 180 poz. 1500.
Ustawa z dnia 28 października 2002 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (2002), Dz. U. z 2002 r. Nr 197 poz. 1661.
Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (2006), Dz. U. z 2006 r. Nr 104 poz. 708.
Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (2006), Dz. U. z 2006 r. Nr 104 poz. 709.
Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (2007), Dz. U. z 2007 r. Nr 89 poz. 590.
Ustawa z dnia 21 listopada 1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskiej (1967), Dz. U. z 1967 r. Nr 44 poz. 220.
Zarządzenie Komendanta Głównego Policji nr 3/96 z dnia 5 lutego 1996 r. w sprawie użycia pododdziałów antyterrorystycznych w przypadku zamachu terrorystycznego (1996), Dz. Urz. KGP z 1996 r.
Zubrzycki W., Jałoszynski K., Babiński A. (2016), *Polska ustawa antyterrorystyczna – odpowiedź na zagrożenia współczesnym terroryzmem*, WSPol, Szczytno.

Problemy bezpieczeństwa w cyberprzestrzeni

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **95–108**

Marian Kopczewski[1]
Akademia Wojsk Lądowych we Wrocławiu
Zbigniew Ciekanowski[2]
Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej
Andrzej Marjański[3]
Społeczna Akademia Nauk

Edukacja podstawą ochrony dzieci w cyberprzestrzeni

Education as the Background for Children's Safety in Cyberspace

Abstract: The article attempts to present the cyberspace environment, the threats it poses to children, and how to counter them. There are a number of definitions both in expert publications and in government documents, which can help to understand what cyberspace is. The changes that have taken place in the beginning of the IT revolution have led to the emergence of new types of cyber threats. A virtual reality user is free to use e-mail, social networking, a wide variety of websites or databases. All this is available anywhere on the ground, the only limitation is the device for Internet access and network coverage. The multiplicity of both portable and fixed devices makes access to cyberspace ever easier. Younger children are getting their mobile devices as a gift, guaranteeing them free surfing the Internet. Old ways of spending free time disappear. Family walks, outdoor fun, playing football with friends is a thing of the past. Fewer children spend time in this way, most of them choose cyberspace.
Key words: threats, cyberspace, children and adolescents, prevention.

[1] marian.kopczewski@awl.edu.pl
[2] zbigniew@ciekanowski.pl
[3] amarjanski@san.edu.pl

Wstęp

Edukacja stanowi jeden podstawowych elementów zapewniania bezpieczeństwa dzieci w cyberprzestrzeni. Młode pokolenie pozostawione samo sobie nie jest w stanie skutecznie obronić się przed współczesnymi zagrożeniami. Dlatego kluczowe jest uświadamianie dzieci o występujących zagrożeniach oraz wyposażenie ich w niezbędną wiedzę pozwalającą uniknąć zagrożeń w Internecie. Najważniejszą rolą w tym procesie odgrywa rodzina, która wychowuje, przekazuje odpowiednie wartości oraz uczy odpowiedniego zachowania.

Kolejnym podmiotem, który także odpowiada za bezpieczeństwo i wychowanie dzieci jest szkoła. To dzięki niej młodzież uczy się jak postępować w przypadku napotkania problemów oraz przekazuje informacje, dzięki którym można zmniejszyć ryzyko wystąpienia zagrożeń. Szkoła przygotowuje zatem dzieci do odpowiedzialnego życia oraz dba o ich rozwój intelektualny. Dlatego działania mające na celu przeciwdziałanie zagrożeniom w Sieci powinny obejmować nie tylko dzieci i młodzież, ale przede wszystkim dwa środowiska, w których główne przebywają, tj. szkołę oraz rodzinę.

Rola rodziców w edukacji dzieci w zakresie bezpieczeństwa w cyberprzestrzeni

Dorośli nie są do końca świadomi zagrożeń znajdujących się w Internecie, dlatego też nie podejmują z dziećmi rozmów na tematy związane z bezpiecznym użytkowaniem Sieci. Większość z nich uważa, że problem bezpośrednio ich nie dotyczy lub posiadają zbyt ograniczoną wiedzę na ten temat, a to właśnie oni stanowią kluczową rolę w procesie przygotowania dziecka do reagowania na niebezpieczne sytuacji. Obcowanie z różnymi treściami znajdującymi się w Internecie to dla młodego człowieka sytuacja nowa i nieznana, tak jak i pojęcie bezpieczeństwa informacyjnego będącego efektem gwałtownego rozwoju techniki i technologii informatycznych [Korzeniowski 2012, s. 148].

Często dziecko nie jest świadome jakie skutki może spowodować jego działanie oraz nie wie jak zachować się w trudnej sytuacji. Zdarza się również, że nie zawsze potrafi posługiwać się informacjami, nawet jeżeli są one mu częściowo znane. Tym samym zadaniem dorosłych nie jest jedynie przekazywanie wiedzy o charakterze teoretycznym, ale również przedstawienie jej w praktyce [Wrońska 2014, ss. 123–124]. „Zdaniem M. Tyszkowej wykonanie czynności w sytuacji trudnej powoduje zmiany w przebiegu działań na skutek zakłóceń w spostrzeganiu i przetwarzaniu danych, co

wynika z silnego napięcia emocjonalnego, jakie wówczas powstaje. Możliwości realizacyjne są wówczas mniejsze niż w sytuacji normalnej" [Gutowska, Rybnik 2010, s. 12].

W toku nauczania należy kłaść nacisk na uczenie dzieci sposobu myślenia istotnego do przewidywania przyszłych zagrożeń i niebezpieczeństw oraz wyćwiczenie i utrwalenie zwyczaju bezpiecznego użytkowania sieci oraz korzystania z jednego najcenniejszych zasobów jakim jest informacja [Liedel 2011a, s. 437]. Dlatego też istotnie jest podnoszenie umiejętności rodziców, którzy sprawują nad nimi bezpośrednią kontrolę. Należy uświadamiać rodziców, zachęcać ich w poszukiwania wiedzy o obecnych i przyszłych zagrożeniach, a przede wszystkim informować o skutecznych sposobach przeciwdziałania zagrożeniom. Dzięki takim działaniom będą oni odpowiednio przygotowani do wprowadzenia teoretycznego i praktycznego swoich dzieci w pełen zagrożeń cyfrowy świat [Wrońska 2014, s. 124].

Dzieci nie są w pełni świadome konsekwencji, jakie mogą je spotkać w Sieci. Rodzice powinni więc dążyć do poznania przyjaciół swojego dziecka oraz osób, z którymi ono koresponduje, sprawdzając jego pocztę internetową. Należy nauczyć dziecko korzystania z komunikatorów internetowych, oraz tego by nie odpowiadało na wiadomości o obraźliwej treści i nie umawiało się na spotkania bez zgody rodzica. Młode pokolenie powinno być świadome, że w każdej chwili może liczyć na pomoc rodzica. W celu zwiększenia ochrony dziecka można wykorzystywać odpowiednie oprogramowanie filtrujące, mające na celu blokowanie stron, na których znajdują się treści o nieodpowiedniej tematyce. Dodatkowo istnieje możliwość sprawdzenia z jakich stron korzysta dziecko – dane te można znaleźć w zakładce „Historia" w niemal każdej przeglądarce internetowej. Należy pamiętać, że żadne oprogramowanie zapewniające ochronę rodzicielską nie zastąpi bezpośredniej rozmowy z dzieckiem, a zapewnienie bezpieczeństwa w Internecie nie może skupiać się jedynie na działaniach, które minimalizują skutki bądź stanowią system ochrony. Gdy jednak pojawiające się problemy przerastają rodziców mogą oni udać się do specjalistów o odpowiedniej wiedzy informatycznej bądź psychologicznej. Niemniej należy pamiętać, że Internet nie jest jedynie źródłem zagrożeń, ale również nieocenionym źródłem wiedzy [*Rady dla rodziców* 2017].

Rola edukacji szkolnej w przygotowaniu do korzystania z sieci

Przygotowanie młodego pokolenia do pracy we współczesnym świecie, a więc również do przeciwdziałania zagrożeniom, jest zadaniem szkoły poprzez wykorzystanie wiedzy, umiejętności i kompetencji nauczycieli [Szweda 2016, s. 164]. Programy szkolne są wzbogacone o tematykę bezpieczeństwa online, co wynika z realizacji

podstawy programowej, w skład której wchodzą zapisy dotyczące bezpiecznego korzystania z komputera i Internetu. Nauczanie szkolne jest tu kluczowe, bowiem bez odpowiedniej umiejętności wykorzystywania komputerów oraz innych urządzeń do pozyskiwania, przechowywania informacji oraz do komunikacji za pośrednictwem Sieci internauta staje się podatny na zagrożenia [Wrońska 2014, s. 125].

Obecny system nauki ulega przemianom. Zaczęto preferować aktywizowanie uczniów do działań twórczych i kreatywności, a nauczyciel staje się organizatorem i koordynatorem tych działań [Węglarz 2004]. Podstawa Programowa Kształcenia Ogólnego określa działalność edukacyjną szkoły przez:

1) „szkolny zestaw programów nauczania, który, uwzględniając wymiar wychowawczy, obejmuje całą działalność szkoły z punktu widzenia dydaktycznego;
2) program wychowawczy szkoły, obejmujący wszystkie treści i działania o charakterze wychowawczym;
3) program profilaktyki, dostosowany do potrzeb rozwojowych uczniów oraz potrzeb danego środowiska, obejmujący wszystkie treści i działania o charakterze profilaktycznym" [Dz. U. z 2012 r., poz. 977].

Szkolny zestaw programów nauczania, program wychowawczy szkoły oraz program profilaktyki muszą stwarzać integralną całość oraz uwzględniać wszelkie wymagania zawarte w podstawie programowej. Z kolei zadaniem szkoły i nauczycieli jest ich przygotowanie oraz realizacja. Działania mające na celu profilaktykę oraz edukację dzieci w dziedzinie bezpieczeństwa w Sieci powinny skupiać całą społeczność szkolną oraz być prowadzone w różnych formach, również poza zajęciami edukacyjnymi z uczniami. Powyższe działania zaczną przynosić rezultaty wyłącznie, gdy będą podchodziły do problemu kompleksowo oraz będą skupiać się na trzech płaszczyznach obejmujących relacje pomiędzy uczniem, rodzicem a nauczycielem [Wrońska 2014, ss. 126–127].

Z raportu dotyczącego diagnozy stanu bezpieczeństwa online w szkołach wynika, że zajęcia mające na celu uświadamianie o zagrożeniach w cyberprzestrzeni są zazwyczaj prowadzone podczas godzin wychowawczych. Dodatkowo część szkół organizuje z okazji Dnia Bezpiecznego Internetu spotkania edukacyjne oraz przeprowadza różne aktywności obejmujące daną tematykę. Nauczyciele zajmują się również przekazywaniem wiedzy na tematy związane z bezpieczeństwem podczas zebrań z rodzicami. W związku z tym niezbędne staje ich wyposażenie w odpowiednie materiały, które mogłyby zostać wykorzystane do prowadzenia zajęć [Makaruk 2013, s. 7].

Skuteczna edukacja nauczycieli musi polegać w pierwszej kolejności na uświadomieniu, jak ważną rolę w dziedzinie zapewniania bezpieczeństwa dzieci korzystają-

cych z Internetu, spełniają kompleksowe działania w obszarze prawa, edukacji i technologii. Głównymi celami ich kształcenia jest przekazanie im wiedzy dotyczącej:
- charakterystyki mediów elektronicznych;
- charakterystyki zagrożeń powiązanych z użytkowaniem Internetu przez dzieci;
- reguł bezpiecznego korzystania z Sieci przez młode pokolenie;
- metod służących zapewnianiu najmłodszym bezpieczeństwa on-line;
- sposobów przekazywania dzieciom wiedzy dotyczącej bezpieczeństwa w Internecie;
- procedur działania podczas zagrożenia [*Raport: Bezpieczeństwo dzieci*… 2008, s. 29].

Niezbędne jest ich wsparcie poprzez zapewnienie specjalistycznych szkoleń, wyposażenie bibliotek w pomocną literaturę oraz materiałów szkolnych pomocnych w prowadzeniu zajęć. Nie można jednak pomijać znaczącej roli rodziców, których pedagogizacja oraz aktywny udział w zadaniach szkoły znacząco zwiększa bezpieczeństwo uczniów [Wrońska 2014, s. 128].

Serwisy i przewodniki edukacyjne jako źródło informacji o bezpieczeństwie w Sieci

Wiele przydatnych informacji dotyczących bezpieczeństwa w sieci można pozyskać w serwisach internetowych dostępnych bezpośrednio dla młodego pokolenia np.: www.dzieckowsieci.pl, www.bezpiecznyinternet.org, www.saferinternet.pl. Przedstawione strony mogą służyć jako pomoc do prowadzenia zajęć lub zostać zaproponowane dzieciom przez nauczycieli jako alternatywa codziennych rozrywek. Serwisem godnym polecenia jest www.sieciaki.pl, który jest w całości poświęcony ochronie dzieci w cyberprzestrzeni. Autorzy wspomnianej strony internetowej pomyśleli również o najmłodszych, gdyż wchodząc na stronę www.przedszkolaki.sieciaki.pl najmłodsi mogą zgłębić pojęcia dotyczące komputera oraz Internetu [*Raport: Bezpieczeństwo dzieci*… 2008, ss. 31–32].

Przewodniki po Internecie stanowią jedną z najczęściej wykorzystywanych form czynności profilaktycznych skierowanych przeciwko zagrożeniom internetowym. Do organizacji zajmującej się popularyzacją przewodników można zaliczyć Childnet International, która na własnej stronie internetowej (www.childnet-int.org) przedstawia w jaki sposób bezpiecznie korzystać z sieci. Hasłem odnoszącym się do wskazówek jakimi mają kierować się dzieci korzystające z Internetu jest „Smart". Całość została przedstawiona w przystępny sposób, dzięki czemu jest to skuteczne narzędzie edukacyjne [Przybysz-Zaremba 2008, ss. 51–52].

Przewodniki stanowią bogate źródło informacji w jaki sposób należy bezpiecznie korzystać z Sieci. Te przeznaczone dla rodziców lub młodzieży są podobne to tych dla

dzieci, różnica polega jedynie na ilości zawartych informacji oraz języku, który jest dopasowany do wieku odbiorców. Poradniki przeznaczone dla opiekunów zawierają dodatkowo porady dotyczące sposobów kontrolowania stron internetowych.

Programowe metody ochrony dzieci

Ważnym elementem przeciwdziałania zagrożeniom są również technologie filtrujące, które skanują treści występujące na stronach internetowych, a w przypadku stwierdzenia na nich nieodpowiednich treści – blokują do nich dostęp. Do takich programów można zaliczyć [Przybysz-Zaremba 2008, s. 53]: Beniamin, Strażnik Ucznia, WebControl lub Anti-Porn. Wykorzystywanie powyższych programów działa zapobiegawczo, chroniąc dzieci przed treściami powiązanymi z seksem oraz przemocą. Za przykład może posłużyć program WebControl, którego zaletą jest systematycznie aktualizowana baza nieodpowiednich stron, którą użytkownik może swobodnie dostosowywać do swoich potrzeb. Ponadto program został wyposażony w moduł umożliwiający ograniczenie dostępu do sieci w określonych przedziałach czasowych. Dodatkowo istnieje możliwość zablokowania dostępu do skrzynki pocztowej, zapisu danych na przenośnych pamięciach oraz nagrywania płyt [WebConntrol 2017]. Opiekunowie mogą skorzystać również z programu monitorującego komunikację sieciową, który umożliwia sprawowanie opieki nad wykorzystaniem dostępu sieciowego przez najmłodszych np. poprzez program Strażnik Ucznia [Przybysz-Zaremba 2008, s. 53].

Ciekawym rozwiązaniem jest program Anti-Porn, który nadaje się do nadzoru sposobu wykorzystania komputera. Aplikacja umożliwia kontrolę odwiedzanych witryn internetowych oraz uruchamianych programów. O skuteczności tego programu może świadczyć fakt, że jest on wykorzystywany przez ponad 8 milionów użytkowników z całego świata. Powyższa aplikacja, oprócz standardowych funkcji, została wyposażona w wiele dodatkowych modułów. Wśród nich można znaleźć moduł blokujący wybrane komunikatory i gry komputerowe oraz ograniczyć do nich czasowo dostęp [Anti-Porn 2017].

Ponadto twórcy najpopularniejszych programów w Internecie, do których można zaliczyć przeglądarki internetowe, wyszukiwarki oraz producenci systemów operacyjnych, dostosowując się do panujących trendów dodali do swoich programów opcje ograniczające dostęp. Dodatkowo takie moduły można spotkać w wielu programach antywirusowych służących głównie do ochrony danych znajdujących się na komputerze [*Raport z badań…* 2009, s. 31].

Niestety, jak wskazują badania przeprowadzone w Wielkiej Brytanii, wielu rodziców nie jest w stanie samodzielnie zainstalować oprogramowania filtrującego, tak

twierdzi 20% z nich, a 26% przyznało, że nie jest pewnych czy jest już w posiadaniu odpowiedniego programu [Przybysz-Zaremba 2008, s. 53].

Cenzor to pierwszy polski program, który umożliwia kontrolę zasobów Internetowych. Skutecznie odmawia dostępu do witryn zawierających niebezpieczne oraz niecenzuralne treści. Program jest dostępny w kilku wersjach:

- Cenzor IND – skierowany dla indywidualnych odbiorców;
- Cenzor EDU – odpowiedni dla placówek oświatowych;
- Cenzor BIZ – stworzony dla firm.

Program jest zabezpieczony hasłem, dzięki czemu wszelka ingerencja mająca na celu zmianę ustawień, wyłączenie programu czy usunięcie katalogu z programem jest utrudniona. Każdy jego użytkownik ma swoje konto, na którym program tworzy historię odwiedzanych stron, z możliwością ich późniejszego odtworzenia. Raport składa się z podstawowych informacji, do których można zaliczyć: adresy przeglądanych stron, godzinę, datę. Bardzo przydatną funkcją jest możliwość zablokowania ściągania „śmieci internetowych", które pobierają się czasami automatycznie, bez wiedzy użytkownika. Administrator aplikacji może w dowolny sposób wpływać na funkcjonowanie zabezpieczeń, usuwać wybrane pozycje witryn z listy stron zakazanych oraz dodawać nowe. Ponadto aplikacja dysponuje funkcjami, pozwalającymi ograniczyć czas spędzany w sieci [Przybysz-Zaremba 2008, s. 54].

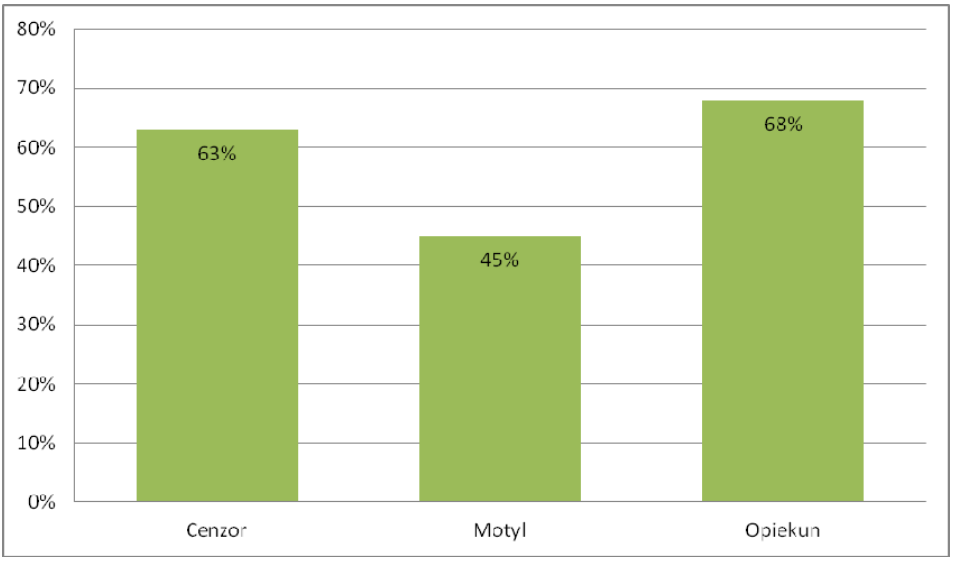
Motyl jest programem umożliwiający kontrolę zasobów internetowych. Aplikacja ta pozwala na blokadę stron z treściami o charakterze erotycznym czy pornograficznym. Ponadto blokuje dostęp do komunikatorów internetowych, czatów oraz bramek SMS. Program skanuje stronę pod kontem występowania nieodpowiednich słów i w przypadku ich znalezienia zamyka witrynę. Jest to możliwe dzięki wbudowanemu słownikowi zawierającemu listę słów zakazanych w różnych językach [Przybysz-Zaremba 2008, ss. 54–55].

Opiekun Dziecka w Internecie jest programem zabezpieczającym dzieci przed szkodliwym wpływem komputera oraz Internetu. Zapewnia on szeroką gamę możliwości chroniących najmłodszych. Aplikacja została wyposażona w moduły analizy stron internetowych, dzięki czemu blokuje strony, które nie znajdują się na liście stron zakazanych. Dodatkowo zawiera bazę ponad 780 tysięcy adresów oraz blisko 3 500 tysiąca nieodpowiednich słów w 7 językach. Wszystkie otwierane strony są zapisywane, co umożliwia ich późniejsze sprawdzenie przez rodziców. Ponadto czas umożliwia ograniczenie czasu spędzanego przed komputerem.

Program ten posiada dwa tryby pracy. Tryb prosty skierowany do grona użytkowników o niewielkiej wiedzy informatycznej, w którym ustawienia zaawansowane zostały ukryte oraz tryb zaawansowany skierowany do opiekunów bardziej biegłych

w obsłudze komputera. Tryb ten został tak skonstruowany, aby nie było możliwości pominięcia mechanizmów weryfikacji treści. Z kolei usunięcie programu wymaga podania odpowiedniego hasła. W przypadku wykasowania części plików, bez całkowitej deinstalacji Opiekuna Dziecka, dostęp do Sieci zostanie całkowicie odłączony. Zabezpieczenie to zostało stworzone w celu uniemożliwienia usunięcia nadzoru programu (rysunki 1, 2 i 3). Aplikacja ta jest całkowicie kompatybilna z popularnymi przeglądarkami internetowymi oraz programami wykorzystującymi protokół http [Opiekun Dziecka 2017].

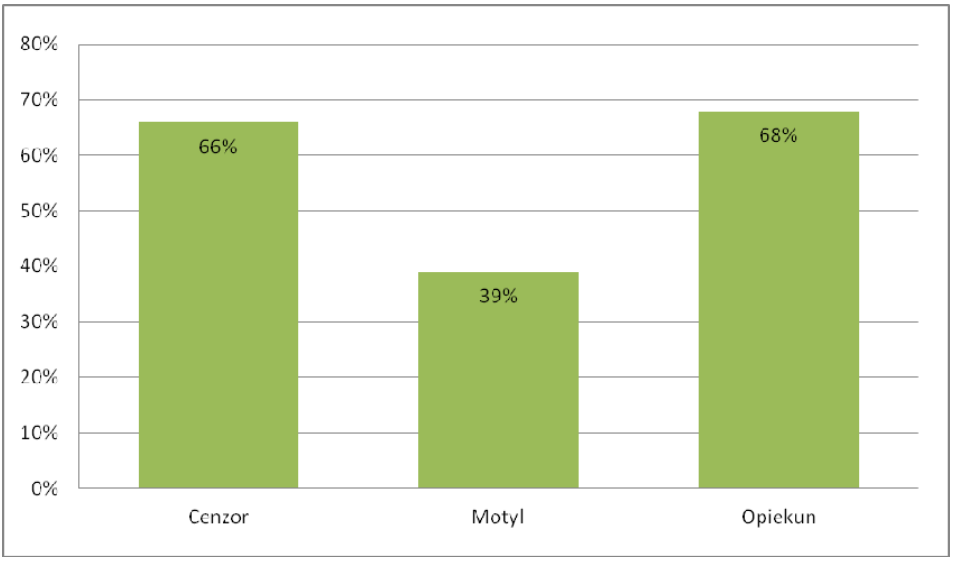
Rysunek 1. Skuteczność aplikacji filtrujących w przeglądarce „Firefox"



Źródło: opracowanie własne na podstawie: [*Raport z badań…* 2009, s. 20].

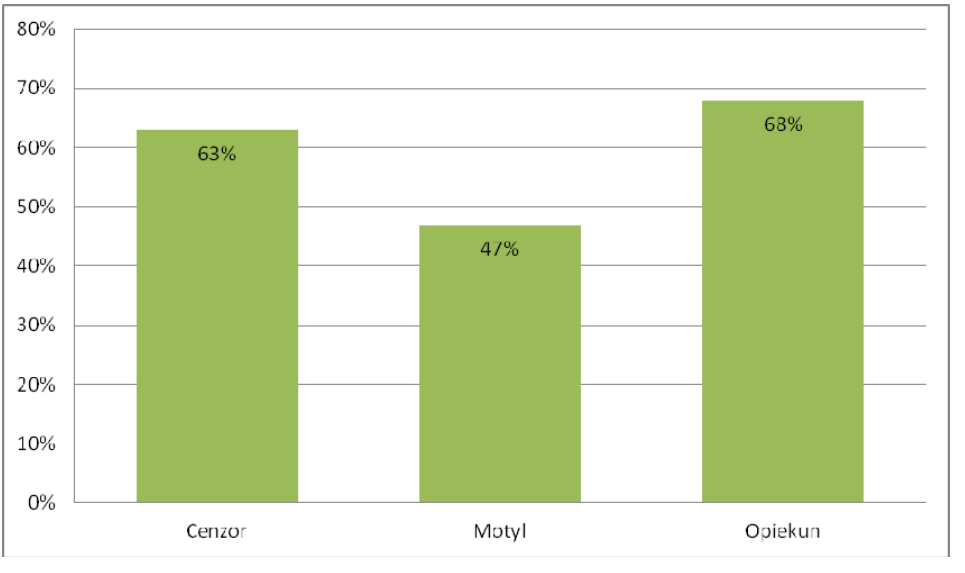
Kolejnym rozwiązaniem zapewniającym ochronę dzieci w cyberprzestrzeni są dedykowane wyszukiwarki internetowe. Programy te stanowią połączenie portalu dla dzieci z bazą stron, po których dziecko może się poruszać [*Raport z badań…* 2009, s. 24]. Do takiej bazy nie zostaną dołączone witryny, które: zawierają przemoc, pornografię, nakłaniają do rasizmu i nienawiści, propagują sekty, zawierają niezrozumiałe treści, treści niezgodne z polskim prawem oraz materiały promujące używki. Decyzję o jej dodaniu określa zespół pedagogów oraz psychologów, którzy czuwają, aby znajdujące się treści na stronie były bezpieczne dla dzieci. Przykładem takiej wyszukiwarki jest Mamuu.pl oraz fragFinn.de, kiddle.co [Góralczyk 2010].

Rysunek 2. Skuteczność aplikacji filtrujących w przeglądarce „Opera"



Źródło: opracowanie własne na podstawie: [*Raport z badań*… 2009, s. 20].

Rysunek 3. Skuteczność aplikacji filtrujących w przeglądarce „Internet Explorer"



Źródło: opracowanie własne na podstawie: [*Raport z badań*… 2009, s. 20].

Programy antywirusowe zapewniają dodatkową ochronę dzieci w cyberprzestrzeni. Jest to możliwe dzięki wyposażeniu ich w moduły kontroli rodzicielskiej. Przykładem takiego programu jest Kaspersky Internet Security, który skutecznie chroni dzieci i młodzież przed niebezpiecznym wpływem komputera i Internetu. Zapobiega przed zbyt długim czasem spędzanym przed komputerem, blokuje dostęp do stron z niebezpiecznymi treściami oraz zapewnia ochronę przed utratą pieniędzy. Można dzięki niemu również zablokować pobieranie niektórych plików. Program umożliwia także ochronę korespondencji. W przypadku włączenia tej funkcji kontroli, wszystkie wiadomości wysyłane na różnych portalach społecznościowych czy przez popularne programy komunikacyjne będą zapisywane w raporcie, który posiada szczegółowe dane. Natomiast w przypadku próby przesłania wiadomości z danymi osobowymi, nastąpi blokada jej [Kaspersky Internet Security 2013].

Bezpieczeństwo infrastruktury informatycznej w szkole

Obecnie niektóre placówki wykorzystują infrastrukturę informatyczną do szeregu działań związanych z organizacją szkoły i prowadzeniem zajęć. Dlatego też kluczowe staje się zapewnienie ich sieci wysokiego poziomu bezpieczeństwa [Stachecki 2013, s. 10]. Coraz więcej dzieci posiada przy sobie urządzenia mobilne. Cechą takich urządzeń jest wygoda użytkowania, poza tym na wyposażeniu mogą mieć aparat, kamerę, dyktafon oraz dostęp do Internetu, co sprawia, że są to doskonałe narzędzia dydaktyczne.

Obecnie występująca tendencja BYOD (*Bring Your Own Device*), polega na przynoszeniu własnych urządzeń, które następnie wykorzystują szkolny dostęp do Internetu, co sprawia duże wyzwanie dla zarówno dla sieci, jak i administratora. Wiele urządzeń jednocześnie wykorzystujących szkolny Internet powoduje różnego rodzaju przeciążenia, które mogą skutkować awarią całej sieci lub nieprzewidywalnymi błędami. W związku z tym, aby zapewnić bezpieczeństwo infrastruktury, z której korzystają dzieci należy wykorzystywać odpowiedni sprzęt, dostosowany do potrzeb placówki. „Najbardziej popularne routery i access pointy z tzw. segmentu SOHO (*Small Office Home Office)* nie nadają się do pracy w warunkach szkolnych. Nie potrafią zapewnić obsługi takiej liczby urządzeń zlokalizowanych często w niewielkiej odległości od siebie. Bardzo łatwo taką sieć przeciążyć i zwyczajnie zablokować. Powinno się sięgać po profesjonalne rozwiązania z dedykowanym kontrolerem WLAN (*WirelessLocal Area Network*), zapewniającym zarówno wysoką wydajność, jak i odpowiedni poziom bezpieczeństwa, z zarządzalnymi, szybkimi przełącznikami, z wysokowydajnym routerem

wyposażonym system IPS i inne mechanizmy zabezpieczające przed atakami i włamaniami" [Stachecki 2013, ss. 10–11].

Szkoła, udostępniając sieć bezprzewodową, staje się niejako dostawcą usług internetowych, dlatego powinna zachować odpowiednie standardy bezpieczeństwa. Najlepiej stworzyć taką infrastrukturę, która będzie podzielona na publiczną, dydaktyczną oraz administracyjną. Z tego względu najlepszym rozwiązaniem jest wprowadzenie serwera, który autoryzuje dostęp do konta oraz gromadzi dane o działalności użytkownika w sieci. Wprowadzenie takiego rozwiązania umożliwia nadanie każdemu użytkownikowi unikalnego konta i hasła. Badania wskazują, że to w bardzo dużym stopniu eliminuje próby powiązane z nieautoryzowanym dostępem oraz skutecznie redukuje liczbę nieodpowiednich komentarzy pojawiających się na forach internetowych, dodatkowo sprawiając, że użytkownicy obawiają się korzystać ze stron o nieodpowiedniej treści [Stachecki 2013, s. 11].

Polityka bezpieczeństwa i zabezpieczenie prywatności w sieci

Zapewnienie bezpieczeństwa w szkolnej Sieci jest związane z wprowadzeniem stosownej polityki bezpieczeństwa infrastruktury informatycznej. Jednak nawet doskonale przygotowana polityka bezpieczeństwa nie będzie skuteczna w przypadku, gdy nie będzie wytrwale realizowana [Stachecki 2013, s. 13].

Zabezpieczenie prywatności w czasie korzystania z usług elektronicznych mogą zapewnić odpowiednie programy gwarantujące anonimowość, które blokują niechcianą pocztę, chronią przed plikami cookie, zapewniają ochronę kryptograficzną oraz P3P. Do podstawowych ustawień wpływających na ochronę prywatności w przeglądarkach internetowych można zaliczyć:

- uruchomienie operacji „nie śledzić" (DNT) w przypadku, gdy opcja nie jest włączona domyślnie;
- zgoda na przyjmowanie plików cookie ze strony innych firm;
- dodatki do przeglądarki służące dla ochrony prywatności, np. NoScript;
- ochrona prywatności poprzez kasowanie plików cookie;
- ustawienia przeglądarki, które będą odrzucać żądania API, służące lokalizacji;
- konfiguracja bezpiecznych połączeń (SSL) [Wojciechowska-Filipiek, Ciekanowski 2016, s. 75].

Technologie pozwalające na zapewnienie odpowiedniego poziomu ochrony prywatności (PET) można z kolei podzielić na 4 podstawowe narzędzia: szyfrowania, polityki, filtrowania i anonimowości. Głównym zadaniem technologii PET jest zwiększenie kontroli prywatności użytkownika oraz kasowanie nieużytecznych danych identyfika-

cyjnych wykorzystywanych w komunikacji. Za przykład takiej technologii może posłużyć protokół (*The Platform for Privacy Preferences*), który służy do wspomagania użytkowników, co do podjęcia decyzji o ujawnieniu danych osobowych. Protokół ten przeprowadza dokładną analizę strony, którą użytkownik zamierza odwiedzić. Wykrywa on ustawienia witryny, które następnie porównuje z preferencjami wprowadzonymi przez administratora [Wojciechowska-Filipiek, Ciekanowski 2016, ss. 75–76].

Wnioski

Ewolucja funkcji informacyjnej jaka dokonała się w ciągu ostatnich kilkunastu lat spowodowała, że zasoby informacyjne stały się kluczowym elementem w funkcjonowaniu społeczeństwa [Liedel 2011b, s.46], a dziecko w dzisiejszym świecie jest narażone na wiele zagrożeń występujących w cyberprzestrzeni, które systematycznie ewoluują. Dlatego też najważniejszym elementem zapewniającym bezpieczeństwo jest edukacja, która powinna towarzyszyć dziecku od samego początku poznania cyberświata. Kluczową rolę w tym zakresie odgrywa rodzina, która wpaja odpowiednie wartości oraz wychowuje młode pokolenie. Często jednak rodzice nie posiadają odpowiedniej wiedzy na temat występujących zagrożeń. Należy zapewnić im dostęp do źródeł informacji oraz informować, w jaki sposób przeciwdziałać zagrożeniom.

Kolejną bardzo ważną rolę w systemie kształcenia dzieci odgrywa szkoła, gdzie młode pokolenie przebywa wśród grupy rówieśników, zdobywa niezbędną wiedzę oraz przygotowuje się do życia we współczesnym świecie pełnym zagrożeń. Dlatego też zadaniem szkoły jest przekazywanie wiedzy na temat bezpiecznego użytkowania komputera oraz występujących niebezpieczeństw. Powyższe zadanie powinno być realizowane w sposób kompleksowy na wielu zajęciach, nie tylko na informatyce.

Ważnym elementem zapewniającym bezpieczeństwo dzieci w cyberprzestrzeni jest również odpowiednie oprogramowanie filtrujące, które w bezpośredni sposób wpływa na ograniczenie kontaktu dziecka z nieodpowiednimi treściami. Szeroki wachlarz programów oferowanych przez producentów sprawia, że miejsce spędzania wolnego czasu, jakim jest obecnie cyberprzestrzeń jest w bardzo skuteczny sposób filtrowana. Dzięki temu dziecko może korzystać ze sprawdzonych, bezpiecznych stron.

W związku z pojawieniem się nowego środowiska, pojawiły się nowe zagrożenia. Długie godziny spędzane przed komputerem powodują wiele dolegliwości fizycznych. Dzieci narażają się tym samym na coraz częstsze wady postawy czy bóle stawów. Ponadto korzystanie z cyberprzestrzeni powoduje wiele zagrożeń psychicznych, które w konsekwencji mogą doprowadzić do różnego rodzaju zaburzeń czy poważ-

nych chorób natury psychicznej. Dochodzą to tego zagrożenia społeczne, które sprawiają, że dziecko ma problemy z odróżnieniem tego co jest fikcją, a co rzeczywistością. Dodatkowo korzystanie z różnych portali społecznościowych sprawia, że dziecko ogranicza kontakt z otoczeniem do minimum, przez co zanika interakcja z rówieśnikami i pogarszają się jego zdolności komunikacyjne, a tym samym powstają zagrożenia Internetowe.

Najskuteczniejszą formą ochrony dzieci w cyberprzestrzeni jest edukacja młodego pokolenia realizowana przez rodziców i szkołę. Dzięki temu dziecko będzie świadome czekających je niebezpieczeństw i ostrożniejsze w Sieci. Jednak najważniejszym elementem zapewniającym bezpieczeństwo jest zainteresowanie ze strony rodzica oraz kontrola, która nie będzie możliwa bez dostatecznej wiedzy na temat występujących zagrożeń i sposobów im przeciwdziałania. Dlatego tak ważna jest edukacja zarówno dzieci jak i rodziców, którzy taką kontrolę sprawują. Pomocne w tym mogą okazać się różnego rodzaju poradniki, które są dostępne w formie elektronicznej, bądź papierowej.

Bibliografia

Gutowska H, Rybnik B. (2010), *Bezpieczna droga do szkoły. Zeszyt metodyczny dla nauczycieli i rodziców,* Image, Warszawa.

Korzeniowski L.F. (2012), *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa.

Liedel K. (2011a), *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej*, [w:] K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red. nauk.), *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, Difin, Warszawa.

Liedel K. (2011b), *Bezpieczeństwo informacyjne państwa*, [w:] K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa*, Difin, Warszawa.

Makaruk K. (2013), *Diagnoza stanu bezpieczeństwa online w szkołach. Raport z badań*, Fundacja Dzieci Niczyje, Warszawa.

Przybysz-Zaremba M. (2008), *Uzależnienie młodzieży od współczesnych mediów*, Oficyna Wydawnicza Prospekt, Olsztyn.

Raport: Bezpieczeństwo dzieci korzystających z Internetu (2008), Fundacja Dzieci Niczyje, Warszawa.

Raport z badań: Rozwiązania Filtrujące Niepożądane Treści w Internecie (2009), NASK, Warszawa.

Stachecki D. (2013), *Bezpieczeństwo szkolnej infrastruktury edukacyjnej*, [w:] *Szkolne standardy bezpieczeństwa dzieci i młodzieży online. Rekomendacje dla szkół*, Fundacja Dzieci Niczyje, Warszawa.

Szweda E. (2016), *Bezpieczeństwo społeczności lokalnych*, Difin, Warszawa.

Wojciechowska-Filipek S., Ciekanowski Z. (2016), *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki-organizacji-państwa*, CeDeWu, Warszawa.

Wrońska A. (2014), *Profilaktyka i reagowanie*, [w:] *Bezpieczeństwo dzieci online. Kompendium dla rodziców, nauczycieli i profesjonalistów*, NASK, Warszawa.

Źródła internetowe

Węglarz A. (2004), *Metody aktywizujące uczniów*, [online], www.awanas.net.pl, dostęp: 17.03.2017.

WebControl (2017), [online], www.dobreprogramy.pl, dostęp:11.03.2017.

AntiPorn (2017), [online], www.dobreprogramy.pl, dostęp:11.03.2017.

Opiekun Dziecka (2017), [online], www.opiekun.pl, dostęp:11.03.2017.

Góralczyk M. (2010), *Wyszukiwarki dla dzieci*, [online], www.finepeformance, dostęp: 11.03.2017.

Kaspersky Internet Security (2013), *Informacje o kontroli rodzicielskiej*, [online], www.supportkaspersky.com.pl, dostęp: 11.03.2017.

Rady dla rodziców (2017), [online], www.saferinterent.pl, dostęp: 11.03.2017.

Akty prawne

Rozporządzenie Ministra Edukacji Narodowej z dnia 27 sierpnia 2012 r. w sprawie podstawy programowej wychowania przedszkolnego oraz kształcenia ogólnego w poszczególnych typach szkół (Dz. U. z 2012 r., poz. 977).

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **109–125**

Zbigniew Ciekanowski[1]
Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej
Marian Kopczewski[2]
Akademia Wojsk Lądowych we Wrocławiu
Andrzej Marjański[3]
Społeczna Akademia Nauk

Bezpieczeństwo dzieci w cyberprzestrzeni w świetle badań

Child Safety in Cyberspace in Light of Research

Abstract: Broad Internet access has many challenges, and often the Internet can be used for illegal purposes. Free access to cyberspace for everyone makes the network full of threats. Particularly vulnerable are children whose minds are just developing. Inappropriate content can be harmful to them, leading to many serious disorders and health problems, both psychological and physical. It is therefore essential to observe basic safety rules, to educate the environment in which children are staying and to control the material being viewed.
Research shows that the most important element of ensuring children safety is parental interest and control that is not possible without sufficient knowledge of the risks and how to counteract them. That is why it is so important to educate both children and parents who exercise such control. Helpful in this may be different types of guides, which are available in electronic or paper form. Parents can learn how to prevent dangers without leaving home.
Key words: safety, cyberspace, children, research results.

[1] zbigniew@ciekanowski.pl
[2] marian.kopczewski@awl.edu.pl
[3] amarjanski@san.edu.pl

Wstęp

Rozwój technologii informacyjnych przyczynia się do szeregu różnorodnych przemian, w każdym obszarze ludzkiej aktywności, także tych realizowanych w przestrzeni publicznej, która została powiększona o cyberprzestrzeń [Andrzejewska, Bednarek 2017, s. 9]. Jest to jeden z najnowszych priorytetów w polskiej strategii bezpieczeństwa ukierunkowanego na rzecz budowy zintegrowanego systemu cyberbezpieczeństwa obejmującego przestrzeń przetwarzania i wymiany informacji tworzonych przez systemy teleinformatyczne [*Doktryna Cyberbezpieczeństwa*… 2015, s. 4, 7]

W dobie postępującej komputeryzacji coraz większa liczba osób ma dostęp do Internetu. Nowe technologie komunikacyjne z każdym dniem zmieniają otaczający nas świat. Dawne formy spędzania wolnego czasu zostają wyparte przez nowe. I tak zamiast spędzać czas na świeżym powietrzu, większość osób przesiaduje coraz dłużej w cyberprzestrzeni i wirtualnej rzeczywistości, gdzie całe społeczeństwo, bez względu na miejsce zamieszkania może swobodnie korzystać z szerokiego dostępu do informacji, wymieniać poglądy z osobą oddaloną o setki kilometrów czy przetwarzać dane o różnej tematyce. Powszechne staje się masowe korzystanie z cyfrowych technologii komunikacyjnych, które w wielu przypadkach stają się najważniejszym rodzajem komunikowania [Barney, ss. 38–44], zaś zasoby informacyjne stanowią jeden z kluczowych elementów funkcjonowania społeczeństwa [Liedel 2011, s. 46]. Korzystanie z Sieci pozwala na realizację aspiracji życiowych oraz tworzy warunki do pracy i nauki [Skrabacz 2012 , s. 32].

Szeroki dostęp do Internetu niesie jednak za sobą wiele wyzwań, ponieważ może być wykorzystywany również w celach niezgodnych z prawem. Swobodny dostęp do cyberprzestrzeni sprawia, że w sieci znajduje się wiele zagrożeń, które mają inny wymiar i skutki niż te dotąd spotykane. Zagrożenia cyberprzestrzeni utożsamia się na równi z niebezpieczeństwami patologicznymi, takimi jak uzależnienie od alkoholu czy narkotyków [Kopczewski, Dudzik 2012, ss. 79–92].

Szczególnie podatne na nie są dzieci, których umysły dopiero się rozwijają, a korzystanie z cyberprzestrzeni wpływa na kształtowanie ich osobowości [Bednarek 2002, s. 246]. Nieodpowiednie treści mogą być dla nich szkodliwe, doprowadzając do wielu poważnych zaburzeń oraz problemów zdrowotnych zarówno natury psychicznej, jak i fizycznej. Dlatego kluczowym staje się przestrzeganie podstawowych zasad bezpieczeństwa, edukacja środowisk, w których przebywają dzieci oraz skuteczna kontrola przeglądanych przez nie materiałów [Kopczewski 2014, ss. 133–135].

Liczni badacze z różnych dziedzin naukowych wskazują na potrzebę zapewnienia bezpieczeństwa w cyberprzestrzeni. Sygnalizuje to m.in. A. Gidens [2010] wskazując

na rosnącą rolę przestrzeni cyfrowej oraz pojawiających się w niej szans i zagrożeń. Konieczne jest zatem skuteczne przeciwdziałanie negatywnym zjawiskom oraz wypracowanie mechanizmów reagowania na nie [Bełza 2011, s. 121]. Istotne znaczenie ma zapewnienie prywatności w czasie korzystania z cyberprzestrzeni dzięki zastosowaniu odpowiednich technologii gwarantujących odpowiedni poziom bezpieczeństwa w Sieci [Wojciechowska-Filipiek, Ciekanowski 2016, s. 75].

Mając na uwadze skalę zjawiska za cel badań przyjęto przedstawienie zagrożeń i sposobów ochrony dzieci w cyberprzestrzeni. Przedstawiony wyżej cel badawczy został zrealizowany na podstawie informacji teoretycznych znajdujących się w literaturze przedmiotu oraz badań własnych. Dla potrzeb niniejszej pracy przyjęto następujący główny problem badawczy: Jakie zagrożenia w cyberprzestrzeni mają największy wpływ na bezpieczeństwo dzieci i jakie istnieją możliwości przeciwdziałania tym zagrożeniom?

Hipotezę główną stanowi założenie, że do najistotniejszych zagrożeń w cyberprzestrzeni zaliczyć możemy zagrożenia fizyczne, psychiczne i społeczne, którym można przeciwdziałać poprzez kontrolę przed bezpośrednim dostępem do niebezpiecznych treści oraz edukacją dzieci przez rodziców i szkołę.

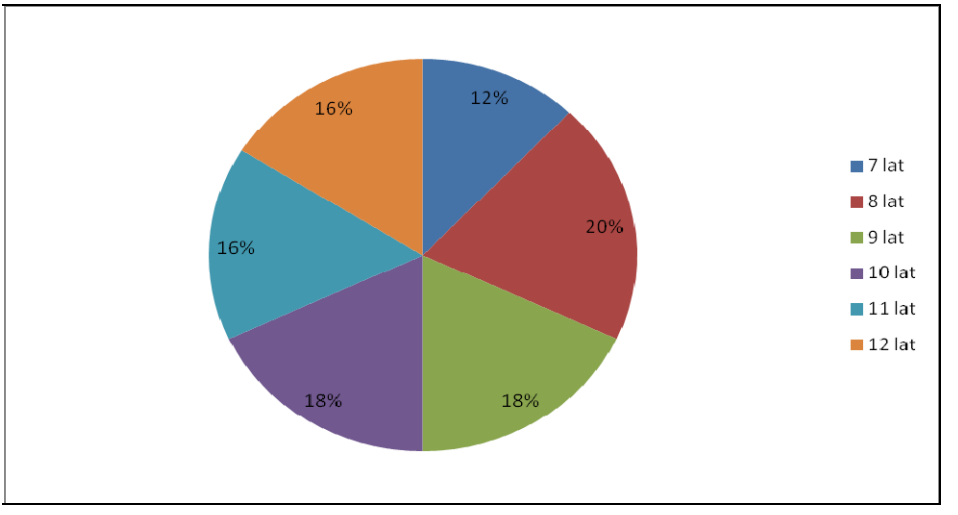
Badania zostały przeprowadzone za pomocą ankiety w formie papierowej, zaś miejscem, w którym przeprowadzono badania była szkoła podstawowa. Ankieta obejmowała łącznie 50 uczniów z podziałem na płeć. Wyniki zostały ukazane w formie wykresów obrazujących dane statystyczne.

Badania

Udział procentowy dzieci biorących udział w badaniu:
- 12% stanowiły dzieci w wieku 7 lat;
- 20% stanowiły dzieci w wieku 8 lat;
- 18% stanowiły dzieci w wieku 9 lat;
- 18% stanowiły dzieci w wieku 10 lat;
- 16% stanowiły dzieci w wieku 11 lat;
- 16% stanowiły dzieci w wieku 12 lat.

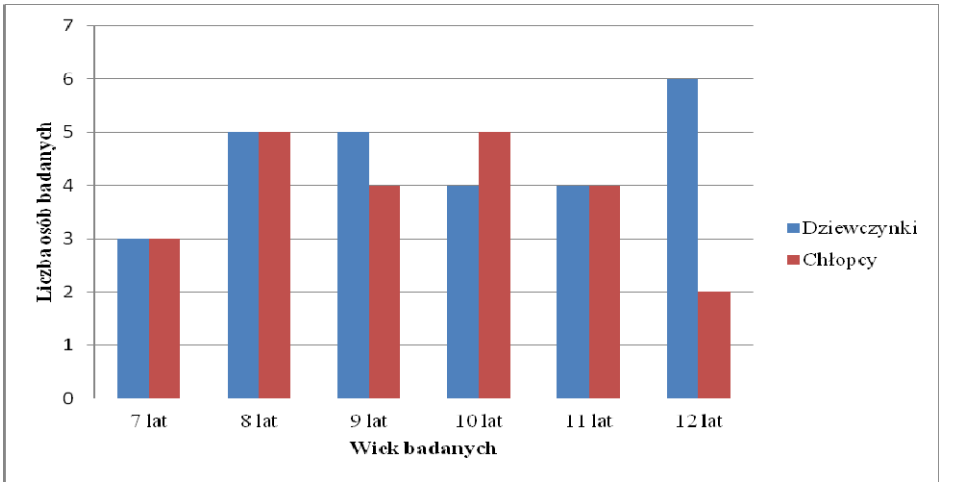
Najliczniejszą grupą badanych były dziewczynki, których liczba wyniosła 27, z kolei chłopców było 23. Rozbieżność pomiędzy obydwiema płciami była niewielka, tym samym badania będą prezentować wyniki na podobnej liczbie badanych z obydwu grup.

Rysunek 1. Przedział wiekowy badanych



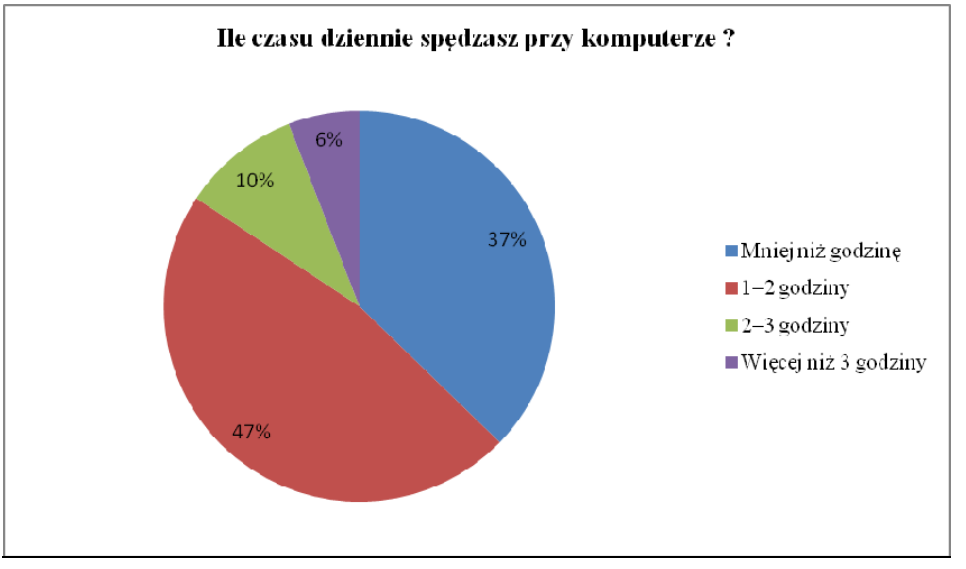
Źródło: badania własne.

Rysunek 2. Płeć badanych



Źródło: badania własne.

Rysunek 3. Dzienny czas spędzany przed komputerem

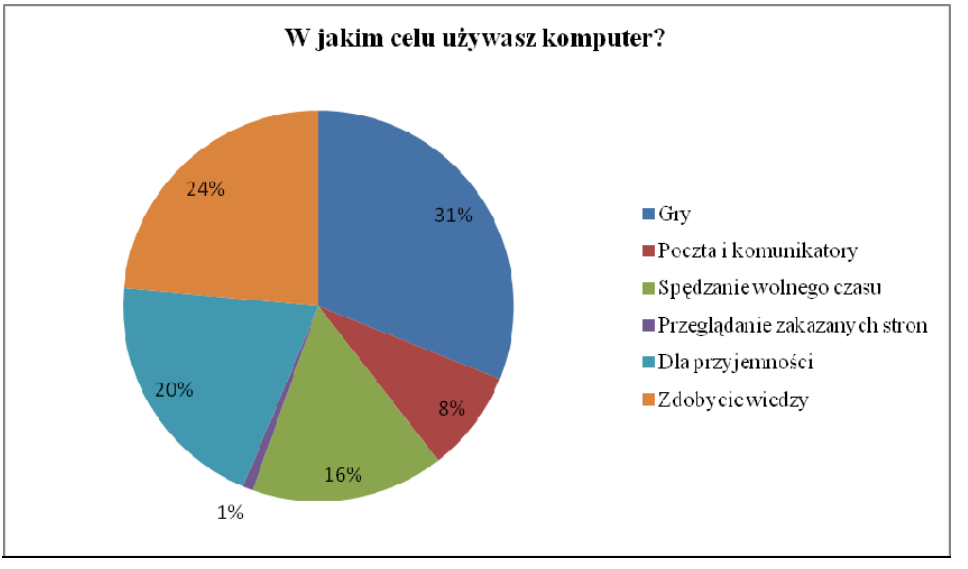


Źródło: badania własne.

Prawie połowa dzieci wskazała, że spędza dziennie przed komputerem około 1–2 godzin. 37% ankietowanych deklaruje, że korzysta z niego mniej niż godzinę dziennie. Z kolei 10% badanych spędza przed komputerem w granicach 2–3 godzin. Należy podkreślić, że najmniej ankietowanych zaznaczyło, że korzysta z niego więcej niż 3 godziny dziennie. Z powyższych danych można wywnioskować, że dzieci nie przesiadują zbyt długo przed komputerem, tym samym nie są narażone na zagrożenia zdrowotne z tym związane, co wskazuje na właściwe korzystanie z komputera przez większość młodego pokolenia.

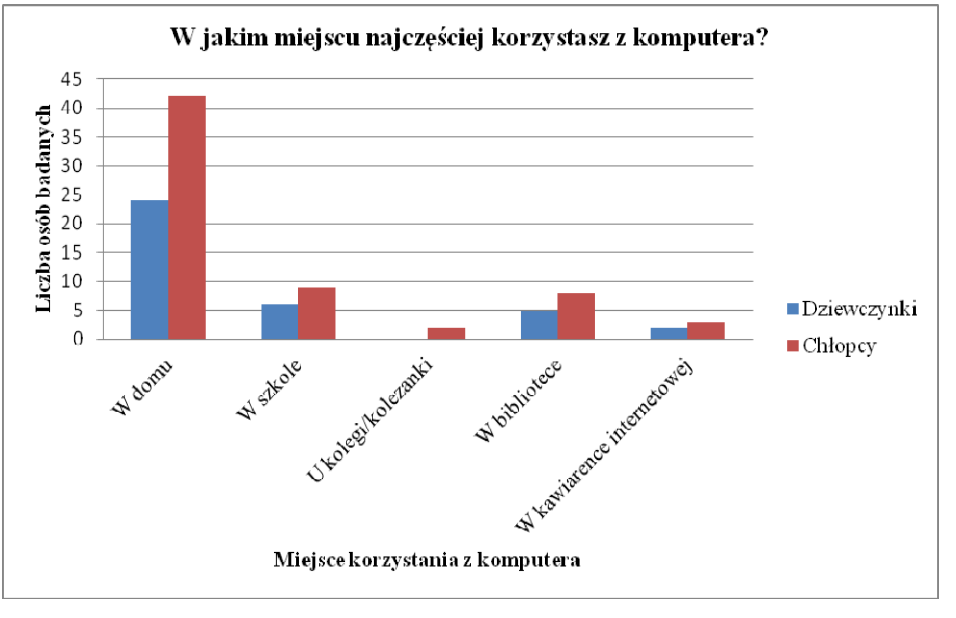
Większość uczniów wskazuje, że komputer wykorzystują najczęściej do gier komputerowych. 24% badanych korzysta z niego w celu zdobycia wiedzy. Rzadziej komputer jest wykorzystywany do komunikacji za pośrednictwem poczty elektronicznej czy komunikatorów. Zaledwie 1% ankietowanych wskazało, że wykorzystuje go do przeglądania zakazanych stron. Powyższe statystyki wskazują, jak dużo czasu dzieci poświęcają na przyjemności oraz na gry komputerowe. Może to prowadzić do wielu uzależnień oraz problemów zdrowotnych. Zamiast spędzać czas w innej formie aż 20% uczniów korzysta z komputera dla przyjemności, nie rozwijając innych swoich pasji.

Rysunek 4. Cel użycia komputera



Źródło: badania własne.

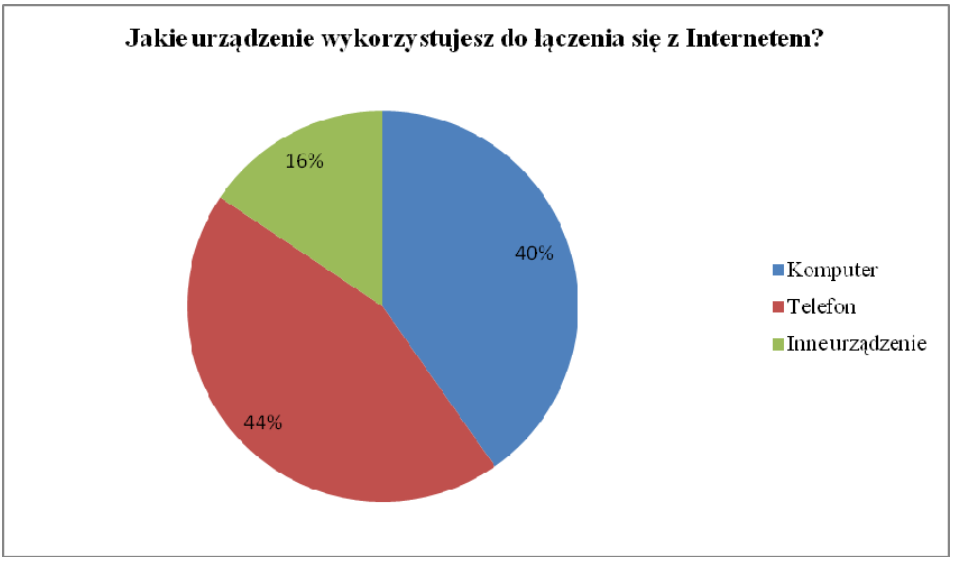
Rysunek 5. Miejsce korzystania z komputera



Źródło: badania własne.

Najczęściej dzieci korzystają z komputera w domu, rzadziej w takich miejscach jak szkoła czy biblioteka. Świadczy to o priorytetowym działaniu mającym na celu zabezpieczenie komputera znajdującego się w domu oraz odpowiedniej kontroli dziecka.

Rysunek 6. Urządzenie wykorzystywane do łączenia się z Internetem

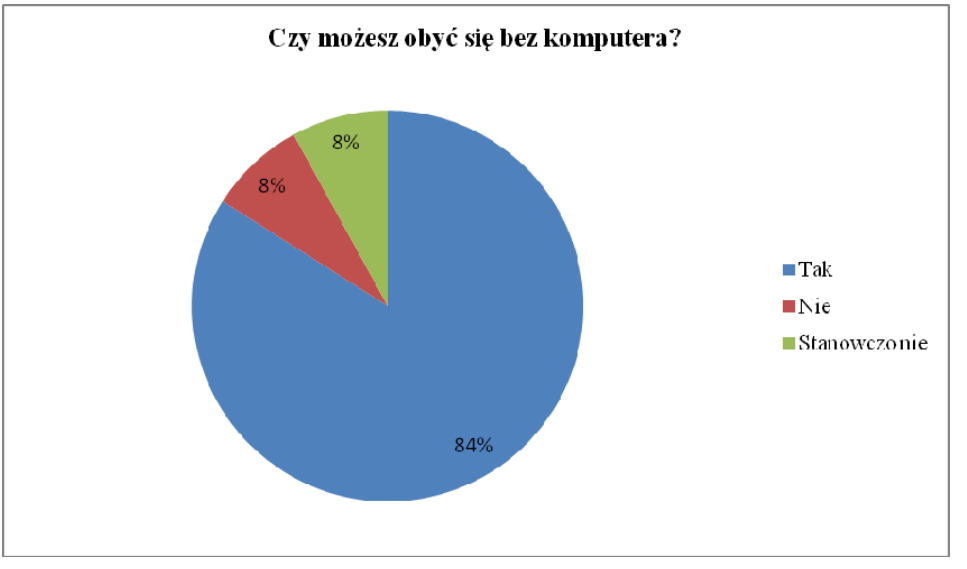


Źródło: badania własne.

Dominującymi urządzeniami, z których korzystają dzieci do łączenia się z Internetem są komputer oraz telefon komórkowy. Smartfony sprawiają, że dostęp do Internetu jest możliwy w dowolnym miejscu, stwarzając tym samym poważne problemy związane z odpowiednią kontrolą dzieci. Mogą one porozumiewać się z dowolnymi osobami oraz korzystać z nieodpowiednich stron bez wiedzy rodziców.

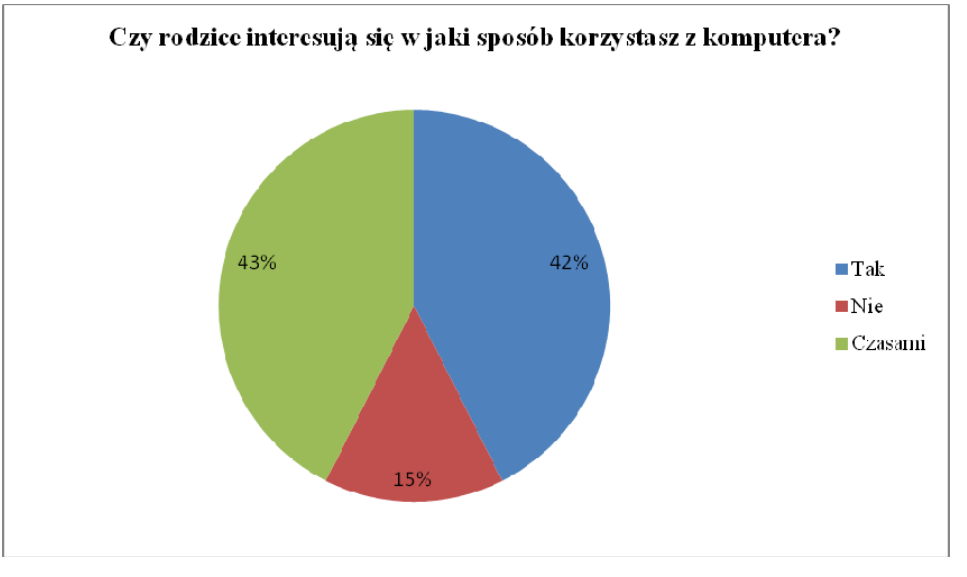
Znacząca grupa badanych dzieci oświadczyła, że może obyć się bez komputera. Jedynie 16% badanych wskazało, że ma z tym problem. Świadczy to o powstającym uzależnieniu od komputera wśród dzieci w wieku szkolnym. Problem ten dotyczy niewielkiej grupy uczniów, jednak należy wziąć pod uwagę młody wiek badanych. W okresie dorastania problem uzależnienia od komputera może dotknąć więcej dzieci.

Rysunek 7. Poziom uzależnienia od komputera



Źródło: badania własne.

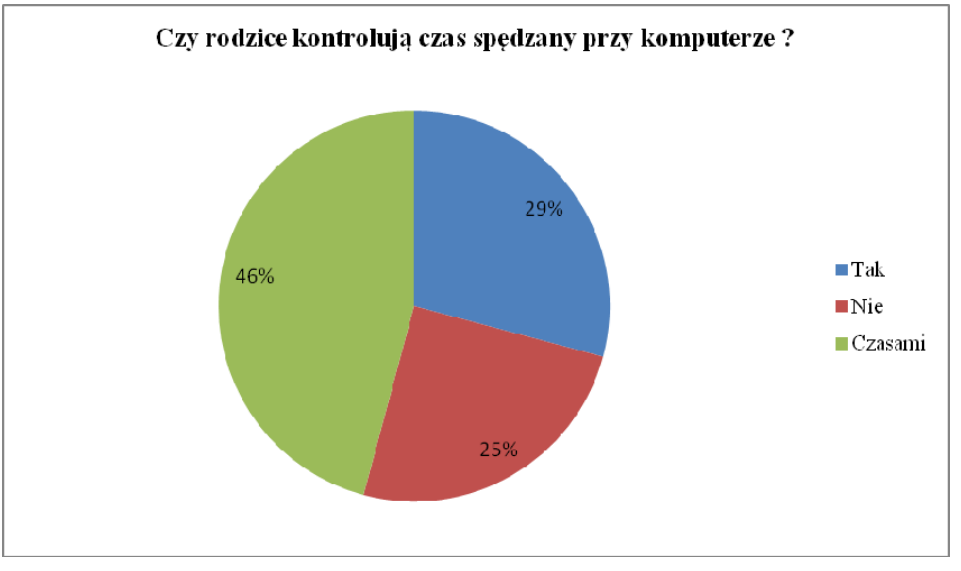
Rysunek 8. Zainteresowanie rodziców dotyczące wykorzystania komputera przez dzieci



Źródło: badania własne.

W ankietach dzieci wskazały, że większość rodziców (85%) interesuje się, w jaki sposób korzystają z komputera, w tym 43% robi to czasami. Jednak 15% badanych deklaruje, że zainteresowanie rodziców nie występuje w ogóle. Ich brak nadzoru sprawia, że dziecko jest pozostawione same sobie w świecie wirtualnym, gdzie może paść ofiarą ludzi o złych intencjach, bądź innych zagrożeń natury psychicznej. Czynnikiem, który powoduje brak zainteresowania rodziców może być ich brak wiedzy o zagrożeniach występujących w sieci, kluczowa zatem staje się odpowiednia edukacja opiekunów.

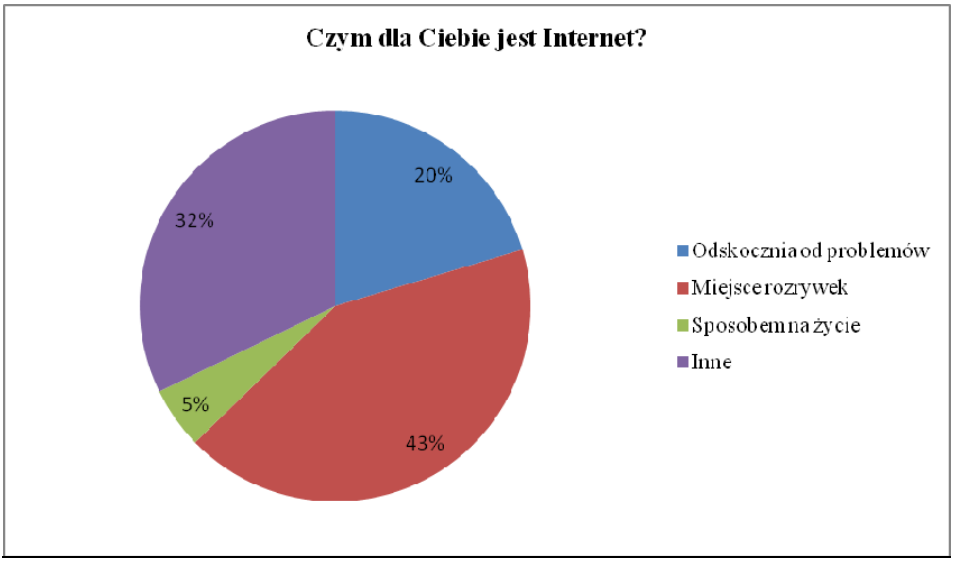
Rysunek 9. Kontrola rodzicielska czasu spędzanego przed komputerem



Źródło: badania własne.

Najczęściej (46%) rodzice sporadycznie kontrolują czas spędzany przed komputerem, jedynie w przypadku 29% badanych robią to przez cały czas. Z kolei 25% ankietowanych wskazuje, że kontrola rodzicielka nie występuje. Powyższe dane wskazują na możliwość wystąpienia uzależnienia wśród grupy badanych nieobjętych ograniczeniem czasowym w korzystaniu z komputera. Ponadto długie przesiadywanie dziecka przed komputerem może powodować jego problemy zdrowotne oraz psychiczne.

Rysunek 10. Ocena czym dla dzieci jest Internet

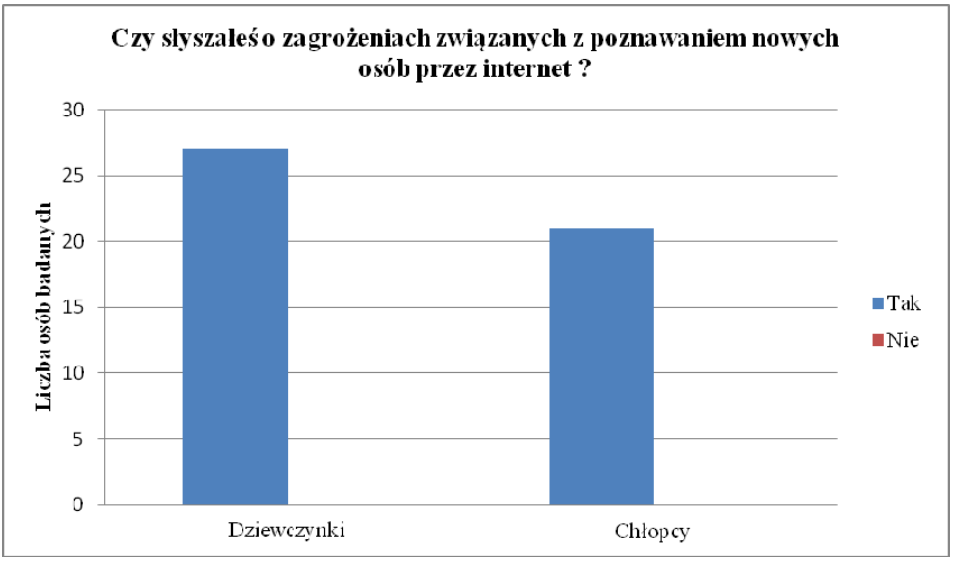


Źródło: badania własne.

Prawie połowa ankietowanych (43%) zaznacza, że Internet jest dla nich miejscem rozrywek. Znaczna część dzieci wskazuje, że poprawna odpowiedź nie znajduje się w ankiecie. Z kolei 5% badanych wskazuje, że jest to dla nich pewien sposób na życie. Część ankietowanych zaznaczyła, że Internet jest dla nich odskocznią od problemów. Wskazuje to, że dzieci, próbując rozwiązać swoje problemy w sieci mogą się narazić na nowe. Mogą bowiem obdarzyć zaufaniem niewłaściwe osoby, które pod pretekstem pomocy chcą zdobyć ich zaufanie. Wszystko to wskazuje na to, że dzieci, zamiast poprosić o pomoc rodziców. szukają rozwiązania problemu w złym miejscu.

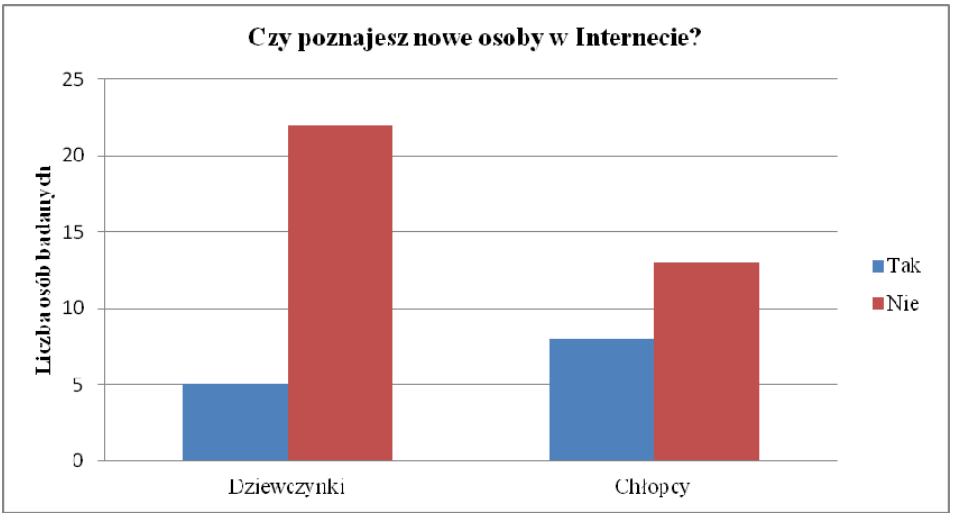
Zarówno dziewczynki, jak i chłopcy deklarują, że słyszeli o zagrożeniach związanych z poznawaniem nowych osób w Internecie. Odpowiedź przecząca w powyższym pytaniu nie występuje. Świadczy to o ich wiedzy na temat wiążących się z tym zagrożeń.

Rysunek 11. Zagrożenia związane z poznawaniem nowych osób przez Internet



Źródło: badania własne.

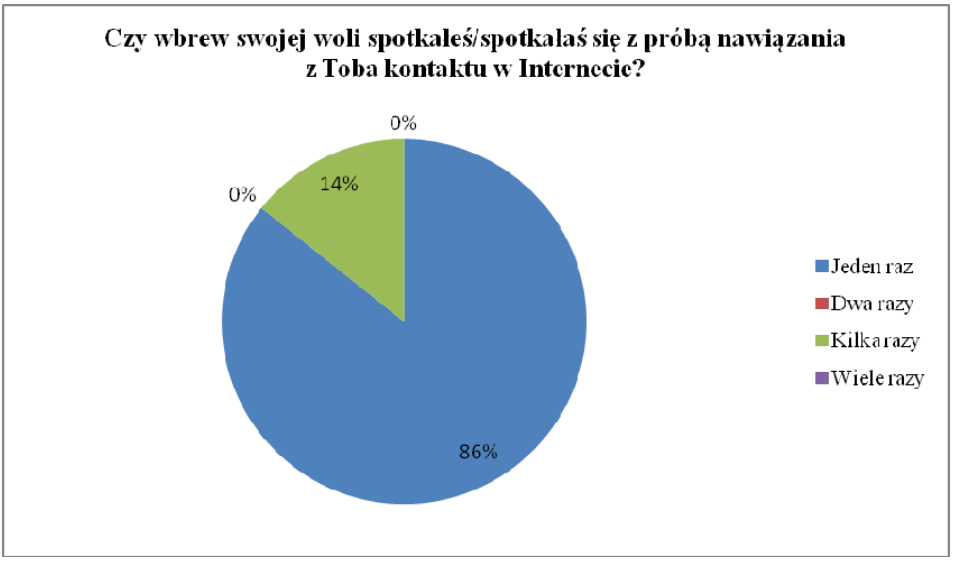
Rysunek 12. Nowe osoby poznawane w Internecie



Źródło: badania własne.

Większość badanych wskazuje, że nie szuka nowych znajomości w Internecie – dominującą grupą są tu dziewczynki. Z kolei u chłopców rozbieżność między odpowiedziami jest znacznie mniejsza. Wiedza na temat występujących zagrożeń związanych z poznawaniem nowych osób w Internecie może mieć wpływ na powyższe rezultaty. Z wykresu można wywnioskować, że dzieci niechętnie poznają w sieci nowe osoby.

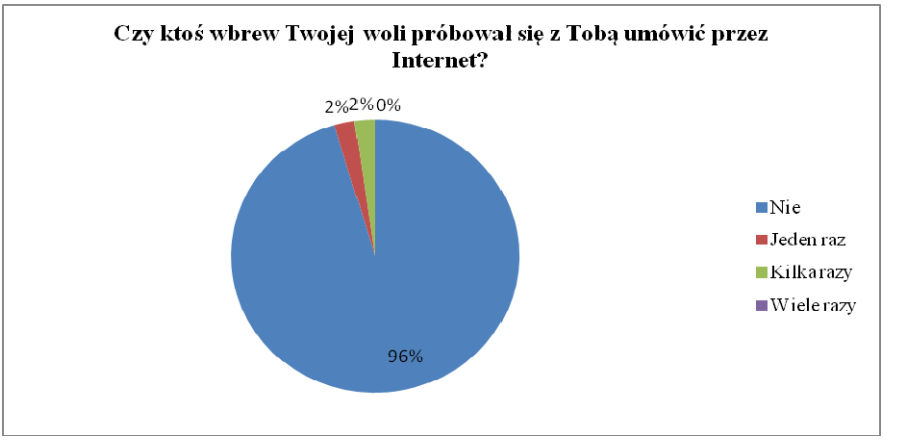
Rysunek 13. Próby nawiązania kontaktu w Internecie wbrew woli dzieci



Źródło: badania własne.

Na postawione pytanie aż 86% badanych dzieci wskazało, że wbrew ich woli próbowano nawiązać z nimi kontakt przez Internet. Z kolei 14% z nich deklaruje, że miało to miejsce kilka razy. Wielokrotne próby nie występowały w grupie badanych. Powyższe badania wskazują, że problem jest bardzo poważny. Należy zatem zwracać baczną uwagę z kim dziecko pisze czy jest to koleżanka, czy też osoba zupełnie obca oraz uświadomić dziecko, by poinformowało opiekunów natychmiast, gdy taki proceder ma miejsce.

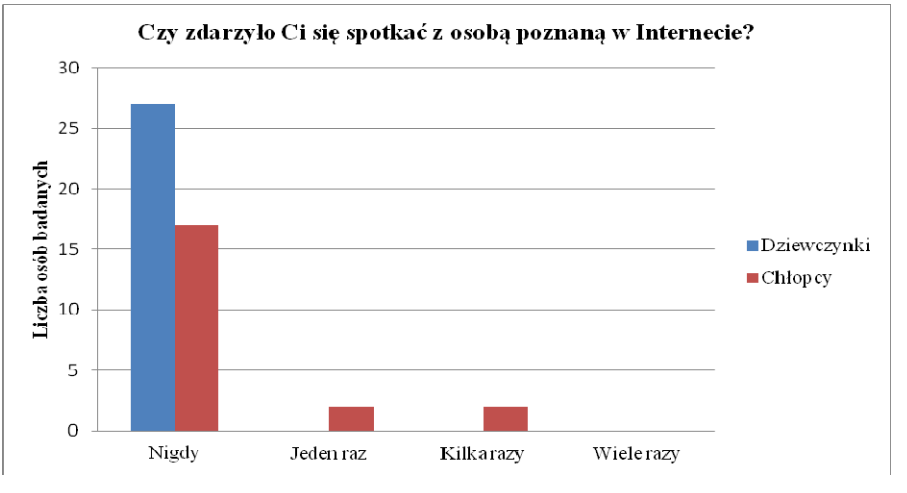
Rysunek 14. Próby umówienia się z dziećmi przez Internet wbrew ich woli



Źródło: badania własne.

Większość badanych (96%) deklaruje, że nigdy nie doszło do próby umówienia się z nimi przez Internet. Jednak 2% dzieci wskazało, że taka próba wbrew ich woli miała miejsce raz bądź kilka razy. Opiekunowie powinni zatem zwrócić uwagę, z kim koresponduje dziecko oraz przeciwdziałać w przypadku, gdy osoby obce próbują nawiązać z nim znajomość.

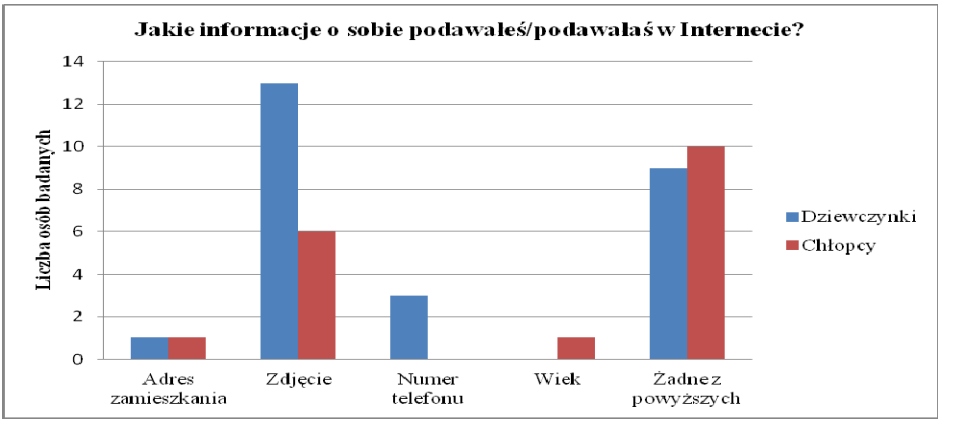
Rysunek 15. Spotkania z osobami poznanymi przez dzieci w Internecie



Źródło: badania własne.

Najwięcej badanych odpowiadało, że nigdy nie spotkało się z osobą poznaną w Internecie. Jedynie w grupie chłopców kilku wskazało, że parę razy doszło do spotkania. Spotkania te mogą być bardzo niebezpieczne dla dzieci, dlatego powinny odbywać się w obecności opiekunów. Jak wynika z przeprowadzonych badań proceder ten nie jest jednak częsty.

Rysunek 16. Informacje najczęściej podawane w Internecie przez dzieci



Źródło: badania własne.

Dzieci najczęściej deklarują, że udostępniały w Internecie swoje zdjęcie. Przeważającą grupą, która wskazała na powyższą odpowiedź są dziewczynki. Znacznie rzadziej udostępniany jest wiek czy adres zamieszkania. Z kolei duża grupa badanych nie udostępnia żadnych danych wskazanych w ankiecie. Wskazuje to na potrzebę kontroli, jakie dane są udostępniane przez dzieci oraz na jakich stronach. Publikowanie danych osobowych jest powszechnie stosowane przez większość społeczeństwa, jednak tak młodzi użytkownicy Sieci muszą wiedzieć co wolno publikować, a czego nie.

Wnioski

Dzieci w przedziale wiekowym 7–11 lat najczęściej korzystają z komputera w domu, w mniejszym stopniu w szkole czy bibliotece. Młode pokolenie potrafi dziennie spędzić średnio 2 godziny przed monitorem, rzadko zdarzają się osoby, które poświęcają znacznie więcej czasu, powyżej 3 godzin. Sam czas spędzany przed komputerem, nie stanowi zagrożenia ponieważ jest zbyt krótki.

Głównym celem przesiadywania dzieci przed komputerem są gry. Dopiero w dalszej kolejności jest on wykorzystywany do zdobywania wiedzy. Część ankietowanych

deklaruje, że nie potrafi obejść się bez komputera. Badania wskazały, że w tak młodym wieku stopniowo pojawiają się objawy uzależnienia.

Czas spędzany przed komputerem, jak i poczynania dziecka w Internecie są w znacznej mierze kontrolowane przez rodziców. Opiekunowie interesują się, co ogląda w cyberprzestrzeni oraz ile czasu jest na to poświęca. Zaledwie niewielka część badanych wskazuje, że w żaden sposób nie jest kontrolowana, co stwarza podstawy do nadużywania przez nich czasu spędzanego przed komputerem i może z czasem powodować ich uzależnienie.

Dzieci deklarują, że Internet stanowi dla nich miejsce rozrywek. Do surfowania po nim wykorzystują głównie smartfon, dopiero w dalszej kolejności komputer. Korzystanie z urządzeń mobilnych sprawia, że dziecko może z dowolnego miejsca korzystać z Internetu, nie podlegając tym samym jakiejkolwiek kontroli.

Większość dzieci zaznacza, że najczęściej publikują w cyberprzestrzeni swoje zdjęcie. Rzadziej udostępniają numer telefonu czy adres zamieszkania. Należy zatem zwracać szczególną uwagę na edukację dzieci w zakresie ochrony informacji oraz skutków podawania danych wrażliwych. Będą one tym samym skuteczniej zabezpieczone przed potencjalnymi zagrożeniami.

W większości dzieci wskazywały, że nie poznają nowych osób w Internecie, jednak pojawiały się próby nawiązania z nimi kontaktu wbrew ich woli. Do spotkań z osobami w Sieci praktycznie nie dochodziło.

Dzieci znają zagrożenia występujące w Internecie, ale powinny być gotowe do zapobiegania im w stosownym momencie. Odpowiedzialność za ich przygotowanie spoczywa na opiekunach, którzy również muszą posiadać niezbędną wiedzę w tym zakresie. W „Zakończeniu" zostaną przedstawione odpowiednie metody przeciwdziałania zagrożeniom występującym w cyberprzestrzeni, które będą pomocne zarówno dla rodziców, jak i dzieci.

Zakończenie

W związku z pojawieniem się nowego środowiska wytworzonego przez rozwój technologiczny pojawiły się nowe zagrożenia. Długie godziny spędzane przed komputerem powodują wiele dolegliwości fizycznych. Dzieci narażone się tym samym na coraz częstsze wady postawy czy bóle stawów. Ponadto korzystanie z cyberprzestrzeni powoduje wiele zagrożeń psychicznych, które w konsekwencji mogą doprowadzić do różnego rodzaju zaburzeń czy poważnych chorób natury psychicznej. Dochodzą to tego zagrożenia społeczne, które sprawiają że dziecko ma problemy z odróżnieniem tego co jest fikcją, a co rzeczywistością. Dodatkowo korzystanie z różnych portali spo-

łecznościowych sprawia, że kontakt dziecka z otoczeniem jest ograniczony do minimum, tym samy zanika interakcja z rówieśnikami, w wyniku czego zdolności komunikacyjne młodego pokolenia są coraz słabsze.

Cyberprzestrzeń jest miejscem wykorzystywanym przez niektóre osoby do własnych egoistycznych celów bądź do celów zarobkowych. Reklamy propagujące strony o nieodpowiedniej treści pojawiają się w miejscach, z których korzystają dzieci. Z kolei tzw. wyskakujące okienka są w stanie przekierować użytkowników Sieci bezpośrednio na stronę z pornografią. Kontakt dzieci, których umysły dopiero się rozwijają z takimi treściami może być bardzo niebezpieczny. Do tego dochodzi pedofilia, gdyż wiele osób wykorzystuje Internet do wyszukiwania potencjalnych ofiar – pedofile często korzystają z portali społecznościowych oraz różnego rodzaju for. Kontakt w Internecie jest ograniczony, tym samy zboczeńcy mogą podawać się za dowolną osobę i nawiązać kontakt z dzieckiem, które może stać się ich ofiarą.

Należy pamiętać, że cyberprzestrzeń, nie jest miejscem, gdzie występują jedynie zagrożenia. Internet to także wspaniałe miejsce, gdzie dziecko może znaleźć różnego rodzaju informacje, pogłębiać swoją wiedzę czy rozwijać swoje zainteresowania. Aby było bezpieczne, należy jednak zapewnić mu jak najskuteczniejszą ochronę, tak żeby występujące zagrożenia nie doprowadziły do tragedii.

Najskuteczniejszą formą ochrony dzieci w cyberprzestrzeni jest edukacja młodego pokolenia, która powinna być realizowana zarówno przez rodziców, jak i szkołę. Przekazywanie wiedzy o występujących zagrożeniach od najmłodszych lat w dużej mierze przyczyni się do zwiększenia bezpieczeństwa dzieci w cyberprzestrzeni. Dzięki takiemu działaniu młode pokolenie będzie świadome czekających je niebezpieczeństw, co będzie skutkowało ich większą ostrożnością. Dodatkowym rozwiązaniem, które będzie zmniejszało kontakt dziecka z występującymi zagrożeniami są programy filtrujące. Dzięki nim, podczas nieobecności rodziców, będzie miało ono utrudniony kontakt z treściami przeznaczonymi dla dorosłych oraz różnego rodzaju forami uznanymi za niebezpieczne. Ponadto dzięki programom rodzic będzie miał możliwość prześledzenia działalności swojego dziecka w Internecie – dzięki rejestrowaniu historii odwiedzanych witryn.

Najważniejszym elementem zapewniającym bezpieczeństwo dzieci jest zainteresowanie ze strony rodzica oraz stosowana kontrola, która nie będzie możliwa bez dostatecznej wiedzy na temat występujących zagrożeń oraz sposobów im przeciwdziałania. Dlatego tak ważna jest edukacja zarówno dzieci, jak i opiekunów, którzy taką kontrolę sprawują. Pomocne w tym mogą okazać się różnego rodzaju poradniki, które są dostępne w formie elektronicznej, bądź papierowej. Dzięki nim rodzic bez wychodzenia z domu może dowiedzieć się, w jaki sposób zapobiegać zagrożeniom.

Bibliografia

Andrzejewska A., Bednarek J. (2017), *Społeczno-edukacyjne konteksty przemian informacyjno-cywilizacyjnych*, „Zeszyty Naukowe Uczelni Warszawskiej", nr 1(55), s. 9.

Barney D. (2008), Społeczeństwo sieci, Wydawnictwo Sic, Warszawa.

Bednarek J. (2002), *Media w edukacji*, Mikom, Warszawa.

Bełza L. (2011), *Główne zagrożenia w obecnym i przyszłym środowisku bezpieczeństwa pozamilitarnego*, „Bezpieczeństwo Narodowe", tom 18, s. 121–137.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej (2015), Biuro Bezpieczeństwa Narodowego, Warszawa.

Gidens A. (2010), *Nowoczesność i tożsamość*, Wydawnictwo Naukowe, PWN, Warszawa.

Kopczewski M. (2014), *Młodzież w cyberprzestrzeni – wyniki badań,* [w:] M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Difin, Warszawa.

Kopczewski M., Dudzik I. (2012), *Zagrożenia jakie niesie korzystanie z cyberprzestrzeni*, „Modele Inżynierii i Teleinformatyki", tom 7, s. 79–92.

Liedel K. (2011), *Bezpieczeństwo informacyjne państwa*, [w:] K. Liedel (red.), *Transsektorowe obszary bezpieczeństwa*, Difin, Warszawa.

Skrabacz A. (2012), *Bezpieczeństwo społeczne. Podstawy teoretyczne i praktyczne,* Elipsa, Warszawa.

Wojciechowska-Filipek S., Ciekanowski Z. (2016), *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki-organizacji-państwa*, CeDeWu, Warszawa.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **127–138**

Nina Stępnicka[1]
Wydział Nauk Społecznych, Katedra Bezpieczeństwa Narodowego
Uniwersytet Jana Kochanowskiego w Kielcach, Filia w Piotrkowie Trybunalskim

Bezpieczeństwo transakcji finansowych i dystrybucji produktów i usług w Dark Necie

Security of the Financial Transactions and Distribution of Products and Services in the Dark Net

Abstract: The Dark Net is a difficult to estimate part of the Deep Internet, which has been deliberately hidden and is not available for users of the standard search engines. The resources of the Dark Net involve criminal trade and services, but there is also some difficult to estimate part, which does not exceed beyond the boundaries of the law. Currencies used in the Dark Net is Bitcoin, Monero and Ethereum, and other means of payment are anonymous payment cards (paysafecard). From the point of view of the security of the economy, illegal contents of the Dark Net is a threat, both for the functioning and safety of the various sectors that are part of it, as well as other areas of social and political life etc. It generates a loss in the budget of all states, which users use its illegal resources, but also it violates public policy and economic governance in the world, with cyber attacks, cyberterrorism and other forms of crime and illegal activities.
Key words: the Dark Internet, the security, cryptomarket, Bitcoin, economy.

Wstęp

Dark Net (w tłumaczeniu na język polski: ciemny Internet, mroczny Internet, ciemna sieć; ang. Dark Internet, Dark Web[2], zwany także Underground Web i Hidden Services

[1] n.stepnicka@unipt.pl.
[2] W dalszej części pracy pojęcia Dark Net, Dark Internet, Dark Web, ciemny Internet, ciemna sieć itp. będą stosowane zamienne.

tj. ukryte usługi) to jedna z najbardziej enigmatycznych przestrzeni (vel pokładów) Internetu, z jednej strony wywołujących coraz większe zainteresowanie, zaś z drugiej stanowiących przedmiot licznych dyskusji i kontrowersji. Ciemny Internet nie jest żadną oddzielną (osobną) siecią, lecz stanowią go specjalne protokoły i aplikacje ulokowane i korzystające z istniejących już sieci. Ta szczególna przestrzeń Internetu, będąca komponentem innej sieci, tzw. głębokiego Internetu (ang. Deep Internet), dostępna jest jedynie dla określonych użytkowników lub grup użytkowników.

Celem pracy jest próba identyfikacji zagrożeń, jakie niesie ze sobą Dark Net oraz oszacowania jej rozmiarów, istotnych z punktu widzenia bezpieczeństwa ekonomicznego i funkcjonowania gospodarki. Praca ma charakter opisowy i może stanowić przyczynek do bardziej pogłębionych badań i analiz. Wprowadzenie do rozważań dotyczących wpływu Dark Netu na gospodarkę poprzedzają m.in. krótka jego charakterystyka wraz z uwzględnieniem rodzajów aktywności gospodarczych i określenie mechanizmu przepływów finansowych, jakim podlegają transakcje w analizowanej części Internetu.

Struktura i zawartość (bezpieczna i niebezpieczna) Dark Netu

Termin „Dark Net" został utworzony w 2002 r. przez programistów firmy Microsoft [Cusack 2015, s. 131], podczas gdy pierwsze oznaki jego funkcjonowania pojawiły się już w połowie lat 90. XX wieku [Hanson 2016, s. 117]. Dark Net stanowi fragment tzw. Deep Internet, czyli głębokiego Internetu[3], który tworzą z reguły legalne katalogi i bazy danych (wymagające haseł i kluczy) i w odróżnieniu od niego Dark Net to ta część Internetu, która została celowo ukryta i jest niedostępna dla użytkowników korzystających ze standardowych wyszukiwarek internetowych (np. Google, Bing, Chrome, Firefox, Safari etc.). Zawartość Dark Netu tworzą różne serwisy i strony online (sklepy, aukcje, fora dyskusyjne, poczta e-mail, materiały archiwalne, warsztaty etc.), jakie funkcjonują w *open web*, tyle że z zachowaniem pełnej anonimowości. Zasoby Dark Netu sklasyfikowane są w ponad 30 językach, z czego blisko 80% stanowią informacje w języku angielskim, 4% w języku niemieckim, blisko 4% w języku chińskim i niecałe 3% w innych językach[4] [DeepLight, 2016, s. 8].

[3] Deep Internet to jedna ze struktur Internetu, do którego zaliczany jest także sieć indeksowana *open web*, czyli otwarty obszar (in. otwarty Internet), z którego korzystają miliardy użytkowników na całym świecie. Zawartość Deep Web jest 500-krotnie razy większa niż pokłady open web, która indeksuje 1,3 miliarda stron internetowych [DeepLight, 2016, s. 5]. W układzie procentowym wartości przypadające na poszczególne „pokłady" Internetu rozkładają się następująco: sieć indeksowana (tj. *open Internet*, in. *Surface Web*) – około 4%, Deep Net – 90%, Dark Web – 6%.

[4] Tj.: amharskim, bułgarskim, duńskim, fińskim, francuskim, greckim, gruzińskim, hebrajskim, hiszpańskim, holenderskim, irlandzkim, kantońskim, koreańskim, kurdyjskim, luksemburskim, malajskim, maltań-

Ahmed El Azab, Mahmood A. Mahmood i Abd El-Aziz podają, że stosunkowo dobrze znanym źródłem treści znajdujących się w ciemnym Internecie jest tzw. sieć Tor (skrót od The Onion Routing), będąca siecią anonimową i narzędziem do szyfrowania, do której dostęp możliwy jest za pośrednictwem wyszukiwarki internetowej Tor, bądź sieć udostępniania plików I2P (tj. Invisible Internet Project), oparta na zasadach działania sieci *peer-to-peer* [2017, s. 248].

W pierwszym ze wspomnianych narzędzi, Dark Net wykorzystuje mechanizm tzw. trasowania cebulowego (ang. *onion routing*), opracowanego de facto w latach 90. XX wieku przez amerykańskie agencje rządowe oraz naukowców z Laboratorium Badawczego Marynarki Wojennej (US Naval Research Laboratory) i Agencji Zaawansowanych Projektów Badawczych (DARPA) celem stworzenia systemu bezpiecznej komunikacji dla wojska i wywiadu. W odróżnieniu od trasowania, sieć I2P powstała w oparciu o modyfikację sieci Freenet i pozwala na „dzielenie ciągłego strumienia danych na mniejsze części, czyli tzw. pakiety" [Lech 2015, online][5].

Zasoby Dark Internetu wyraźnie różnią się od zasobów otwartego Internetu i dotyczą np. handlu i usług o charakterze przestępczym czy zarządzania złośliwym oprogramowaniem. W Dark Necie aktywność prowadzą głównie ci, którzy pragną być anonimowi, np.: oszuści, podżegający do przemocy, paserzy, handlarze pirackimi kopiami filmów, towarami luksusowymi, bronią i materiałami wybuchowymi, fałszywymi banknotami, kradzionymi dokumentami tożsamości i danymi (pochodzącymi z kont bankowych, kont PayPal, kart kredytowych etc.), nielegalnymi informacjami, licencjami, oprogramowaniem, dziecięcą pornografią, lekami, żywym towarem itp., fałszerze usług związanych z dokumentacją, dealerzy narkotyków i środków dopingujących, przestępcy, pedofile, hakerzy, członkowie organizacji terrorystycznych etc. Znaczna część nielegalnych transakcji w Dark Necie to typowe oszustwa, polegające

skim, norweskim, ormiańskim, polskim, portugalskim, rosyjskim, rumuńskim, szwedzkim i włoskim [DeepLight, 2016, s. 8].

[5] Trasowanie cebulowe polega kolejno na wielowarstwowym szyfrowaniu danych, przesyłaniu ich przez szereg węzłów (tzw. routerów cebulowych), a następnie rozszyfrowywaniu w taki sposób, by z punktu widzenia docelowego komputera ruch pochodził z wyjściowego węzła sieci Tor. Taka procedura postępowania skutkuje ukryciem źródła danych (gdyż serwery funkcjonują w formie usług o ukrytej lokalizacji) oraz większą anonimowością, będącą konsekwencją wielowarstwowego szyfrowania po stronie użytkownika Internetu i serwisu, stanowiącego zasób Dark Netu. Z kolei sieć I2P pozwala na przesyłanie wiadomości pomiędzy kolejnymi węzłami sieci. „Wiadomości mogą być zamykane w strukturze zwanej główką czosnku (ang. *garlic*), która zawiera też informację o bardzo krótko <<żyjącym>> tunelu nadawczym, za pośrednictwem którego wysyłana jest paczka. Podczas przesyłania informacji stosowane jest szyfrowanie na czterech warstwach: wiadomości (zaszyfrowanie danych użytkownika, przesyłanych od węzła źródłowego do docelowego), główki czosnku (zbiór wiadomości już wcześniej zaszyfrowanych z informacjami na temat trasy), wewnątrz tunelu (informacje <<wtłaczane>> do tunelu) i między bramami różnych tuneli" [Lech 2015, online].

na wyłudzaniu pieniędzy, zagrażające bezpieczeństwu gospodarczemu w skali mikro-, jak również makro.

Z drugiej strony Dark Net obejmuje także aktywność niewykraczającą poza granice obowiązującego prawa. Medium to pełni rolę platformy komunikacji m.in. dla ludzi z różnych krajów, których prawo nie pozwala swoim obywatelom na tworzenie platform pozwalających na swobodną wymianę informacji i poglądów, przesyłanie, publikowanie, przeglądanie stron internetowych [Aschmann, Leenen i Viuureen 2017, s. 16]. Jak podaje M. Puczyński, ten pozytywny wymiar funkcjonowania Dark Netu dotyczy również whistleblowingu, tj. „demaskowania nieuczciwej działalności w organizacjach publicznych i korporacjach" [2016, online], mechanizmu publikacji informacji w przypadku śmierci lub zaginięcia ich posiadacza, bezpiecznego kontaktu, prywatnych rozmów bez podsłuchu, jak również stanowi miejsce pracy niezależnych społecznych aktywistów, dysydentów oraz dziennikarzy, a nawet trolli, który obawiają się o swoje bezpieczeństwo. Ponadto analizowany fragment Dark Netu obejmuje legalny ruch przesyłany przez różne firmy technologiczne, takie jak np.: Facebook czy Departament Stanu Stanów Zjednoczonych i inne organizacje rządowe [Patterson 2016, online].

Według badań pt.: „Deeplight", przeprowadzonych przez firmy Intelliagg i Darksum w kwietniu 2016 r., liczba stron internetowych, przypisanych do mrocznej sieci o rozszerzeniu „.onion" wynosiła nie więcej niż 30 tysięcy funkcjonujących w tym samym czasie. To zdecydowanie mniej niż zakładają statystyki innych firm i agencji badawczych. Ponadto analiza dostępnych danych wykazała, że 48% stron zawiera treści zabronione przez prawo: pornografię, dane skradzionych kart kredytowych, pomoc w nielegalnych operacjach finansowych, fora służące do sprzedaży narkotyków etc. Pozostałą zawartość Dark Netu stanowią informacje, które nie naruszają prawa [Józefiak 2016, online][6].

System finansowy Dark Netu

System finansowy Dark Netu zbudowany jest w oparciu o tzw. metodę *paysafecard*, która nie wymaga podawania danych osobowych, numeru konta bankowego czy karty kredytowej, jak również kryptowaluty (ang. *cryptocurriencies*), zwane wirtualnymi walutami alternatywnymi, będące zaszyfrowanym umownym środkiem płatniczym

[6] Jak wynika z Deeplight, specjalistom Intelliagg i Darksum udało się przeanalizować 46% stron Dark Netu, do których mieli dostęp. Pozostałe 54% Dark Netu to adresy stron, jakie pojawiały się „przez chwilę" i trudno oszacować, jaka jest ich zawartość, aczkolwiek stwierdzono, że są to serwery, które zazwyczaj służą wymianie danych, obsłudze chat-roomów lub zarządzaniu złośliwym oprogramowaniem [Józefiak 2016, online].

wykorzystywanym przez określoną grupę, stanowiącym alternatywę wobec walut tradycyjnych i posiadającym charakter wirtualny [Kurek 2014, s. 190; Stępnicka 2017, ss. 125–137].

Jedną z walut najczęściej używanych w transakcjach Dark Netu jest Bitcoin, przyjmujący postać cyfrowego kodu, będącego elektronicznym ciągiem indywidualnych i niepowtarzalnych znaków [Rodwald 2013, ss. 91–102]. Pozorne bezpieczeństwo, jakie zapewnia ta wirtualna waluta, wynika z jej nieuregulowanego charakteru, anonimowości płatności, a także wahań jej wartości. Jak podkreślają Ira Winkler i Araceli T. Gomes [2016, s. 74], anonimowe wykorzystanie Bitcoina w transakcjach handlowych sprawia, że waluta ta wielokrotnie wykorzystywana jest w oszustwach online, także dokonywanych w Dark Necie. Za Jerry Brito i Andrea Castillo przykładami takiego użycia Bitcoina mogą być finansowanie działań terrorystycznych czy handel nielegalnymi towarami [2013, s. 26].

W rzeczywistości Bitcoin nie jest całkowicie anonimowy, ponieważ opiera się na wspólnym rejestrze, pokazującym wszystkie transakcje portfela płatności [Bhardwaj 2017, s. 55]. Z punktu widzenia Dark Netu i transakcji w nim dokonywanych najważniejszymi cechami Bitcoina są [Stępnicka 2017, ss. 129–130]:

- brak fizycznego korelatu, który zastąpiony został formą cyfrową zapisaną w systemie;
- dokonywanie transakcji z wykorzystaniem systemu *peer-to-peer*, tj. bez udziału instytucji finansowych oraz centralnego emitenta upoważnionego do emisji i kreowania polityki pieniężnej;
- globalny zasięg, nieodwracalność i natychmiastowość transakcji.

Przykładami innych kryptowalut chroniących prywatność finansową w Dark Necie są także Monero i Ethereum. Nie są one pochodnymi Bitcoina, ale bytami „samymi w sobie", które wyróżnia „dziwny paradoks prywatności", przez co uchodzą za typowe „waluty zła", wykorzystywane m.in. przez organizacje kryminalistyczne. W porównaniu z Bitcoinem, Monero i Ethereum, określane są jako bezpieczne zdecentralizowane księgi transakcji, które wyróżniają ponadto skalowalność oraz anonimowość, zapewniająca praktycznie całkowitą niemożliwość wykrycia. Monero największą popularność zyskała w 2016 r., kiedy użytkownicy Dark Netu zdecydowali się używać jej do nielegalnych transakcji, co sprawiło, że waluta ta stała się jeszcze bardziej wartościowa [Richmond 2017, s. nlb]. O coraz większej popularności kryptowalut w handlu w Dark Necie świadczą dane m.in. z 2016 r., kiedy cena Bitcoina wzrosła dwukrotnie, Ethereum dziesięciokrotnie, zaś Monnero około 27-krotnie [Greenberg 2017, online].

Czarny rynek w Dark Necie a bezpieczeństwo

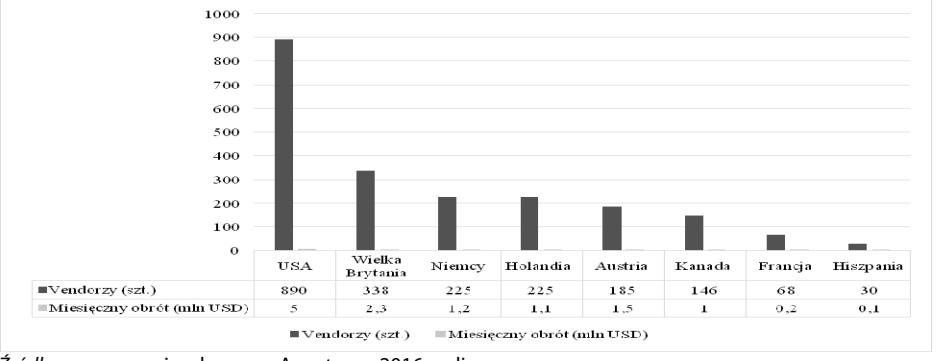
Istotnym z punktu widzenia rozważań pracy i bezpieczeństwa gospodarczego wydają się pojęcia czarnego rynku (ang. *black market*), kryptorynku (ang. *cryptomarket*), rynku Dark Net (ang. *darknet market*) lub oszukańczych ryków (ang. *fraudulnet markets*), na którym funkcjonują komercyjne strony internetowe, działające za pośrednictwem Dark Netu.

Na czarnym rynku Dark Netu funkcjonują m.in:

- aukcje internetowe, mające postać typowych list przedmiotów oferowanych do sprzedaży, przygotowanych na wzór serwisu eBay, wraz z uwzględnieniem zaawansowanych funkcji związanych z wyszukiwaniem, oceną, systemem reputacji i wysyłką [Williams 2017, s. 94];
- markety, zwane rynkami zaproszeń, skierowanymi do konkretnych odbiorców (ang. *Invite/ Referral Only Markets*), wymagające kodu oraz linku referencyjnego umożliwiających wejście na stronę, rejestrację oraz dokonanie zakupów;
- markety z opcją *multisig* (ang. *Multisig or Trusted*), czyli zwielokrotnionym wskaźnikiem bezpieczeństwa niż w innych marketach i sklepach oraz z gwarancją obsługi klienta będącą istotnym wyróżnikiem produktów i usług, które mogą być reklamowane lub zwrócone na wypadek „wadliwości" (np. w przypadku wadliwych kart płatniczych etc.);
- sklepy z opcją Escrow (ang. *Escrow Markets*), udostępniające opcję depozytu i natychmiastowej finalizacji;
- tzw. *vendors shop*, czyli strony, które nie są marketami, ale należą do indywidualnych sprzedawców, którzy za ich pośrednictwem mogą dokonywać dystrybucji różnych dóbr i usług;
- rynki internetowe obsługiwane w innych językach niż język angielski (ang. *Markets For Specific Languages/Countries*);
- nowe rynki (ang. *New Markets&Under Construction*), jeszcze nieniezweryfikowane [por.: Darkmarkety, 2015, online].

W 2016 r. największy udział w tworzeniu czarnego rynku w Dark Necie miały Stany Zjednoczone, gdzie strony internetowe z różnymi ofertami prowadziło blisko 900 dostawców, zaś miesięczny obrót ze sprzedaży w Dark Necie wynosił 5,0 mln USD. Na drugim miejscu ukształtowała się Wielka Brytania, dla której liczba dostawców w badanym okresie wynosiła około 340, zaś obrót 2,3 mln USD [Armstrong 2016, online]. Liczbę sprzedających i miesięczny obrót sprzedaży w Dark Necie w 2016 r. przedstawia rysunek 1.

Rysunek 1. Liczba sprzedających (tzw. vendorów) i miesięczny obrót sprzedaży w Dark Necie w 2016 r.



Źródło: opracowanie własne za: Armstrong 2016, online.

Z uwagi na anonimowość (tzw. anonimizację danych), będącą najważniejszą cechą tej części Internetu, Dark Net uławia przestępczość związaną głównie z narkotykami, w szczególności ich produkcją i sprzedażą detaliczną [Martin 2014, s. 3]. Według danych holenderskiego think-tanku Rand, przestępczość narkotykowa i handel nielegalnymi substancjami stanowi około 57% całkowitej sprzedaży w Dark Necie [Dark Net 2016, online].

Jak podaje europejski raport narkotykowy z 2017 r.: „Według ostatniego badania dotyczącego sprzedaży na 16 głównych rynkach tego rodzaju w latach 2011–2015, szacuje się, że sprzedaż narkotyków stanowiła ponad 90% całkowitych przychodów finansowych globalnych serwisów sprzedażowych w Dark Necie. Zgodnie z doniesieniami prawie połowa (46%) całej sprzedaży generowana była przez sprzedających z Europy, co stanowiło łącznie szacunkową kwotę 80 mln euro przez cały okres prowadzenia badania. Głównymi europejskimi krajami pochodzenia, według wolumenu sprzedaży, były Niemcy, Holandia oraz Wielka Brytania, przy czym za większość przychodów odpowiadały stymulanty, a w szczególności MDMA i kokaina" [Europejski 2017, s. 20].

Według Brendyna Lotza, „społeczność narkotykowa ma charakter samoregulujący, nawet samokontrolny. Sprzedawcy polegają na recenzjach i komentarzach, aby budować swoją markę i generować zamówienia. Nowi dostawcy szybko oferują bezpłatne próbki, a społeczność z przyjemnością testuje nowy produkt. Recenzje są zgodne ze standardowym szablonem, w którym użytkownicy oceniają czas wysyłki, czystość, ogólne doświadczenia związane z dostawą i sprzedawcą. Społeczność szybko unika oszustów, gdy pojawiają się ostrzeżenia o znikających paczkach lub gdy kupujący otrzymują mniej, niż połowę tego, za co zapłacili" [Lotz 2017, online].

Przykładem pierwszego serwisu, działającego tylko na czarnym rynku w Dark Necie i zajmującego się m.in. dystrybucją narkotyków, był Silk Road (pol. Jedwabny Szlak)[7], zwany „narkotykowym eBayem" (ang. „eBay of illicit drugs") lub „narkotykowym Amazonem". Podobnie, jak ten najpopularniejszy na świecie serwis aukcyjny, Silk Road wyposażony był w usługi Escrow, system płatności elektronicznych (Bitcoin) oraz system *vender feedback*, pozwalający na ocenę transakcji [Williams 2017, s. 91]. Twórcą Silk Road był Ross Ulbricht (pseud. „Dread Pirate Roberts"). Za pośrednictwem serwisu można było kupić leki, narkotyki, jak również inne legalne i nielegalne produkty. Serwis ten funkcjonował w Dark Necie od lutego 2011 r. do października 2013 r. Zarejestrowanych w nim było kilka tysięcy kont sprzedawców i ponad sto tysięcy kont kupujących, którzy w badanym okresie dokonali blisko dwa miliony transakcji. Dane wykazują, że wartość transakcji dokonywanych w ciągu jednego miesiąca w serwisie wynosiła około 1,2 mln USD, zaś całkowity przychód serwisu w latach 2011–2013 szacowany był na 213 milionów USD.

Zamknięcie Silk Road nie przyczyniło się jednak do wyeliminowania nielegalnego handlu w Dark Necie [Sammons 2015, s. 146]. Jak podają Jerry Brito i Andrea Castillo [2013, s. 25], Devin Williams [2017, s. 93] i Pierluigi Paganini [2014, online], przedsięwzięciami funkcjonującymi na czarnym rynku Dark Netu po Silk Road były: Black Market Reloaded, AlphaBay, TheRealDeal, Sheep Marketplace, Utopia, Black Goblin Market, CannabishRoad, Black Bank, Bloomsfield, Babylon, OpenBazar, Silk Market 2.0. i inne (tabela 1).

Według badań European Monitoring Centre for Drugs and Drug Addiction (EMCDDA), w latach 2011–2017 największymi źródłami nielegalnej sprzedaży narkotyków w Dark Necie były Niemcy, Wielka Brytania, Holandia oraz Belgia. W badanym okresie sprzedawcy narkotyków w tych trzech krajach osiągnęli łączny przychód w wysokości kolejno: 26,6 mln euro, 20,3 mln euro, 17,9 mln euro i 5 mln euro, co w przypadku łącznego przychodu Niemiec, Wielkiej Brytanii i Holandii stanowi zdecydowanie więcej, aniżeli wielkość przychodów uzyskanych przez pozostałe kraje Unii Europejskiej łącznie. Sprzedawcy w tym kraju, którzy w tym okresie osiągnęli czwarty najwyższy przychód, Belgia, nabyli mniej niż 5 milionów euro w tym samym okresie [Tharoor 2017, online].

[7] Jednym z pierwszych przykładów serwisów prowadzących sprzedaż nielegalnych produktów w Dark Necie był The Farmers' Market, założony w 2006 r. i przeniesiony do Dark Netu w 2010 r. W 2012 r. serwis został zlikwidowany. Uchodzi on za protoplastę kolejnych serwisów, jakie powstawały w Dark Necie.

Tabela 1. Wybrane sklepy w Dark Necie i ich oferta

Nazwa sklepu (aukcji) online	Oferowane produkty i usługi
Agora Marketplace	narkotyki
AlphaBay Market	usługi hackowania, inne oszustwa
Andromeda Market	narkotyki
Babylon (Włochy)	leki, narkotyki
Black Bank Market	narkotyki
BlueSjy Marketplace	narkotyki
Evolution Marketplace	dziecięca pornografia, kradzione karty kredytowe, usługi płatnych morderstw, zabójstw, terroryzm, prostytucja, schematy Ponziego (tj. piramidy finansowe) i loterie
Outlaw Market	narkotyki
Pandora Openmarket	narkotyki
Silk Road	trucizny i broń masowego rażenia, zabójstwa, kradzione karty kredytowe etc.
The Pirate Matket	narkotyki
Tor Bazar Alpha	narkotyki

Źródło: opracowanie własne za: Williams 2017, s. 95; Paganini 2014, online.

Z kolei badania Rand z 2016 r. wykazały, że większość vendorów narkotykowych w Dark Necie zarabia od 10,5 mln do 18,5 miliona euro miesięcznie, z czego 70% dochodu stanowi sprzedaż marihuany (konopi indyjskich), ekstazy i środków pobudzających, a najwyższy udział w zakupach stanowią transakcje hurtowe o wartości 1 tys. USD i więcej. Najwięcej dostawców narkotykowych funkcjonuje w Stanach Zjednoczonych (około 3,9 tys.) i generują oni 36% światowego przychodu sprzedaży narkotyków o wartości około 5,0 mln euro. Na drugim miejscu znajduje się Wielka Brytania (338 sprzedawców) i Niemcy (225 sprzedawców) [Dark Net 2016, online].

Resumując, likwidacja Dark Netu wydaje się niemożliwa. Tę gospodarczą stronę ciemnego Internetu można zaliczyć do szarej strefy o charakterze online tyle, że bardziej rozbudowanej pod względem rodzaju aktywności i procederów wpisujących się na tę zacienioną stronę gospodarki oraz trudniejszej do zidentyfikowania, m.in. ze względu na specyficzne kodowanie stron internetowych, warunkujących anonimowość użytkowników oraz fałszowanie informacji o ich lokalizacji.

Podsumowanie

Dark Net stanowi część Internetu, zaś jego powstanie związane było z utrzymaniem prywatności i anonimowości. System wymiany plików w Dark Necie, jak również układ graficzny witryn zbliżony jest do tych, jakie funkcjonowały w otwartym Internecie w latach 90. XX w. Najwcześniejsze rynki związane z działalnością m.in. nielegalną pojawiły się na początku 2010 r. w formie zaszyfrowanej usługi pocztowej, zaś z biegiem czasu zostały przeniesione do tzw. sieci anonimowych. Największy udział w nielegalnej aktywności Dark Netu stanowi przestępczość narkotykowa.

Wyróżnia się cztery sektory Dark Netu: rynkowy, cyberprzestępczy (ang. *Cyber Warfare*), monitorowania i szpiegostwa (ang. *Spying Monitoring*) i komunikacji (ang. *Communication*). Sektor rynkowy koncentruje się wokół rynku narkotyków, procederu „prania pieniędzy", handlu ludźmi, złośliwego oprogramowania, usług związanych z zabójstwami, bronią, nielegalnymi instrukcjami, zakazaną pornografią i piractwem. Pozostałe sektory tworzą m.in.: usługi ransomware oraz dystrybucja w zakresie cyberprzestępczości, prześladowanie, monitorowanie prześladowców i terrorystów, a także komunikowanie się w zakresie omijania cenzury, stosowania sprzeciwów politycznych, sprawy związane z pozbawieniem praw czy współpracy [Deacon 2015, online].

Z punktu widzenia gospodarki, nielegalna zawartość Dark Netu stanowi zagrożenie, zarówno dla funkcjonowania i bezpieczeństwa różnych sektorów będących jej częścią, jak również innych obszarów życia społecznego, politycznego etc. Generuje ona straty w budżecie wszystkich państw, których użytkownicy korzystają z jej nielegalnych zasobów, ale także narusza porządek publiczny i ład gospodarczy na świecie, z cyberatakami, cyberterroryzmem i innymi formami przestępstw oraz nielegalnej aktywności włącznie.

Bibliografia

Armstrong M. (2016), UK a Hub for Illicit Drug Sales, „Statista" [online], https://www.statista.com/chart/5511/uk-a-hub-for-illicit-drug-sales/, dostęp: 07.12.2017 r.

Azab A.E., Mahmood M.A., El-Aziz A. (2017), Effectiveness of Web Usage Mining Technique in Business Aplication [w:] The Dark Web: Breakthroughs in Research and Practice, Management Association, Information Resources, IGI Global, Hershey.

Aschmann M., Leenen L., Viuureen J.J. (2017), The Utilisation of the Deep Web for Military Counter Terrorist Operations [w:] A.R. Bryant, J.R. Lopez, R.F. Mills (red.), Proceedings of the 12th International Conference on Cyber Warfare and Security: Hosted ByWright State University & the Center for Cyberspace Research, Air Force Institute of Technology, Publishing International Limited Reading, Dayton.

Bhardwaj A. (2017), Crypto Currency For Beginners, OnlineGatha, Indira Nagar.

Brito J., Castillo A. (2013), Bitcoin: A Primer for Policymakers, Mercatus Center at George Mason University, Mason.

Cusac C.M. (2015), Pornography and The Criminal Justice System, CRC Press, Boca Raton.

Darkmarkety – jak zacząć kupować, lub przynajmniej zaspokoić ciekawość [online], https://hyperreal.info/info/darkmarkety-jak-zaczac-kupowac-lub-przynajmniej-zaspokoic-ciekawosc, dostęp: 06.12.2017 r.

Dark Net Markets Revenue Analysis (2016), „Dark Net Markets" [online], https://darknet markets.co/dark-net-markets-revenue-analysis/, dostęp: 07.12.2017 r.

Deacon B.W. (2015), The Darknet (Deep Web) Explained [online], https://www.linkedin. com/pulse/darknet-deep-web-explained-bradley-w-deacon/, dostęp: 10.12. 017 r.

DeepLight – Shininhg a Light or a Dark Web (2016), Intelliagg, London-Stockholm.

Drugs and the Darknet Perspectives for Enforcement, Research and Policy (2017), European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) – Europol, Lisbon.

Europejski raport narkotykowy. Tendencje i osiągnięcia (2017), Urząd Publikacji Unii Europejskiej, Luksemburg.

Greenberg A. (2017), Monero, the Drug Dealer's Cryptocurrency of Choice, Is on Fire, „Wired" [online], https://www.wired.com/2017/01/monero-drug-dealers-cryptocurrency-choice-fire/, dostęp: 24.11.2017 r.

Hanson J. (2016), The Social Media Revolution: An Economic Encyclopedia of Friending, Following, Texting, and Connecting: An Economic Encyclopedia of Friending, Following, Texting, and Connecting, Greenwood, Santa Barbara.

Józefiak B. (2016), Ponad połowa treści w darknecie jest legalna, „Cyberdefence24" [online], http://www.cyberdefence24.pl/347102,ponad-polowa-tresci-w-darknecie-jest-leg alna, dostęp: 26.11.2017 r.

Kurek R. (2014), Alternatywne waluty wirtualne, „Annales Universitatis Mariae Curie-Skłodowska. Sectio H, Oeconomia", nr 3.

Last M., Markov A., Kandel A. (2008), Multi-lingual Detection of Web Terrorist Content, [w:] H. Chen, C.C. Yang (eds.), Intelligence and Security Informatics: Techniques and Applications, Springer, Heidelberg-Berlin.

Lech K. (2015), Dark Web, Deep Web – internet jest głębszy i mroczniejszy niż myślisz, „PCWorld" [online], https://www.pcworld.pl/news/Dark-Web-Deep-Web-internet-jest-glebszy-i-mroczniejszy-niz-myslisz,403732.html, dostęp: 23.11.2017 r.

Lotz B. (2017), Research Suggests the Dark Web Is Not As Aark As We Think [online], https://www.htxt.co.za/2016/11/02/research-suggests-the-dark-web-is-not-as-dark-as-we-think/, dostęp: 10.12.2017 r.

Martin J. (2014), Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs, Palgrave, New York.

Paganini P. (2014), The Rapid Growth of Darknet Black Markets [online], http://hplus magazine.com/2014/09/08/rapid-growth-darknet-black-markets/, dostęp: 26.11.2017 r.

Patterson D. (2016), The Light Side of the Dark Web [online], https://www.techrepublic. com/article/the-light-side-of-the-dark-web/, dostęp: 10.12.2017 r.

Puczyński M. (2016), Darknet: broń, pedofilia, cebula, narkotyki… i bezpieczeństwo zwykłych ludzi [online], https://puczynski.gadzetomania.pl/59077,darknet, dostęp: 23.11.2017 r.

Richmond T.J. (2017), Bitcoin: The Ultimate Bible – How To Make Money Online With Cryptocurrency Trading, Pronoun.

Rodwald P. (2013), Kryptograficzne funkcje skrótu, „Zeszyty Naukowe Akademii Marynarki Wojennej", nr 2 (193).

Sammons J. (2015), Digital Forensics: Threatscape and Best Practices, Syngress, Waltham.

Stępnicka N. (2017), Waluty alternatywne jako środki wymiany międzynarodowej oraz narzędzie ekonomii społecznej, „Przedsiębiorczość i Zarządzanie", Wybrane problemy zarządzania i finansów w sektorze prywatnym i publicznym, t. XVIII, z. 11, cz. 3.

Tharoor A. (2017), Report Shows Most Influential Countries in European Darknet Drug Trade, „Talking Drugs" [online], http://www.talkingdrugs.org/report-shows-the-most-influential-countries-in-european-darknet-drug-sales, dostęp: 07.12.2017 r.

Williams D. (2017), Cryptocurrency Compendium: A Reference for Digital Currencies: a Reference for Digital Currencies, Lulu.com, New York.

Winkler I., Gomes A.T. (2016), Advanced Persistent Security: A Cyberwarfare Approach to Implementing Adaptive Enterprise Protection, Detection, and Reaction Strategies, Syngress, Cambridge.

Bezpieczeństwo lokalne, narodowe i międzynarodowe – teoria i praktyka

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **141–152**

Piotr Daniluk[1]
Wydział Nauk o Bezpieczeństwie
Akademia Wojsk Lądowych

Podejście scenariuszowe w badaniu bezpieczeństwa

Scenario Approach to Research in Security Sciences

Abstract: The article concerns the assessment of the possibility of using a scenario approach in the threats analysis. The choice of the scenario approach results from the fact that it is part of the assumptions of basic security theory and its features that best suit the nature of contemporary threats. The analysis of the scenario planning achievements has led to the identification of dominant models. Their aggregation and final selection allowed to focus on two schools. The first one approaches the scenarios in a classical way, at the beginning making valuation of factors and indicating trends, which gives the normative character to the choices made. Pessimistic, optimistic and probable scenarios are created here. The second school puts down valuation, and thus the decision, until it is actually, and not only subjectively, necessary. In this case scenarios for specific narrations occur. The choice of approach should be determined by the purpose of use and the competences of the implementers (participants).
Key words: scenario approach, scenario planning, security.

Wprowadzenie

Specyficzną cechą nauki o bezpieczeństwie, poniekąd upodobniającą ją do nauki o zarządzaniu, jest prowadzenie szeregu badań mających na celu nie tylko diagnozę sytuacji, jak to ma miejsce w wielu innych dyscyplinach, ale przede wszystkim przewidywanie. Z tego też powodu u podstaw wyodrębniania teorii bezpieczeństwa powinny stać koncepcje antycypowania przyszłości: planistyczna, ewolucyjna, pozycyjna

[1] piotr.daniluk@awl.edu.pl

oraz zasobowa [Dawidczyk, Gryz, Koziej 2006, ss. 95–105, Gryz 2010, ss. 29–31]. Są one szczególnie przydatne do opisu zjawisk w obszarze bezpieczeństwa narodowego, sektorowego czy też wewnętrznego, a kłopotliwe w przypadku teorii bezpieczeństwa w stosunkach międzynarodowych (realizm, liberalizm, konstruktywizm i teorie krytyczne).

Autor artykułu proponuje zwrócić uwagę na podejście scenariuszowe, które wywodzi się ze szkoły planistycznej. Jest ono niezwykle przydatne we współczesnych badaniach w zakresie zarządzania [Heijden 2000, ss. 36–52] oraz potencjalnie – w dziedzinie bezpieczeństwa [Jemioło, Dawidczyk 2008, ss. 73–83], czego wykazanie będzie celem tego artykułu. Planowanie scenariuszowe stanowi prawdopodobnie jedyną tak skuteczną odpowiedź metodologii na, określoną przez klasyka teorii planistycznej H.I. Ansoffa, rosnącą turbulentność otoczenia [Ansoff 1985, s. 58].

Celem artykułu jest określenie możliwości wykorzystania podejścia scenariuszowego w badaniach w zakresie bezpieczeństwa. W związku z tym dokonano próby odpowiedzi na pytanie: Czy istnieje współcześnie możliwość zastosowania myślenia scenariuszowego również poza paradygmatem planistycznym i obszarem zarządzania, czyli we wszystkich czterech podstawowych podejściach do bezpieczeństwa? Założono, że nowoczesne planowanie scenariuszowe powinno spełnić wymagania badań w ujęciu podstawowych teorii bezpieczeństwa. W związku z tym przeprowadzono analizę stanu wiedzy w tym obszarze oraz zweryfikowano ją w wyniku empirycznych badań jakościowych w postaci analizy dokumentów, obserwacji i grupowych wywiadów zogniskowanych, przy czym dokonano triangulacji badań własnych. W artykule podjęto więc zupełnie nierozwijany w naszym kraju, a tylko wzmiankowany, wątek teorii bezpieczeństwa w ujęciu narodowym i w tak nakreślonym kontekście, po raz pierwszy, poddano naukowej analizie planowanie scenariuszowe.

Kluczowe koncepcje podejścia scenariuszowego

Pierwszy pojęcia „scenariusz", w stosunku do sposobów ujmowania przyszłości, użył H. Kahn, odróżniając prognozowanie od tworzenia obrazów przyszłości [Ringland 2006, ss. 13–14]. Podejście scenariuszowe pozwala planować w coraz bardziej niepewnych czasach (dlatego też jest nazywane „planowaniem scenariuszowym"). Jest to posiadana – lub kształtowana i rozwijana – umiejętność „pluralizmu" i holizmu myślenia otwierająca drogę do budowania wielorakich, możliwych koncepcji przyszłości na podstawie tworzonych wątków, fabuły i prowadzonej narracji. Podejście to nie stanowi prognozy, rozkładu normalnego ani desygnacji celów. Jest raczej sposo-

bem ujmowania dynamicznych sytuacji prowadzących do kreślenia różnorodnych obrazów przyszłości [Ralston, Wilson 2006, ss. 3–16].

Pojawienie się myślenia systemowego w latach drugiej wojny światowej oraz na początku lat 50. XX w. (badania operacyjne, teoria gier, planowanie ilościowe) zainicjowało powstanie podejścia scenariuszowego, jako odpowiedzi na niedostatki tego pierwszego oraz jego rozwinięcie [Ringland 2006, s. 15].

Narodzin koncepcji planowania scenariuszowego upatruje się w okresie po zakończeniu drugiej wojny światowej, kiedy to w Stanach Zjednoczonych, w ramach Rand Corporation, przeprowadzono zaawansowane badania nad wariantami przyszłego konfliktu globalnego pomiędzy USA a ZSRR. To wtedy H. Kahn zbudował scenariusze dotyczące w przyszłości wykorzystania nowoczesnych technologii, w tym broni jądrowej. W latach 60. XX w., w tej samej instytucji, dokonano analiz scenariuszowych konsekwencji wojny wietnamskiej. W 1967 r. H. Kahn i A.J. Wiener opublikowali *The Year 2000: A Framework for Speculation on the Next Thirty-Three Years,* pierwszą w historii tak odważną analizę o podłożu naukowym, sięgającą nowego wieku [Kahn, Wiener 1967].

Podejście scenariuszowe zastosowano w Stanford Research Institute (SRI) i firmie Shell oraz przy kreśleniu raportu *Granice wzrostu* przez Klub Rzymski [Ringland 2006, ss. 15–16]. Rozwój planowania scenariuszowego przebiegał więc od sfery bezpieczeństwa i obronności, poprzez sferę ekonomiczną (Shell, McKinsey, Global Business Network) po obszar projektów społecznych (konsekwencje społeczne wojny w Wietnamie), regionalnych i narodowych w Norwegii, Kanadzie, Finlandii, Gwatemali, Szkocji i RPA [Ringland 2006, ss. 117–118].

Najbardziej znane, i szczegółowo przeanalizowane w wielu światowych publikacjach, jest studium przypadku dotyczące planowania scenariuszowego firmy Royal Dutch Shell wprowadzone przez P. Wacka na przełomie lat 60. i 70. XX w. Zbudowano wtedy scenariusze opisujące przyszłą sytuację na rynkach naftowych, wśród których był ten ziszczający się w nieodległej przyszłości. Metoda ta okazała się przydatna również w 1979 i 1986 r. Nie spełniła swojego zadania wobec narastających presji społecznych w obliczu zachodzących zmian środowiskowych w 1994 i 1995 r., wobec których należało zastosować podejście ewolucyjne [Obłój 2007, ss. 220–224]. Zmiany te uwzględnia już macierz *stakeholders* [Godet 2006, ss. 262–270].

Szczegółowy opis modelu myślenia scenariuszowego przedstawia P. Schwartz [Schwartz 1991]. Widać w nim wyraźny wpływ w obszarze naukowym – H. Kahna i praktycznym – P. Wacka. W opracowaniu tym za cenne należy uznać nie tylko częste odwołanie się do przykładów z obszaru bezpieczeństwa, ale chyba po raz pierwszy – jeszcze przed szkołą kopenhaską – tak szczegółowe nakreślenie zasad i metodologii

oceny sił kluczowych dla makrośrodowiska, oparte na typologii STEPE (ang. *Society*, *Technology*, *Economics*, *Politics*, *Environment*) [Schwartz 1991, ss. 100–108, 122–134, 164–172, Buzan, Waever, Wild 1997, ss. 49–160].

Na uwagę zasługuje również koncepcja myślenia scenariuszowego oparta na uczeniu się ujmowania przyszłości za pomocą mapy powiązań oraz sprzężeń pomiędzy podmiotami i zjawiskami, co pozwoliło swobodnie przemieszczać się pomiędzy makro- i mikrośrodowiskiem [Fahey, Randall 1998, ss. 43–51, 141–156].

Ważną koncepcją planowania scenariuszowego jest model zaproponowany przez G. Ringlanda, w którym wyłączono metodę delficką z planowania scenariuszowego, a przypisano ją do prognozowania [Ringland 2006, ss. 33–35, 258–342].

Koncepcję reprezentującą dorobek Stanford Research Institute ujęto w postaci procesu złożonego z kilkunastu szczegółowo zdefiniowanych etapów. Widać w niej bardzo wyraźne wpływy „logiki intuicyjnej" i metod rozpowszechnianych przez Global Business Network (GBN). Model ten opiera się na kolejnym realizowaniu analiz sił makrootoczenia, mikrootoczenia i kluczowych *stakeholders* [Ralston, Wilson 2006, ss. 39–177].

Francuskie podejście do planowania scenariuszowego reprezentowane jest przez M. Godeta w oparciu o analizę: strukturalną (metoda Micmac), aktorów (metoda Mactor), morfologiczną i wywiadów eksperckich. Charakterystyczną cechą tej koncepcji jest wnikliwa analiza złożonej sieci powiązań *stakeholders*, co wskazuje na połączenie dorobku szkoły planistycznej i ewolucyjnej [Godet 2006, ss. 120–129, 263–270].

Współcześnie rozpowszechniona jest koncepcja dynamicznego reagowania na rosnącą niepewność otoczenia K. Heijdena, bazująca na dostosowywaniu myślenia scenariuszowego do zakresu złożoności otoczenia. Koncepcja ta opiera się na budowaniu jak największej liczby możliwych scenariuszy otoczenia, redukowanych do czterech, bez ich wartościowania w wymiarach rodzaju, siły i prawdopodobieństwa wpływu. Stanowi to kontekst testowania jakości konstruowanych strategii [Heijden 2000, s. 45, ss. 67–71].

W pewnym sensie operacjonalizacją koncepcji K. Heijdena jest model planowania scenariuszowego U. Pillkahna oparty na kompleksowym wykorzystaniu wielu metod heurystycznych, analizy strategicznej i foresightu pozwalających na przyjmowanie dowolnej perspektywy czasowej i badaniu różnych sfer otoczenia – od technologicznej po społeczną i polityczną. Autor w ten sposób wykazuje, że istotą podejścia scenariuszowego jest na tyle otwarta architektura, że zmienia się ona w bardzo małym stopniu w zależności od rodzaju reprezentowanego w badaniach podmiotu i środowiska [Pillkahn 2008].

Na uwagę zasługują polskie koncepcje planowania scenariuszowego. Jedną z pierwszych była opracowana przez zespół badawczy A. Klasika, dlatego też oprzyrządowano ją metodami ilościowymi [Klasik 1993, ss. 99–114].

Współczesną i ciekawą koncepcją podejścia scenariuszowego jest zaproponowany przez P. Cabałę model bazujący na podejściu ilościowym, w którym zawarto elementy teorii gier [Cabała 2012, ss. 18–72, 121–168].

W kierunku wspólnego lub nowego modelu podejścia scenariuszowego. Wskazania do badań empirycznych

Przeprowadzoną analizę dorobku w zakresie planowania scenariuszowego można streścić w postaci zbioru następujących wniosków:

1. Choć minęło ponad 60 lat od pierwszego naukowego zastosowania planowania scenariuszowego przez H. Kahna i od tego czasu opracowano wiele koncepcji takiego postępowania badawczego, to najczęściej uwaga jest skupiana wokół dwóch modeli – Royal Dutch Shell oraz Stanford Research Institute [Ralston, Wilson 2006, ss. 8–26].
2. Analiza tych modeli pozwala stwierdzić, że różnią się one uwagą zwracaną na określone środowiska, co potwierdza tezę mówiącą o tym, iż myślenie scenariuszowe jest na tyle elastyczne, że współcześnie może mieć zastosowanie we wszystkich podejściach do otoczenia, czasu i wielkości podmiotu [Heijden 2000]. To z kolei wskazuje na możliwość zastosowania go we wszystkich czterech paradygmatach strategicznych.
3. W myśleniu scenariuszowym najczęściej uwaga zwracana jest na makrootoczenie, co wpisuje je tym samym w założenia teorii planistycznej [Ansoff 1985, Schwartz 1991, Klasik 1993]. W takim przypadku analiza prowadzona jest nawet dla horyzontu kilkudziesięcioletniego i dotyczy wielkich podmiotów [Kahn 1967, 1976]. Nowsze badania wykazują, że scenariusze mogą być bardziej elastyczne, pozwalając na przemieszczanie się między makrootoczeniem i mikrootoczeniem, co wpisuje się w założenia teorii ewolucyjnej, a nawet ujmować problematykę sektorową [Heijden 2000, Godet 2006, Ralston, Wilson 2006, Ringland 2006, Obłój 2007, Cabała 2012].
4. Powyższe konstatacje uprawniają do twierdzenia, że podejście scenariuszowe łączy dorobek tak rozbieżnych w swoich założeniach szkół, jak: planistyczna z ewolucyjną oraz pozycyjna z zasobową, na co nie pozwalała żadna inna metodologia. Dla planowania scenariuszowego teorie wyznaczają jedynie zakres, w którym po-

winny zawierać się budowane koncepcje scenariuszy, modele strategii będące ich pochodną oraz przyjęte metody badawcze [Heijden 2000].

5. Wykazano, że mimo pochodzenia podejścia scenariuszowego ze szkoły planistycznej, dzięki wzbogacaniu metodologicznemu oraz zastosowaniu w coraz to innych obszarach wiedzy i praktyki, zakres wykorzystania tej koncepcji może obejmować wszystkie podstawowe teorie bezpieczeństwa.

W następnym etapie procedury badawczej powyższe wnioski zostały poddane empirycznej ocenie i weryfikacji, szczególnie w odniesieniu do bezpieczeństwa i obronności.

Badania dokumentów normatywnych

W wyborze dokumentów normatywnych w obszarze bezpieczeństwa kierowano się zasadą nie tylko wykorzystania scenariuszy w przedstawianych koncepcjach, ale też w stosowanej metodologii, co zawęziło analizę do strategii sektorowych. Decyzja o sklasyfikowaniu strategii do konkretnej teorii bezpieczeństwa opierała się na złożonym kryterium określonym szczegółowo w literaturze przedmiotu [Obłój 2007, ss. 60–148, Urbanowska-Sojkin 2011, ss. 90–114], w którym należało uwzględnić specyfikę nauk o bezpieczeństwie.

Za interesujący dokument spełniający powyższe kryteria uznano *Strategiczny Przegląd Obronny* [MON 2011]. Podstawą jego tworzenia były kanony szkoły planistycznej – analiza TWOS/SWOT, analiza STEPE oraz scenariusze procesów w otoczeniu. Przyjęty odległy horyzont czasowy (lata 2030–2035), rozpatrywany rodzaj strategii (strategia poziomu rozwoju) i jej wpływ na strukturę (postulat spłaszczenia struktury dowództw), istotna rola przypisana zarządzaniu strategicznemu Siłami Zbrojnymi oraz znaczny stopień operacjonalizacji – to również cechy charakterystyczne dla szkoły planistycznej. Analiza strategiczna oparta na scenariuszach ma charakter wartościujący, co powoduje, że wnioski ze scenariuszy przenosi się na konkretne modele strategii. Zestandaryzowany proces analizy strategicznej generuje szablonowe dwie strategie zasadnicze, które różnią się tylko złożonością uwzględnianego otoczenia [MON 2011, ss. 25–30, 57–82, 107–139].

Natomiast *Strategiczny Przegląd Obronny 2016* wpisuje się najlepiej w założenia szkoły pozycyjnej. Świadczy o tym koncentracja uwagi na otoczeniu konkurencyjnym, a szczególnie jego kluczowym podmiocie, jakim jest Rosja oraz rodzaj formułowanej strategii (strategia poziomu konkurencji, jako odpowiedź na działania głównego aktora). Obrona własnego terytorium, zwiększenie liczebności i jakości sił zbrojnych, postawienie na racjonalność rozumianą jako „systematyczna i chłodna analiza" – są to

również przesłanki teorii pozycyjnej. Mimo deklarowanej w dokumencie długoterminowości, jedynie analiza makrootoczenia jest realizowana do 2032 r. z wykorzystaniem metod jakościowych, takich jak: obserwacja, scenariusze i badania delfickie. Treść samej strategii ma znacznie krótszą perspektywę (2020 r.), którą determinują przeprowadzone kalkulacje ekonomiczno-finansowe. Zastosowane metody weryfikujące scenariusze – gry strategiczne i symulacje oraz analizy koszt-efekt – mają charakter ilościowy, który nie pozwala na planowanie w dłuższym niż 2 lata horyzoncie czasowym. Zbudowane scenariusze – pesymistyczne i optymistyczne – opierają się na wartościowaniu, co skutkuje standardowymi opcjami strategicznymi [MON 2016].

Analizie poddano również dokumenty transsektorowe, w obszarze informacyjnym i cyberprzestrzeni, a mianowicie: *Doktrynę cyberbezpieczeństwa RP* [BBN 2015b] oraz projekt *Doktryny bezpieczeństwa informacyjnego RP* [BBN 2015a]. Oba dokumenty, z powodu zastosowania w nich podejścia „od zewnątrz do wewnątrz", można przypisać do szkoły zasobowej w teorii bezpieczeństwa, biorąc pod uwagę przede wszystkim ich strukturę i kolejność analizy (najpierw cele i analiza wymiaru krajowego, a na końcu ograniczona analiza wymiaru zewnętrznego) oraz fakt, że największą uwagą poświęcono w nich samemu systemowi (koncepcje zadań – operacyjnych i przygotowawczych). Istotną cechą zastosowanego tu podejścia jest podkreślenie potrzeby współpracy grupy podmiotów, których kompetencje uzupełniają się (podmioty państwowe, prawne, operatorzy, obywatele). W centrum uwagi są więc elementy tworzące kompetencje (miękkie, techniczne i organizacyjne) państwa w obszarze informacyjnym. Uwzględnienie interesów tych grup w treści strategii wynikowej oraz znaczny charakter deskryptywny dokumentów może wskazywać na istnienie w nich pewnych pierwiastków podejścia ewolucyjnego. W prezentowanym ujęciu zasobowym zastosowano podejście systemowe, formułując rozliczne zadania dla podsystemów, a mianowicie: kierowania, operacyjnego oraz wsparcia publicznego i prywatnego. Podejście scenariuszowe dotyczy sposobu budowania strategii. Przy tworzeniu analizowanych dokumentów wykorzystano metodologię opisaną poniżej.

Badania fokusowe

Autor artykułu uczestniczył w realizacji badań sondażowych, ankietowych i fokusowych związanych z opracowaniem *Doktryny cyberbezpieczeństwa* [BBN 2015b] oraz *Doktryny bezpieczeństwa informacyjnego* [BBN 2015a]. W ramach tych prac odbyło się kilkanaście spotkań ekspertów z różnych środowisk. Sprawozdanie niniejsze dotyczy jednej sesji (4.03.2015 r.) – zogniskowanego wywiadu grupowego opartego na celowo dobranej grupie przedstawicieli środowiska akademickiego (zespół 10 ekspertów

oraz 4 organizatorów badań), który spełniał wymóg różnorodności reprezentowanych instytucji naukowo-badawczych i interesów oraz jednorodności obszaru zainteresowania (eksperci do spraw bezpieczeństwa w wymiarze informacyjnym) [BBN 2015c]. Podczas sesji poruszono cztery zagadnienia dotyczące otoczenia konkurencyjnego oraz kilkanaście związanych z oceną potencjału informacyjnego. W formułowanych wypowiedziach dominowało konstruowanie wizji zjawisk w otoczeniu, którym od razu przypisywano odpowiednie reakcje aktorów instytucjonalnych i społecznych. Interakcje w grupie nie powodowały zmiany podejścia do analiz bezpieczeństwa, lecz powielanie lub wzmacnianie już określonych scenariuszy otoczenia. Wyjątkowe skupienie uwagi na własnym potencjale, gdzie uwarunkowania zewnętrzne były ograniczane tylko do jednego aktora, wskazywały na dominujące podejście zasobowe. Dopełnieniem tych badań były rozesłane kwestionariusze-ankiety do wypełnienia przez ekspertów po spotkaniach fokusowych. Nie były to badania delfickie, gdyż nie ponawiano cyklu sondażowego. Układ treści ankiet wymagał wczesnego oceniania charakteru analizowanych zjawisk (podejście wartościujące) oraz skupienia uwagi na potencjale społecznym i technologicznym naszego kraju, co ponownie wpisywało się w kanony szkoły zasobowej oraz pozycyjnej.

Badania dokumentów wytworzonych i obserwacja

Badania empiryczne związane z podejściem scenariuszowym oparto również na obserwacji powstawania oraz ocenie dokumentów, związanych z realizacją analiz strategicznych bezpieczeństwa, przez kilkuosobowe zespoły[2]. Celem tych badań było nie tylko określenie możliwości zastosowania scenariuszy w ramach różnych teorii bezpieczeństwa, ale również wskazanie metodologii najlepiej spełniającej te wymagania. Zespoły podzielono na dwie grupy realizujące odmienne rodzaje planowania scenariuszowego, które opisane są w literaturze przedmiotu jako klasyczne oraz redukujące ocenę [Heijden 2000, ss. 141–247, Daniluk 2015, ss. 79–220].

Klasyczny rodzaj planowania scenariuszowego, oparty na wczesnym wartościowaniu (rodzaju, siły i prawdopodobieństwa wpływu trendów), był wspomagany przez takie metody podejmowania decyzji, jak: grupy nominalne oraz badania delfickie, w których budowano platformę konsensusu opinii i oceny, pozwalającą jednocześnie dokonywać pewnych uogólnień obejmujących szerszy obszar problemowy.

[2] Projekt *Analiza zagrożeń dla Dolnego Śląska* był realizowany w ramach grantu MNiSW na Wydziale Nauk Społecznych i Dziennikarstwa Dolnośląskiej Szkoły Wyższej we Wrocławiu w latach 2012–2015. Uczestniczyło w nim m.in. 96 zespołów złożonych z 3 studentów studiów drugiego stopnia na kierunku: bezpieczeństwo narodowe (dobór wstępny celowy, podział na grupy oraz przydział rodzaju metody scenariuszowej losowy).

W analizie makrootoczenia (analizy: STEPE, scenariuszowa, synergiczna, krzyżowa wpływów i ETOP) duża niepewność determinowała postępowanie wpisujące się w założenia teorii planistycznej w wyniku: rozpatrywania odległego horyzontu czasowego i otoczenia, dążenia do racjonalnej oceny zjawisk stochastycznych, dominującej roli kierowników zespołów określających kluczowe kryteria, ekstrapolacji jakościowej, dążenia do strukturyzacji i dyscyplinowania procesu analizy, podporządkowania argumentacji wyceny trendów skutkom, a nie przyczynom.

W analizie mikrootoczenia (*stakeholders*) duża złożoność procesów i podmiotów skłaniała do podejścia ewolucyjnego w wyniku: skracania horyzontu czasowego, uwzględniania kultury strategicznej oraz koalicji politycznych, odchodzenia od racjonalności przy jednoczesnym intensywnym poszukiwaniu aktualnych informacji, koncentracji uwagi na nielicznych obszarach, dążenia do nieprecyzyjności, jednakowego uwzględniania najważniejszych sił i ich wektorów oddziaływania, operowania raczej opisem niż oceną. Przy zawężeniu obszaru uwagi do sektora zaczęły dominować cechy myślenia pozycjonującego objawiające się: koncentracją na podmiotach najbliższych oraz najbardziej wyrazistych, porównywaniem potencjału i wielkości podmiotów, poszukiwaniem możliwości wyliczenia określonych relacji, grupowaniem podmiotów i dążeniem do graficznego zobrazowania dynamiki sytuacji.

W analizie potencjału oraz w procesie budowania wariantów strategii dominowało podejście zasobowe (systemowe, procesowe lub funkcjonalne), pomijające znaczenie otoczenia w kształtowaniu kompetencji badanych podmiotów.

W fazie wyboru strategii dominowała analiza TOWS/SWOT zgodnie z modelami opisanymi w literaturze przedmiotu [Obłój 2007, ss. 337–358, MON 2011, ss. 101–148, Daniluk 2015, ss. 206–224]. Wykazany tu schematyzm działania, oparty na przypisywaniu ocenionych scenariuszy i potencjałów do ograniczonego zbioru strategii, wpisuje się w założenia szkoły planistycznej.

Zespoły, które zastosowały podejście scenariuszowe, oparte na redukowaniu wartościowania, w wyniku wykorzystania badań typu *Policy Delphi*, uwypuklały rozbieżności opinii i oceny. Tworzono scenariusze za pomocą wygenerowania zdarzeń, a nie trendów (co eliminowało ocenianie) oraz ich pogrupowania w strukturze jednego z trzech lub czterech scenariuszy. W sytuacji wyczerpania się zbioru generowanych zdarzeń, nadawano nazwy-hasła scenariuszom, do których budowano fabułę. Przyjęty rodzaj myślenia wymuszał na uczestnikach w fazie tworzenia scenariuszy bardziej dynamiczne ujmowanie otoczenia, stroniące od szybkiej kategoryzacji i wykazujące cechy podejścia jakościowego, podobnego do procesu badawczego w teorii ugruntowanej. Opisowy charakter tak budowanych scenariuszy wskazuje na wyraźne cechy podejścia ewolucyjnego, wystrzegającego się oceniania, a poprzestającego na okre-

śleniu jak największej liczby czynników [Cieślik 1997, s. 192]. Procesowi temu towarzyszyło intensywne zdobywanie informacji, ich aktualizowanie oraz ciągłe korygowanie wyłaniających się koncepcji otoczenia, aż do momentu wyczerpania się pomysłów na ich elementy składowe. W przedstawianej metodologii wymagające było nie tylko redukowanie wartościowania w trakcie budowania scenariusza, ale dopasowanie do tak napisanych narracji optymalnego rozwiązania. W fazie budowania strategii wykorzystywano głównie podejście zasobowe oparte na określeniu kompetencji podmiotu. Następnie koncepcje te były testowane na zbudowanych modelach otoczenia. Weryfikacja opierała się o założenia szkoły pozycyjnej, w której w centrum uwagi znajduje się badanie relacji pomiędzy aktorem otoczenia a wybranymi elementami organizacji.

Metodologia ta umożliwiała naturalne wykorzystanie metod ilościowych i jakościowych, w którym zbudowane jakościowo (teoria ewolucyjna) scenariusze służą do testowania modeli o charakterze ilościowym. Scenariusze te mogą mieć charakter ilościowy (teoria planistyczna lub pozycyjna) i być weryfikowane przez modele opisowe (teoria ewolucyjna lub zasobowa).

Podsumowanie

Na podstawie dokonanej analizy literatury przedmiotu wykazano szerokie możliwości zastosowania podejścia scenariuszowego w ramach podstawowych paradygmatów strategicznych. Weryfikacja empiryczna nie tylko potwierdziła takie możliwości, ale pozwoliła je odnieść do badań w zakresie bezpieczeństwa i obronności oraz ukierunkowała uwagę na dwie różniące się, ale możliwe do przeprowadzenia, metodologie planowania scenariuszowego spełniającego założenia uwzględnianych teorii.

Podejście wartościujące (klasyczne) wywodzi się ze szkoły planistycznej, przez co, jako prostsze i bazujące na schematach, doczekało się wielu opracowań. Należy jednak pamiętać, że narzuca ono łączenie określonych rozwiązań ze zbudowanymi i ocenionymi już scenariuszami otoczenia. Automatyzm i bezwzględne poddanie myślenia procedurom na etapie wyboru strategii jest wadą tego podejścia z punktu widzenia kreatywności i elastyczności, ale może być jednak także zaletą, pozwalając kształcić umiejętność funkcjonowania w warunkach ograniczeń normatywnych i nacisków politycznych, które nie są tak uwypuklane w podejściu niewartościującym. Ponieważ jest sformalizowane, podejście to stosowane jest wobec sytuacji kryzysowych i w dydaktyce, pozwala bowiem porządkować działania i systematyzować informacje. Proces realizacji tej metodologii przebiega od makrootoczenia (szkoła planistyczna), poprzez mikrootoczenie (szkoła ewolucyjna) i sektor (szkoła pozycyjna) po podmiot

(szkoła zasobowa) [Daniluk 2015]. Badania scenariuszowe mogą więc być prowadzone jako samodzielne dla każdego z tak określonych środowisk lub jako komplementarny proces.

Weryfikacji poddano również podejście redukujące wartościowanie scenariuszy, które testuje strategie na tak zbudowanych modelach otoczenia. Pozwala ono wyjść poza ramy teorii planistycznej i w sposób adaptacyjny ujmować otoczenie oraz budować elastyczne strategie (dopasowywać charakter badań do charakteru zjawisk) [Heijden 2000, s. 45]. Ten model planowania scenariuszowego jest wymagający, ale najbardziej przydatny w prowadzeniu badań związanych ze zróżnicowanymi zagrożeniami i podmiotami. Proces realizacji metodologii przebiega od budowania scenariuszy (indukcyjnie – szkoła ewolucyjna, dedukcyjnie – szkoła planistyczna) poprzez budowanie strategii (podejście zasobowe) po testowanie strategii (podejście pozycyjne). Metodologia scenariuszowa oparta na redukowaniu wczesnego wartościowania jest ukierunkowana na antycypowanie przyszłości, co wskazuje na jej wielki potencjał.

Szczególnie to właśnie podejście będzie przedmiotem dalszych badań realizowanych przez autora artykułu, gdyż, jako najbardziej uniwersalne, można je rozwijać i doskonalić. Niezaprzeczalnym atutem tej koncepcji jest możliwość zastosowania metod eksperymentu naukowego do testowania strategii w środowisku zbudowanych modeli otoczenia. Pozwoli to w sposób ilościowy zweryfikować koncepcje określone wcześniej w wyniku stosowania metod jakościowych.

Konsekwencją przedstawionych wyników badań są prace związane ze zbudowaniem założeń do gry decyzyjnej *KRYZYS 2018* w Akademii Wojsk Lądowych, w której planuje się przeprowadzenie serii eksperymentów naukowych.

Bibliografia

Ansoff H.I. (1985), *Zarządzanie strategiczne*, Państwowe Wydawnictwo Ekonomiczne, Warszawa.

BBN [Biuro Bezpieczeństwa Narodowego] (2015a), *Doktryna bezpieczeństwa informacyjnego RP. (Projekt)*, Warszawa.

BBN [Biuro Bezpieczeństwa Narodowego] (2015b), *Doktryna cyberbezpieczeństwa RP*, Warszawa.

BBN [Biuro Bezpieczeństwa Narodowego] (2015c), *Forum Bezpieczeństwa*, [online] https://www.bbn.gov.pl/pl/wydarzenia/6488,Pierwsze-spotkanie-Strategicznego-Forum-Bezpieczenstwa-nt-wojen-informacyjnych.html?search=927106612, dostęp: 10.02.2018.

Buzan B., Waever O., Wild J. (1998), *Security. A New Framework for Analysis*, Lynne Rienner Publishers, London.

Cabała P. (2012), *Planowanie scenariuszowe w zarządzaniu bezpieczeństwem strategicznym przedsiębiorstwa*, Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie, Kraków.

Cieślik M. (red.) (1997), *Prognozowanie gospodarcze. Metody i zastosowania*, Wydawnictwo Naukowe PWN, Warszawa.

Daniluk P. (2015), *Bezpieczeństwo i zarządzanie. Analiza strategiczna*, Difin, Warszawa.

Dawidczyk A., Gryz J., Koziej S. (2006), *Zarządzanie strategiczne bezpieczeństwem. Teoria – praktyka – dydaktyka*, Wyższa Szkoła Humanistyczno-Ekonomiczna, Łódź.

Fahey L., Randall M. (red.) (1998), *Learning from the Future. Competitive Foresight Scenarios*, John Wiley & Sons, New York.

Godet M. (2006), *Creating Futures. Scenario Planning as a Strategic Management Tool*, Economica, Paris.

Gryz J. (2010), *Zarys podstaw teorii bezpieczeństwa*, Akademia Obrony Narodowej, Warszawa.

Heijden K. (2000), *Planowanie scenariuszowe w zarządzaniu strategicznym*, Oficyna Ekonomiczna, Kraków.

Jemioło T., Dawidczyk A. (2008), *Wprowadzenie do metodologii badań bezpieczeństwa*, Akademia Obrony Narodowej, Warszawa.

Klasik A. (red.) (1993), *Planowanie strategiczne*, Państwowe Wydawnictwo Ekonomiczne, Warszawa.

Kahn H. (1976), *The Next Two Hundred Years: A Scenario for America and the World*, William Morrow & Company, New York.

Kahn H. (1967), *The Year 2000: A Framework for Speculation on the Next Thirty-Three Years*, Macmillan Publishing Company, New York.

MON [Ministerstwo Obrony Narodowej] (2017), *Koncepcja obronna RP*, Warszawa.

MON [Ministerstwo Obrony Narodowej] (2011), *Strategiczny Przegląd Obronny RP. Profesjonalne Siły Zbrojne RP w nowoczesnym państwie. Raport*, Warszawa.

Obłój K. (2007), *Strategia organizacji. W poszukiwaniu trwałej przewagi konkurencyjnej*, Państwowe Wydawnictwo Ekonomiczne, Warszawa.

Pillkahn U. (2008), *Using Trends and Scenarios as Tools for Strategy Development*, Publicis Corporate Publishing, Erlangen.

Ralston B., Wilson I. (2006), *The Scenario-Planning Handbook. A Practitioner's Guide to Developing and Using Scenarios to Direct Strategy in Today's Uncertain Times*, Thomson South-Western, Mason.

Ringland G. (2006), *Scenario Planning. Managing for the Future*, John Wiley & Sons, Chichester.

Schwartz P. (1996), *The Art of the Long View*, Currency Doubleday, New York.

Urbanowska-Sojkin E. (red.) (2011), *Podstawy wyborów strategicznych w przedsiębiorstwach*, Państwowe Wydawnictwo Ekonomiczne, Warszawa.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **153–166**

Julia Anna Gawęcka[1]
Uniwersytet Jana Kochanowskiego w Kielcach
Filia w Piotrkowie Trybunalskim

Obrona cywilna w polskim dyskursie politycznym i publicznym a kwestie bezpieczeństwa społeczności lokalnych

Civil Defence in Polish Political and Public Discourse and Local Community Security Issues

Abstract: The paper refers to the author's research on civil defence in Poland. The author has made an attempt to analyze the approach to civil defence and its impact on the security of the local communities, referring to specific polemics characteristic of Polish political and public discourse.
Key words: Civil defence, local community security, state security, National Civil Defence of Poland, The State Fire Service.

Wprowadzenie

Pojęcie obrony cywilnej, choć popularne w okresie tzw. zimnej wojny, w XXI w. pozostaje terminem nieznanym i niedoprecyzowanym. Niemniej jednak daje się zauważyć, zwłaszcza w państwach Europy Zachodniej i Północnej (np. w Konfederacji Szwajcarskiej, Republice Federalnej Niemiec oraz w Królestwie Szwecji), pojawiającą się już od

[1] juliagrochocka@onet.eu

kilku lat tendencję do traktowania obrony cywilnej[2] (OC) jako istotnego elementu warunkującego bezpieczeństwo państwa. Konsekwencją zainteresowania zagadnieniami obrony cywilnej jest widoczny wzrost znaczenia świadomości społecznej, co do postępowania w sytuacjach nadzwyczajnych, bez konieczności uciekania się wyłącznie do rozwiązań instytucjonalnych, zagwarantowanych przez władze państwowe.

Niestety, pomimo pojawienia się charakterystycznych trendów proobronnych, poziom zainteresowania i świadomości społeczeństwa polskiego w zakresie funkcjonowania obrony cywilnej w dalszym ciągu nie spełnia pożądanych oczekiwań. Niewiedza Polaków, a tym samym niechęć wobec jakichkolwiek inicjatyw na rzecz obrony cywilnej, wynika w głównej mierze z wadliwego i nieefektywnego systemu prawno-organizacyjnego, a także jest konsekwencją jawnej bierności elit politycznych, dla których kwestie ochrony ludności i obrony cywilnej nie stanowią atrakcyjnego przedmiotu debat.

Autorka, wykorzystując badania własne (ilościowe – ankieta anonimowa oraz jakościowe – wywiad kwestionariuszowy), podjęła się w artykule analizy obrony cywilnej i jej wpływu na bezpieczeństwo społeczności lokalnych, odwołując się do konkretnych polemik charakterystycznych dla polskiego dyskursu politycznego i publicznego. Na potrzeby artykułu za dyskurs[3] uznano rozmowę, myślowe ujmowanie otaczającej rzeczywistości społecznej i politycznej, a także schemat poznawczy wykorzystywany do kreowania powszechnie podzielanych wyobrażeń [Howarth 2015, s. 14].

Obrona cywilna – rozważania definicyjne

Współczesna OC funkcjonuje w oparciu o przepisy zarówno prawa międzynarodowego, jak i regulacje wewnętrzne poszczególnych państw. Istotnym aktem prawnym o charakterze międzynarodowym, którego przepisy definiują termin „obrona cywilna", jest Protokół dodatkowy do Konwencji Genewskich z 12 sierpnia 1949 roku dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych, sporządzony w Genewie 8 czerwca 1977 roku [Dz. U. z 1992 r. Nr 41, poz. 175].

Zgodnie z treścią art. 61a Protokołu OC została utożsamiona z działalnością polegającą na wypełnianiu wszystkich bądź tylko niektórych zadań humanitarnych na

[2] Autorka świadomie używa w artykule pojęcia obrony cywilnej, zapisywanego małymi lub dużymi literami. Definiując zagadnienie w kategoriach instytucjonalnych, powołując się na całą strukturę, organizację i system OC, autorka używa dużych liter, w pozostałych przypadkach – małych.

[3] Ponadto, podążając za rozważaniami Marka Czyżewskiego, Sergiusza Kowalskiego oraz Andrzeja Piotrowskiego [Czyżewski, Kowalski, Piotrowski 2010], pod pojęciem dyskursu publicznego autorka rozumie „wszelkie przekazy dostępne publicznie". Natomiast dyskurs polityczny utożsamia z wypowiedziami polityków na tematy związane z otaczającą rzeczywistością, mającą bezpośredni wpływ na egzystencję i bezpieczeństwo społeczeństwa.

rzecz ochrony ludności cywilnej przed wszelkimi zagrożeniami, zarówno czasu pokoju, jak i wojny. Przepisy ujęte w Protokole za OC uznały także przezwyciężanie bezpośrednich następstw zagrożeń czasu wojny i pokoju wraz z zapewnieniem warunków koniecznych do przetrwania. Na szczególną uwagę zasługują wspomniane zadania humanitarne OC, do których zaliczono: 1) służbę ostrzegawczą; 2) ewakuację; 3) przygotowywanie i organizowanie zbiorowych środków ochrony ludności; 4) obsługę środków zaciemnienia; 5) ratownictwo; 6) służby medyczne, pierwszą pomoc, a także opiekę religijną; 7) walkę z pożarami; 8) wykrywanie i oznaczanie stref uznanych za niebezpieczne oraz odkażanie i inne działania ochronne; 9) dostarczanie pomieszczeń doraźnych i zaopatrzenia; 10) udzielanie pomocy doraźnej dla przywrócenia i utrzymania porządku w strefach dotkniętych klęskami oraz doraźne przywrócenie funkcjonowania służb użyteczności publicznej; 11) pomoc w grzebaniu zmarłych; 12) ratowanie dóbr gwarantujących przetrwanie; 13) dodatkową aktywność warunkującą wypełnienie innego zadania, w tym planowanie i prace organizacyjne.

Wyszczególnione zadania OC w czasie klęsk żywiołowych i ewentualnych konfliktów zbrojnych w zasadzie wyczerpują katalog powinności tejże struktury ujęty w prawie międzynarodowym.

Nieco odmienne rozumienie istoty OC prezentują regulacje prawne obowiązujące w Polsce. W zasadzie jedynym aktem prawnym, w oparciu o który funkcjonuje w Polsce OC, jest ustawa z dnia 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. Należy podkreślić, że na mocy art. 137 tejże ustawy [Dz. U. 1991 Nr 114, poz. 491] za obronę cywilną uznano ochronę ludności, zakładów pracy i urządzeń użyteczności publicznej oraz dóbr kultury, jak również ratowanie i udzielanie pomocy poszkodowanym w czasie wojny, a także współdziałanie w zwalczaniu klęsk żywiołowych, zagrożeń środowiska i usuwanie ich skutków.

Z poczynionych przez autorkę rozważań bezsprzecznie wynika, iż to właśnie prawo międzynarodowe w sposób precyzyjny wymienia zadania OC czasu wojny i pokoju. W przypadku regulacji polskich ustawa o powszechnym obowiązku obrony RP nie reguluje w pełni kwestii związanych z OC, co więcej, wprowadza jedynie zbędny chaos.

Niemniej jednak zaproponowany 22 grudnia 2016 roku przez Komendę Główną Państwowej Straży Pożarnej projekt ustawy o ochronie ludności i OC jest próbą zniwelowania nieścisłości definicyjnych, wprowadzenia obligatoryjnych rozróżnień i rozwiązania problemów prawno-organizacyjnych. W projekcie ustawy pojawiły się bowiem dwa istotne terminy – „ochrona ludności" i „obrona cywilna". W rozumieniu przepisów projektu ochrona ludności ma polegać na „zintegrowanej działalności organów administracji publicznej właściwych w sprawach ochrony ludności, jak również innych podmiotów realizujących zadania mające na celu ochronę życia i zdrowia

ludności przebywającej na terytorium RP, ochronę mienia, dziedzictwa kulturowego oraz środowiska naturalnego, w sytuacji wystąpienia zagrożeń naturalnych lub spowodowanych przez człowieka" [Projekt 2016]. Tak rozumiana ochrona ludności miałaby funkcjonować w sytuacjach kryzysowych i stanach nadzwyczajnych czasu pokoju i przekształcać się w obronę cywilną w trakcie stanu wojennego lub konfliktu zbrojnego. Biorąc pod uwagę brak konkretnego modelu funkcjonowania OC w Polsce, a także niskie nakłady przeznaczane z budżetu państwa na finansowanie zadań OC (22 139 tys. zł w 2016 roku), takie rozwiązanie problemu wydaje się być słuszne i uzasadnione. Przy aktualnym (nadal fatalnym) stanie OC [Grochocka 2017, ss. 139–164], potwierdzonym również w analizie raportu Najwyższej Izby Kontroli z 2012 roku [Raport NIK 2012], nie jest możliwe tworzenie OC od podstaw, nie posiłkując się efektywnie działającymi podmiotami z zakresu ochrony ludności, nie stanowiącymi jednocześnie formalnej części struktur OC. Zatem pomysł wykorzystania dostępnego potencjału jest na chwilę obecną jedynym sensownym rozwiązaniem.

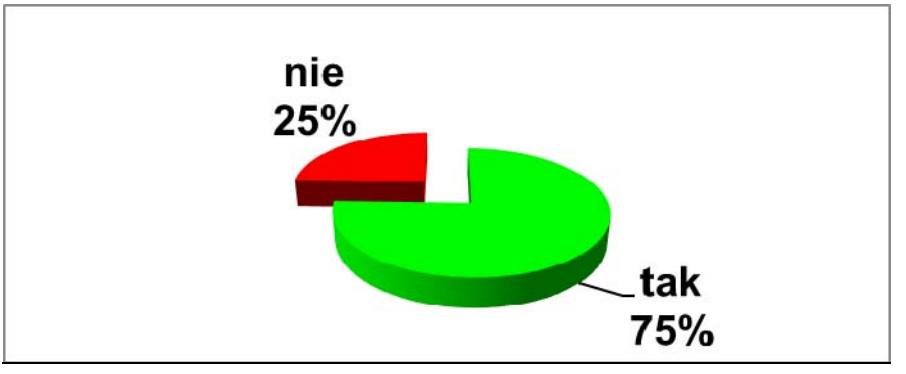
Obrona cywilna w dyskursie publicznym. Świadomość obywateli a poziom bezpieczeństwa społeczności lokalnych

Podejmując polemikę na temat OC w Polsce w kontekście zapewnienia bezpieczeństwa społeczności lokalnych, należy przede wszystkim zastanowić się nad kwestią definiowania OC przez obywateli oraz nad problematyką świadomości społecznej, a także miejscem OC w dyskursie publicznym. Otóż, jak wynika z badań autorki, wiedza obywateli na temat OC potwierdza indolencję polskiego systemu OC. Bez wątpienia niski poziom wiedzy obywateli na tematy związane bezpośrednio z ochroną ludności i OC jest konsekwencją bagatelizowania przez państwo walorów edukacji dla bezpieczeństwa. Obywatele niezainteresowani problematyką bezpieczeństwa nie wykazują również aktywności w tej dziedzinie, polegając jedynie na gwarancjach państwowych.

Chcąc udowodnić mierną wiedzę obywateli na temat OC, autorka powołała się na badania własne przeprowadzone w okresie od 11 sierpnia do 30 września 2016 roku na grupie 151 respondentów w wieku od 18 do 65 roku życia. Respondenci wzięli udział w anonimowej ankiecie, dzięki której stała się możliwa ocena OC w polskim dyskursie publicznym.

Zasadnicze pytanie ankiety dotyczyło znajomości pojęcia obrony cywilnej (zob. rysunek 1).

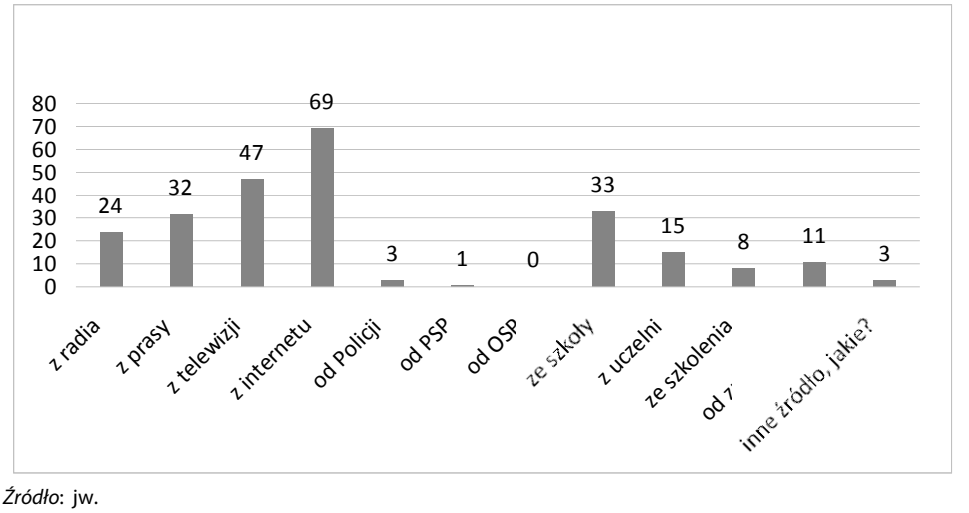
Rysunek 1. Czy Pan/Pani wie, co oznacza pojęcie obrony cywilnej?



Źródło: opracowanie własne na podstawie badań zrealizowanych dzięki narzędziom dostępnym na stronie internetowej eBadania.pl, http://www.ebadania.pl/reports/31084/Ankieta_z_zakresu_poziomu_wiedzy_o_Obronie_Cywilnej.xls.

Znajomością terminu wykazało się 114 (75%) ze 151 respondentów, natomiast dla 37 osób pojęcie było całkowicie nieznane i niezrozumiałe. W przypadku wyboru odpowiedzi negatywnej ankietowany był automatycznie odsyłany do pytań, które nie były w sposób bezpośredni związane z funkcjonowaniem OC, niemniej jednak dotyczyły zadań wykonywanych przez organy i formacje OC w Polsce. Spośród 114 osób, które pozytywnie odpowiedziały na pytanie o znajomość terminu OC, najwięcej badanych (69) zadeklarowało, że wiedzę o OC pozyskuje głównie z Internetu (zob. rysunek 2).

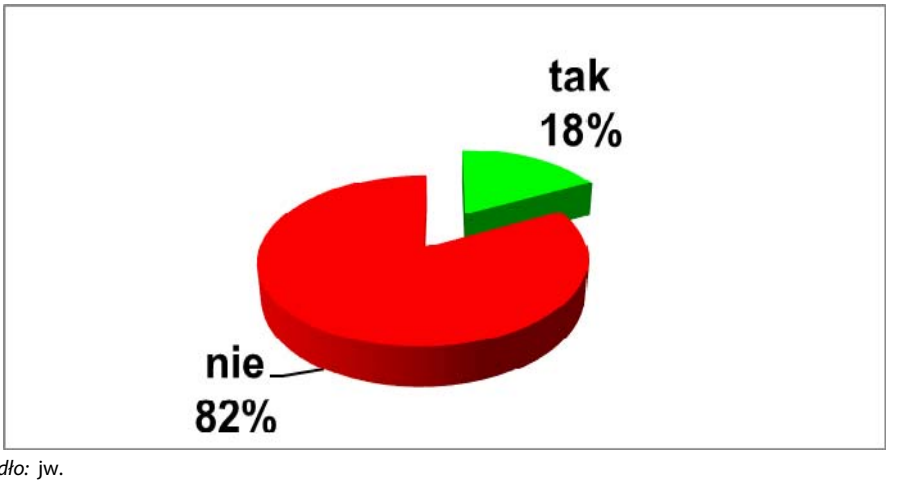
Rysunek 2. Skąd Pan/Pani dowiedział/a się o obronie cywilnej?



Źródło: jw.

Ponadto respondenci za źródła informacji na temat OC uznali radio, prasę oraz telewizję (łącznie 103 osoby), szkołę (33), znajomych (11), Policję (3) lub własną wiedzę logiczną (3). Badania wykazały również, że szkolenie nie stanowi wartościowego źródła informacji o OC, gdyż jedynie 8 osób uznało tę formę za jeden ze sposobów uzupełniania teorii i praktyki. Co więcej, okazało się, że służby odpowiedzialne za realizację zadań OC w Polsce także nie przyczyniają się do zwiększania świadomości wśród obywateli (tylko 1 osoba korzystała z wiedzy od Państwowej Straży Pożarnej – PSP, natomiast nikt nie wspomniał o Ochotniczych Strażach Pożarnych – OSP, których członkowie zostali powołani do służby w formacjach OC). Brak rzetelnej wiedzy obywateli potwierdziło także pytanie o znajomość osób związanych bezpośrednio z OC (zob. rysunek 3).

Rysunek 3. Czy w Pana/Pani otoczeniu znajdują się osoby związane z obroną cywilną?

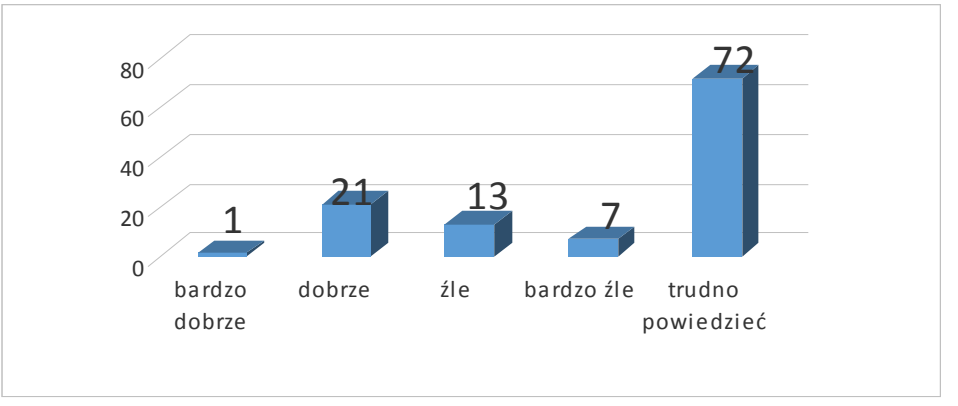


Źródło: jw.

Spośród 114 badanych aż 94 (82%) nie znało żadnej osoby ze swojego bliskiego otoczenia, która partycypowałaby w zadaniach OC. Jedynie 20 osób (18%) na zadane pytanie odpowiedziało twierdząco, przytaczając głównie obowiązki dotyczące ochrony ludności przed zagrożeniami i przezwyciężanie następstw zagrożeń, zwłaszcza w przypadku pożarów i klęsk żywiołowych.

Ostatnie pytanie, skierowane do grupy 114 osób, które potwierdziły znajomość pojęcia obrony cywilnej, dotyczyło wyrażenia opinii o funkcjonowaniu tej struktury w Polsce (zob. rysunek 4).

Rysunek 4. Jak ocenia Pan/Pani funkcjonowanie OC w Polsce?

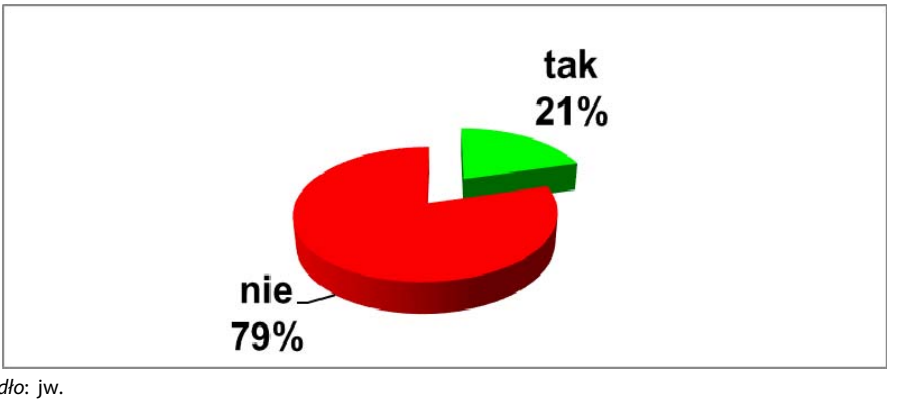


Źródło: jw.

Tylko jeden respondent ocenił pozytywnie funkcjonowanie OC, 21 uznało, że OC w Polsce działa dobrze, 20 ankietowanych skrytykowało funkcjonowanie OC, natomiast aż 72 ze 114 nie miało zdania na ten temat.

Odpowiedzi na następne pytania udzielali już wszyscy ankietowani. Autorka chciała w ten sposób uzyskać wiedzę na temat świadomości obywateli w przypadku pojawienia się konkretnych zagrożeń. Pytanie o znajomość zasad postępowania w przypadku wystąpienia skażenia także udowodniło brak jakiegokolwiek przygotowania społeczeństwa polskiego do sytuacji nadzwyczajnych (zob. rysunek 5).

Rysunek 5. Czy zna Pan/Pani zasady postępowania w przypadku skażenia środkami masowego rażenia, toksycznymi środkami przemysłowymi lub substancjami promieniotwórczymi?

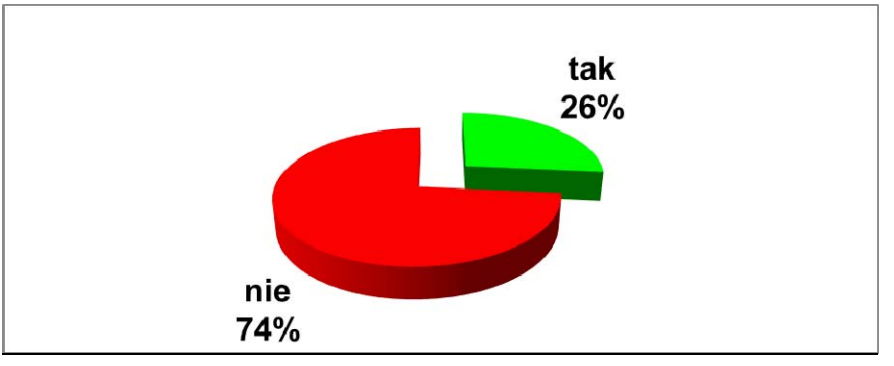


Źródło: jw.

Spośród 151 ankietowanych jedynie 31 osób (21%) potwierdziło znajomość tych za-sad, natomiast aż 120 badanych (79%) nie potrafiło opisać, jak należy zachować się w przypadku konkretnego rodzaju skażenia.

Podobny poziom niewiedzy wśród obywateli udowodniło pytanie o znajomość miejsca ewakuacji w przypadku zagrożenia (zob. rysunek 6).

Rysunek 6. Czy zna Pan/Pani miejsce ewakuacji, gdzie należy się udać w przypadku zagrożenia?



Źródło: jw.

W trakcie badania aż 111 osób ze 151 (74%) nie potrafiło zlokalizować miejsca ewakuacji w swoim sąsiedztwie. Natomiast 40 badanych (26%), którzy pozytywnie odpowiedzieli na to pytanie, jako miejsce ewakuacji wskazało w sposób ogólnikowy: schron, urząd gminy, piwnicę, szkołę, nie podając konkretnego adresu.

Wyniki badania udowodniły, jak nikłą rolę w dyskursie publicznym odgrywa problematyka OC. Zatem, zasadna staje się konstatacja, iż jedynie systematyczne szkolenia ludności cywilnej są w stanie zagwarantować poczucie bezpieczeństwa i zwiększyć świadomość obywateli w tej kwestii.

Kolejną grupą, stanowiącą podmiot dyskursu publicznego, byli eksperci zajmujący się OC. Autorka, korzystając z kwestionariusza wywiadu, poprosiła o udział w badaniu:

1) gen. bryg. Leszka Suskiego – Komendanta Głównego PSP – Szefa Obrony Cywilnej Kraju;
2) gen. bryg. w st. spocz. Wiesława Bogdana Leśniakiewicza – Komendanta Głównego PSP i Szefa OCK (2008–2015);
3) st. bryg. w st. spocz. Dariusza Marczyńskiego – Dyrektora Krajowego Centrum Koordynacji Ratownictwa i Ochrony Ludności (2009–2016),
4) nadbryg. w st. spocz. dr. Ryszarda Grosseta – prof. wizytującego Szkoły Głównej Służby Pożarniczej; Dyrektora Krajowego Centrum Koordynacji Ratownictwa Ko-

mendy Głównej PSP (1998–2000); Zastępcę Komendanta Głównego PSP i Zastępcę Szefa OCK (2000–2005); byłego Rektora Szkoły Głównej Służby Pożarniczej;

5) st. bryg. Mariusza Koniecznego – Zastępcę Komendanta Wojewódzkiego PSP w Łodzi (2007–2016);
6) Franciszka Krynojewskiego – właściciela Agencji Konsultingowej „Mikado", autora publikacji z zakresu ochrony ludności i OC.

Wszyscy eksperci biorący udział w wywiadzie jednogłośnie stwierdzili, że OC nie funkcjonuje w sposób należyty i wymaga zmian systemowych (prawno-organizacyjnych). L. Suski jako przyczynę fatalnej kondycji OC wskazał brak ujednoliconych regulacji prawnych jasno „określających kompetencje władz, obowiązki obywateli oraz sposoby zwiększania świadomości społeczeństwa w zakresie ochrony ludności" [Archiwum autorki]. Komendant uznał za obligatoryjne precyzyjne sformułowanie zadań ochrony ludności, uwzględniając jednocześnie obowiązujące akty prawne.

Równie krytyczną opinię o OC wyraził W.B. Leśniakiewicz, który wskazał na deficyt wzajemnych relacji dotyczących zagadnień ochrony ludności czasu wojny i pokoju oraz ograniczony zakres zadań na rzecz pomocy humanitarnej, co potęguje chaos kompetencyjny oraz dublowanie się zadań. Leśniakiewicz dostrzegł również brak ustalonej odgórnie odpowiedzialności za stan faktyczny OC, a także fikcyjne i niedoinwestowane formacje OC, od których wymaga się stałej gotowości na czas kryzysu, pokoju i wojny. Według eksperta obligatoryjny proces usprawnienia systemu OC powinien uwzględniać proces poszerzenia kręgu podmiotów należących do systemu.

Natomiast D. Marczyński wskazał na brak zainteresowania władz państwowych OC, który wynika z braku odpowiedzialności za bezpieczeństwo obywateli, zbyt permisywnego podejścia do identyfikacji współczesnych zagrożeń, a w konsekwencji nieadekwatnej do aktualnych wyzwań wizji funkcjonowania całego systemu. Według D. Marczyńskiego, aby dokonać koniecznych zmian w obszarze OC, należy określić jej zadania na czas kryzysu, pokoju i wojny, a także skonsolidować działania wszystkich organów władzy, służb ratowniczych, instytucji publicznych oraz organizacji pozarządowych, które w codziennej pracy realizują zadania ochrony ludności i w przypadku wystąpienia sytuacji kryzysowych mogłyby podjąć współpracę.

Zdaniem R. Grosseta OC w Polsce jest w stanie „permanentnej reorganizacji od 2000 roku", kiedy to podejmowano nieudolne próby wypracowania pożądanej ustawy. Grosset wspomniał o potrzebie wykreowania jednolitego Krajowego Systemu Ratownictwa i Ochrony Ludności, który jako konglomerat wszystkich służb, inspekcji, straży oraz organizacji pozarządowych w przypadku zagrożeń militarnych przekształcałby się w system OC. Grosset zaproponował również opracowanie siatki (matrycy)

bezpieczeństwa i procedur reagowania jej elementów na zagrożenia, co umożliwiłoby wnikliwą analizę potencjału oraz stopnia przygotowania tych służb, zwłaszcza podczas ćwiczeń zgrywających (rzeczywistych i aplikacyjnych) [Archiwum autorki].

Według M. Koniecznego OC w Polsce to „martwa formacja, która nie ma żadnej faktycznej możliwości realnego działania, […] jest to tylko wirtualny twór nie mający mocy sprawczych w sferze organizacyjno-logistycznej" [Archiwum autorki]. Jako przykłady działań doskonalących, M. Konieczny zaproponował podpisanie porozumień z podmiotami gospodarczymi dysponującymi sprzętem przydatnym w fazie reagowania i odbudowy, ale dostępnym na podstawie monitoringu i odpowiedniej gotowości operacyjnej.

F. Krynojewski wskazał na brak korelacji pomiędzy przepisami prawa polskiego a regulacjami I Protokołu dodatkowego z 8 czerwca 1977 roku do Konwencji Genewskich z 1949 roku. Krynojewski dostrzegł także wadliwy system organizacyjny OC, oparty w głównej mierze na PSP oraz OSP, zatem na formacjach, które realizują się już w KSR-G. F. Krynojewski, jako jedyny z ekspertów nie mający związku z PSP, wskazał na konieczność oddzielenia OC od PSP i OSP i zastąpienia ich strukturami znajdującymi się bezpośrednio w ministerstwie spraw wewnętrznych i administracji.

Podsumowując, w zasadzie wszyscy specjaliści uznali zgodnie, że aby usprawnić polski system OC, należy w pierwszej kolejności dokonać istotnych rozważań definicyjnych, tak aby funkcjonująca w czasie pokoju ochrona ludności przekształcała się na wypadek zagrożeń czasu wojny w obronę cywilną, realizując wówczas zadania humanitarne i zapewniając podstawowe warunki dla przetrwania ludności cywilnej. Ponadto, w opinii ekspertów, dalszy rozwój systemu wymaga od państwa i instytucji odpowiedzialnych za zapewnienie bezpieczeństwa wypracowania konkretnego modelu funkcjonowania OC w Polsce, z uwzględnieniem aktualnych potrzeb i możliwości.

Obrona cywilna w dyskursie politycznym

Nieco inaczej prezentuje się aspekt obecności zagadnień OC w dyskursie politycznym. Należy mieć na uwadze, że brak aktywności polityków w przedmiocie OC nie wynika z ich niewiedzy, lecz przede wszystkim jest skutkiem postrzegania OC w kategoriach zbędnego i generującego dodatkowe koszty aspektu bezpieczeństwa. Niewątpliwie marginalizacja znaczenia OC utrudnia zrozumienie jej istoty, uniemożliwiając tym samym przeprowadzenie wskazanej modernizacji systemu, dostosowanego do nowych wyzwań i zagrożeń.

Jak wynika z badań autorki, najbardziej aktywną grupę polityków, jeśli chodzi o zainteresowanie omawianą problematyką, stanowili posłowie Prawa i Sprawiedli-

wości (Grzegorz Puda, Dariusz Piontkowski), Platformy Obywatelskiej (Anna Nemś), Kukiz'15 (Anna Maria Siarkowska) oraz Polskiego Stronnictwa Ludowego (Zbigniew Sosnowski). W artykule przywołano jedynie wybrane poglądy, które w opinii autorki wydają się najbardziej interesujące.

Poseł D. Piontkowski w interpelacji z 28 czerwca 2012 roku, skierowanej do ówczesnego ministra spraw wewnętrznych, poruszył kwestię wyników raportu Najwyższej Izby Kontroli. Analiza NIK obejmowała okres od 28 czerwca do 16 listopada 2011 roku i dotyczyła przygotowania struktur OC do realizacji zadań w okresie wojny i pokoju [Informacja NIK 2012, ss. 6–11]. Poseł, powołując się na krytyczną opinię o stanie OC, domagał się od ministra wyjaśnienia braku podjęcia działań na rzecz poprawy sytuacji w systemie OC. Ponadto zaproponował wyegzekwowanie od Szefa OCK niezbędnych informacji o przyczynach stwierdzonych przez NIK nieprawidłowości. Pozostałe pytania dotyczyły ewentualnych działań, jakie zostały podjęte przez państwo w ostatnich latach na rzecz unowocześnienia OC, upowszechnienia wiedzy o obronności i poprawy infrastruktury obronnej [Interpelacja 6304]. Odpowiedzią na interpelację posła było sformułowanie przez podsekretarza stanu Romana Dmowskiego ogólnikowych mechanizmów naprawczych, które miały być rzekomo implementowane przez resort [Odpowiedź na interpelację nr 6304].

Warto nadmienić, że poseł D. Piontkowski, zaniepokojony wydarzeniami na Ukrainie, w lipcu 2014 roku wystosował kolejną interpelację, tym razem do ministra obrony narodowej, domagając się informacji na temat ewentualnej reformy OC, ze wskazaniem jej głównych kierunków i założeń. W interpelacji pojawił się postulat wzmocnienia roli OSP oraz weryfikacji kompetencji i wiedzy szefów OC gmin [Interpelacja 27667]. W odpowiedzi na interpelację podsekretarz stanu w Ministerstwie Obrony Narodowej Maciej Jankowski, poza przywołaniem wyników badań społecznych, poinformował, iż nie jest właściwą osobą w przedmiocie interpelacji i skierował pismo do ministra spraw wewnętrznych [Odpowiedź na interpelację nr 27667].

Natomiast poseł G. Puda apelował o dostosowanie modelu OC do bieżących potrzeb wynikających z członkostwa Polski w Unii Europejskiej. Puda podkreślił, iż działania OC mają charakter społeczny, zatem nie mogą ich zastąpić rodzaje Sił Zbrojnych, nawet Wojska Obrony Terytorialnej. G. Puda zaznaczył również, że to właśnie przygotowanie społeczności lokalnych zadecyduje, w jakim stopniu uda się zminimalizować skutki potencjalnej katastrofy [Interpelacja nr 6417].

Posłanka PO, A. Nemś, podobnie jak D. Piontkowski, powołując się na wyniki raportu NIK z 2012 roku, domagała się wytłumaczenia stwierdzonych przez NIK błędów w OC oraz przedstawienia konkretnych rozwiązań zaistniałych problemów, w tym

podjęcia obligatoryjnych prac legislacyjnych inicjujących konieczne zmiany w systemie [Interpelacja 11391].

Również posłanka Kukiz'15, A.M. Siarkowska, odniosła się do raportu NIK z 2012 rok, pytając Szefa OCK, co zmieniło się od tamtego czasu w OC i jakie działania zostały podjęte na rzecz poprawy sytuacji [Zapis przebiegu posiedzenia Komisji Administracji i Spraw Wewnętrznych z dnia 13 kwietnia 2016 roku].

Natomiast poseł PSL, Z. Sosnowski, stwierdził, że prace nad ustawą o ochronie ludności i OC trwają zbyt długo; chciał dowiedzieć się, czy założenia i treści nowej ustawy wykorzystują dorobek poprzedników, czy przesłanki projektu są zbieżne z wcześniejszymi postulatami [Zapis przebiegu posiedzenia Komisji Administracji i Spraw Wewnętrznych z dnia 13 kwietnia 2016 roku].

Jak dowiodła analiza polskiej myśli politycznej, problematyka OC w dyskursie politycznym nie zajmuje istotnego miejsca. Jedynie wybrani politycy dostrzegają konieczność debatowania o szeroko pojętej ochronie ludności i OC. Zatem, można pokusić się o stwierdzenie, że zawarte w programach wyborczych obietnice troski o bezpieczeństwo społeczności lokalnych i bezpieczeństwo państwa stają się jedynie frazesami.

Uwagi końcowe

Podsumowując rozważania na temat OC w polskim dyskursie politycznym i publicznym, autorka sformułowała trzy istotne spostrzeżenia.

Po pierwsze, wydaje się, że OC w Polsce pomimo zaniedbania ze strony państwa w XXI wieku będzie stanowić ważny element pozamilitarnego systemu bezpieczeństwa, warunkujący właściwe funkcjonowanie ludności cywilnej, zarówno w trakcie zagrożeń czasu pokoju, jak i wojny. Postępująca redefinicja pojęcia bezpieczeństwa oraz pojawienie się jego nowych zagrożeń wymuszają niejako na instytucjach państwowych zainteresowanie kwestiami OC i w konsekwencji rozwiązanie wszystkich problemów uniemożliwiających właściwe jej funkcjonowanie. Państwo, chcąc realizować swój konstytucyjny obowiązek zagwarantowania bezpieczeństwa (przede wszystkim bezpieczeństwa społeczności lokalnych), nie może skupiać się wyłącznie na trosce o stan liczebny i wyposażenie armii. Podążając za przykładem państw Europy Zachodniej, kluczowe staje się również uświadamianie i szkolenie społeczeństwa.

Po drugie, niewiedza obywateli na tematy związane z ochroną ludności i OC, a w konsekwencji niechęć do wspólnych działań na rzecz bezpieczeństwa dowodzą indolencji władz w zakresie przygotowania społeczeństwa do radzenia sobie w sytuacjach kryzysowych. Jak wskazują doświadczenia ze współczesnych konfliktów zbrojnych, bazowanie wyłącznie na rozwiązaniach instytucjonalnych, oferowanych przez

państwo w XXI w. staje się niewystarczające. Dlatego też ważne w tym aspekcie jest zainteresowanie ze strony obywateli oraz chęć uczestnictwa we wszelkich organizowanych przez państwo inicjatywach na rzecz poprawy bezpieczeństwa i zwiększania świadomości w zakresie postępowania w sytuacjach nadzwyczajnych.

Po trzecie, ochrona ludności i OC winna stać się ważnym przedmiotem debat politycznych, gdyż to elity rządzące mają zasadniczy wpływ na kształtowanie regulacji prawnych i kreowanie właściwych ram organizacyjnych systemu bezpieczeństwa państwa. Świadomi w kwestiach ochrony ludności i OC politycy swoją działalnością na arenie politycznej są w stanie zwiększyć poziom świadomości społeczeństwa, wykształcając w obywatelach poczucie odpowiedzialności za bezpieczeństwo, począwszy od wspólnoty lokalnej, a skończywszy na wspólnocie narodowej.

Bibliografia

Archiwum autorki (2016), *Wywiad kwestionariuszowy*.

Czyżewski M., Kowalski S., Piotrowski A. (red.) (2010), *Rytualny chaos: studium dyskursu publicznego*, Wydawnictwa Akademickie i Profesjonalne, Warszawa.

Grochocka J.A. (2017), *Obrona cywilna w Polsce. Stan obecny i możliwe perspektywy rozwoju,* [w:] O. Wasiuta, P. Mazur (red.), *Współczesne problemy bezpieczeństwa państwa. Księga pamiątkowa ku czci Tomasza Jana Biedronia*, Katedra Pedagogiki Katolickiej, Stalowa Wola.

Howarth D. (2005), *Dyskurs*, przeł. A. Gąsior-Niemiec, Oficyna Naukowa, Warszawa.

Interpelacja nr 11391 do ministra spraw wewnętrznych w sprawie wyników kontroli NIK w zakresie „Przygotowania struktur obrony cywilnej do realizacji zadań w okresie wojny i pokoju" z dnia 7 listopada 2012 roku, [online] www.orka.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=47F9E660, dostęp: 12 września 2017.

Interpelacja nr 27667 do ministra obrony narodowej w sprawie reformy obrony cywilnej z dnia 22 lipca 2014 roku, [online] www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=6BB4FD27, dostęp: 12 września 2017.

Interpelacja nr 6304 do ministra spraw wewnętrznych w sprawie wyników kontroli Najwyższej Izby Kontroli dotyczącej przygotowania struktur obrony cywilnej do realizacji zadań w okresie wojny i pokoju z dnia 28 czerwca 2012 roku, [online] www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=1EF46FE6&view=null, dostęp: 12 września 2017.

Interpelacja nr 6417 do ministra obrony narodowej, ministra spraw wewnętrznych i administracji w sprawie koniecznych zmian w systemie funkcjonowania Obrony Cywilnej Kraju z dnia 23 września 2016, [online] www.sejm.gov.pl/sejm8.nsf/InterpelacjaTresc.xsp?key=265AEC7E, dostęp: 12 września 2017.

NIK (2016), *Informacja o wynikach kontroli Przygotowanie struktur obrony cywilnej do realizacji zadań w okresie wojny i pokoju*, [online] www.nik.gov.pl/plik/id,3953,vp,5028.pdf, dostęp: 12 września 2017.

Odpowiedź podsekretarza stanu w Ministerstwie Obrony Narodowej – z upoważnienia ministra – na interpelację nr 27667 w sprawie reformy obrony cywilnej z dnia 18 sierpnia 2014 roku, [online] www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=77AC9A96, dostęp: 12 września 2017.

Odpowiedź podsekretarza stanu w Ministerstwie Spraw Wewnętrznych – z upoważnienia ministra – na interpelację nr 6304 w sprawie wyników kontroli Najwyższej Izby Kontroli dotyczącej przygotowania struktur obrony cywilnej do realizacji zadań w okresie wojny i pokoju z dnia 30 lipca 2012 roku, [online] www.sejm.gov.pl/sejm7.nsf/InterpelacjaTresc.xsp?key=0708D797&view=null, dostęp: 12 września 2017.

Projekt ustawy o ochronie ludności i obronie cywilnej z dnia 22 grudnia 2016 roku, [online] www.ock.gov.pl/prawo/projekty_aktow_prawnych, dostęp: 15 stycznia 2017.

Protokół dodatkowy do Konwencji Genewskich z 12 sierpnia 1949 roku dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych, sporządzony w Genewie 8 czerwca 1977 roku [Dz. U. z 1992 r. Nr 41, poz. 175].

Ustawa z dnia 21 listopada 1967 roku o powszechnym obowiązku obrony Rzeczypospolitej Polskiej [Dz. U. z 1991 r. Nr 114, poz. 491].

Zapis przebiegu posiedzenia Komisji Administracji i Spraw Wewnętrznych z dnia 13 kwietnia 2016 roku, nr 31, [online] http://www.sejm.gov.pl/Sejm8.nsf/biuletyn.xsp?documentId=27E4F02D73844F8BC1257F990041BE30, dostęp: 12 września 2017.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **167–179**

Roman Stawicki[1]
Społeczna Akademia Nauk

Kształtowanie bezpieczeństwa lokalnego na przykładzie Komendy Powiatowej Policji w Legionowie

Shaping Local Security by the Example of Police District Headquarters in Legionowo

Abstract: The first part of the article presents the essence and nature of basic tasks performed by the police field units. In next part, local security was diagnosed on the basis of data collected by Police Headquarters in Legionowo. Another important problem was the analysis of preventive programs implemented in Legionowo district. The final part deals with the summary of local security shaping on the example of the Police District Headquarters in Legionowo, as well as the projection of changes, i.e. proposed actions for improvement of this process.
Key words: security, threats, crimes, offense, locality, police, cooperation.

Wstęp

Współcześnie zapewnienie bezpieczeństwa społecznościom lokalnym staje się jednym z priorytetów państwa oraz struktur jego władzy i administracji publicznej, w tym Policji. Najbardziej rozpoznawalnym projektem w zakresie kształtowania bezpieczeństwa w przestrzeni lokalnej jest rządowy program ograniczenia przestępczości i aspołecznych zachowań „Razem bezpieczniej"[2]. Jego nadrzędnym celem jest ograniczenie zjawisk i sposobów postępowania, które budzą wśród obywateli powszechny sprze-

[1] rstawicki@spoleczna.pl
[2] Pierwszy ogólnokrajowy program profilaktyczny, opracowany z inicjatywy Władysława Stasiaka – podsekretarza stanu w Ministerstwie Spraw Wewnętrznych i Administracji, został uchwalony przez Radę Ministrów w dniu 18 grudnia 2006 roku.

ciw oraz poczucie zagrożenia. Program „Razem bezpieczniej", realizowany przy właściwej diagnozie zagrożeń i oczekiwań społecznych, obejmuje wiele obszarów życia społecznego [Serafin, Parszowski 2011, s. 240]. Projekt ten niewątpliwie spowodował pewien przełom w postrzeganiu bezpieczeństwa jako dobra wspólnego, jak również przekonał wiele podmiotów o konieczności podejmowania, na zdecydowanie większą skalę niż dotychczas, działań o charakterze zapobiegawczym.

Policja jako podmiot, który w największym stopniu wpływa na stan porządku i bezpieczeństwa publicznego ma swój znaczący udział w realizacji programu „Razem bezpieczniej". Podejmuje ona ponadto wiele innych działań mających wpływ na poczucie bezpieczeństwa obywateli. W tym miejscu zasadnym jest przywołanie chociażby nowej *Koncepcji działań Policji w zakresie profilaktyki społecznej na lata 2016–2018* [Komenda Główna Policji 2015]. W ramach prac nad wspomnianym dokumentem dokonano analizy dysfunkcyjności dotychczasowych rozwiązań i wyznaczono cele dla całej policyjnej formacji na najbliższe trzy lata. Koncepcja ta stała się także fundamentem do podjęcia działań zmierzających do udoskonalenia pracy Policji w obszarze szeroko rozumianej profilaktyki społecznej. Innym dobrym przykładem może być wdrożona w drugiej połowie 2016 roku Krajowa Mapa Zagrożeń Bezpieczeństwa, która stanowi element procesu zarządzania bezpieczeństwem i porządkiem publicznym realizowanym w partnerstwie międzyinstytucjonalnym oraz społecznym. W ramach organizacji Policji za realizację zadań na poziomie lokalnym odpowiadają między innymi komendy powiatowe.

Celem przeprowadzonych badań było zdiagnozowanie zakresu współuczestnictwa Komendy Powiatowej Policji w Legionowie w kształtowaniu bezpieczeństwa lokalnego. Realizacji tak sformułowanemu celowi służyły następujące problemy badawcze:

1. Jakie zadania realizują jednostki terenowe Policji, co stanowi istotę ich działania na rzecz projekcji bezpieczeństwa lokalnego?
2. W jaki sposób Komenda Powiatowa Policji w Legionowie przeprowadza diagnozę zagrożeń dla bezpieczeństwa społeczności lokalnej?
3. Czy realizowane przez Komendę Powiatową Policji w Legionowie projekty profilaktyczne są adekwatne do zidentyfikowanych zagrożeń oraz oczekiwań wspólnoty lokalnej?

Podstawową metodą wykorzystywaną w przygotowaniu artykułu była analiza ilościowo-jakościowa dokumentacji oraz literatury naukowej. Przedmiotem badań objęto funkcjonowanie Komendy Powiatowej Policji w Legionowie w 2016 roku, w trzech zasadniczych aspektach dla bezpieczeństwa społeczności lokalnej tj.: wykonywanych zadań, diagnozowania zagrożeń, jak również realizowania projektów profilaktycznych.

Istota i charakter podstawowych zadań realizowanych przez jednostki terenowe Policji

Polska Policja została utworzona na mocy uchwalonej 6 kwietnia 1990 r. ustawy o Policji [Dz. U. z 2015 r., poz. 355, z późn. zm.], która była jedną z pierwszych ustaw w nowych warunkach ustrojowych Rzeczypospolitej Polskiej. Policja jest formacją uzbrojoną służącą do ochrony bezpieczeństwa i porządku publicznego. Jej jednostki organizacyjne wykonują, oprócz zadań określonych w Konstytucji RP, obowiązki wynikające z ustawy o Policji oraz zadania na podstawie innych ustaw szczególnych, przepisów wykonawczych, wewnętrznych aktów kierowania oraz umów i porozumień międzynarodowych [Cylkowski 2015, s. 134]. Do podstawowych zadań Policji należy m.in.:

1) „ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobra;
2) ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania;
3) inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi; […]
4) wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców;
5) nadzór nad strażami gminnymi (miejskimi) oraz nad specjalistycznymi uzbrojonymi formacjami ochronnymi w zakresie określonym w odrębnych przepisach" [Dz. U. z 2015 r. poz. 355, z późn. zm., art. 1 ust. 2].

Warto zwrócić uwagę, że zadania wymienione w pkt 1–3 mieszczą się wprost w zakresie profilaktyki predeliktualnej, czyli przedprzestępczej. Natomiast pozostałe zadania, w tym wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców są zadaniami profilaktyki postdeliktualnej, czyli poprzestępczej. Zatem misją Policji jest zapobieganie popełnianiu przestępstw i wykroczeń w celu zapewnienia odpowiedniego poziomu bezpieczeństwa i porządku publicznego.

Również w regulacjach prawnych niższego rzędu ta filozofia działania znajduje swoje odzwierciedlenie. Potwierdzają to chociażby przepisy zawarte w Zarządzeniu nr 1041 Komendanta Głównego Policji z dnia 28 września 2007 r. w sprawie szczegółowych zasad organizacji i zakresu działania komend, komisariatów i innych jednostek organizacyjnych Policji [Dz. Urz. KGP z 2013 r., poz. 50 z późn. zm.]. Zgodnie z tym

aktem prawnym do zakresu działania komend powiatowych policji należy w szczególności:

1) tworzenie i realizacja, we współdziałaniu z organami samorządu terytorialnego oraz organizacjami i instytucjami pozarządowymi, programów prewencyjnych ukierunkowanych na:
   a) ujawnianie, zapobieganie i zwalczanie zjawisk patologii społecznej, zwłaszcza wśród dzieci i młodzieży;
   b) zapewnienie mieszkańcom możliwości sygnalizowania lub zgłaszania Policji o zdarzeniach i sytuacjach zagrażających bezpieczeństwu ludzi i mienia albo porządkowi publicznemu, a także stworzenie warunków umożliwiających natychmiastową reakcję Policji na takie sygnały lub zgłoszenia;
   c) organizowanie, koordynowanie i wykonywanie czynności patrolowych, interwencyjnych oraz ochronnych;
   d) edukacja mieszkańców w zakresie uwarunkowań dotyczących utrzymywania porządku i bezpieczeństwa publicznego oraz aktywnego udziału w przedsięwzięciach profilaktycznych podejmowanych na obszarze powiatu;
2) wykonywanie czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych w celu ujawniania przestępstw i sprawnego wykrywania ich sprawców, współdziałając z innymi jednostkami Policji.

W tym wewnętrznym akcie kierowania Komendanta Głównego Policji katalog zadań również rozpoczyna się od powinności opracowywania i realizacji programów prewencyjnych w szeroko rozumianym partnerstwie społecznym. Ponadto wskazano w nim priorytety podejmowanych działań zapobiegawczych w ramach tzw. prewencji przedprzestępczej. Jednocześnie należy podkreślić, że do strategicznych kierunków działania komend powiatowych Policji zaliczono też edukację mieszkańców w zakresie bezpieczeństwa lokalnego oraz ich aktywny udział w projektach prewencji kryminalnej. Dopiero w dalszej części katalogu zadań znajduje się ujawnianie przestępstw i wykrywanie ich sprawców. Oczywiście pełen zakres działania jednostek organizacyjnych Policji na szczeblu powiatu jest znacznie większy i obejmuje aż 24 zadania i kilkanaście podzadań. Oprócz tego każda komenda powiatowa posiada regulamin organizacyjny, który doprecyzowuje wykonywane zadania, przyporządkowuje je do poszczególnych struktur organizacyjnych, a także określa nadzór nad ich skuteczną i efektywną realizacją.

Po przeprowadzonej analizie regulacji prawnych, w których znajdują się zadania powierzone do realizacji jednostkom terenowym Policji, w tym komendom powiatowym zasadnym jest stwierdzenie, iż ich istotą jest przede wszystkim zapobieganie, czyli nie dopuszczanie do powstania zjawisk kryminogennych. Jednak jeżeli już one

zaistnieją to należy w sposób sprawny wykryć ich sprawców i udzielić odpowiedniej pomocy ofiarom. W dalszej części artykułu zostanie przedstawione studium przypadku poprzez odwołanie się do praktyki działania Komendy Powiatowej Policji w Legionowie. Teren działania tej jednostki organizacyjnej Policji obejmuje granice administracyjne powiatu legionowskiego, którego powierzchnia wynosi około 40 000 ha, a zamieszkuje na jego terenie ponad 113 000 tys. osób. W skład powiatu wchodzi miasto Legionowo i cztery gminy (Serock, Nieporęt, Jabłonna i Wieliszew). Gęstość zaludnienia powiatu legionowskiego wynosi 293 osoby/km^2. Najwyższy stopień zaludnienia występuje w samym mieście Legionowo (4 001 osób/km^2). Przy czym trzeba podkreślić, że gmina miejska Legionowo ma największą gęstość zaludnienia wśród 2 478 gmin w Polsce [Główny Urząd Statystyczny 2016, s. 12].

Diagnoza zagrożeń dla bezpieczeństwa lokalnego przeprowadzona przez Komendę Powiatową Policji w Legionowie

Komenda Powiatowa Policji w Legionowie (zwana dalej KPP), podobnie jak inne jednostki terenowe Policji, do diagnozowania zagrożeń w przestrzeni lokalnej najczęściej wykorzystuje metodę okresowej oceny stanu bezpieczeństwa i porządku publicznego. W ramach tej metody dokonywane są miesięczne, kwartalne, półroczne i roczne analizy dotyczące popełnianych przestępstw oraz wykroczeń, a także zjawisk kryminogennych występujących na terenie powiatu legionowskiego.

W 2016 roku wszczętych zostało ogółem 2 513 postępowań przygotowawczych, w tym 1 654 dotyczyły przestępstw kryminalnych. Ze zgromadzonych statystyk policyjnych wynika, iż w stosunku do 2015 r. nastąpił spadek (o 155) ogólnej liczby wszczętych postępowań przygotowawczych. Z kolei wskaźnik wykrywalności w całym powiecie w 2016 r. wynosił 54,58%, był w 2015 r. nieco mniejszy – 54,24%. Dane o wskaźniku wykrywalności najważniejszych dla społeczności lokalnej kategoriach przestępstw i ich liczbie przedstawiono w tabeli 1.

Najwięcej (aż 453) postępowań przygotowawczych wszczęto w związku z popełnieniem przestępstwa kradzieży cudzej rzeczy. Jednak wskaźnik wykrywalności w przypadku tej kategorii przestępstw ukształtował się na poziomie zaledwie 30,02% i był najniższy spośród siedmiu kategorii szczególnie dotkliwych społecznie przestępstw. Natomiast najmniej (tylko 17) popełniono przestępstw typu bójka lub pobicie. Jednocześnie, na podkreślenie zasługuje fakt dużej skuteczności KPP w zwalczaniu tej kategorii przestępczości, o czym świadczy wysoki wskaźnik wykrywalności, który ukształtował się na poziomie 72,02%.

Tabela 1. Dane dotyczące najbardziej dotkliwych społecznie przestępstw i ich wykrywalność w 2016 roku

KATEGORIA	Liczba wszczętych postępowań przygotowawczych	Wykrywalność
Bójka lub pobicie	17	72,02%
Uszczerbek na zdrowiu	37	70,04%
Uszkodzenie mienia	129	33,03%
Rozbój, kradzież rozbójnicza	22	42,09%
Kradzież z włamaniem	324	42,02%
Kradzież samochodów	56	40,00%
Kradzież cudzej rzeczy	453	30,02%
Ogółem:	**1 038**	**36,09%**

Źródło: opracowanie własne na podstawie: Komenda Powiatowa Policji w Legionowie [2016].

Z kolei liczba wykroczeń ujawnionych w 2016 r. wynosiła 25 177. Wykroczenia, chociaż są czynami o mniejszej społecznej szkodliwości, również mają istotny wpływ na porządek i bezpieczeństwo społeczności lokalnych. Dane dotyczące poszczególnych rodzajów wykroczeń prezentuje tabela 2.

Tabela 2. Dane dotyczące wykroczeń ujawnionych na terenie powiatu legionowskiego w 2016 r.

	RODZAJE WYKROCZEŃ	Liczba wykroczeń
WYKROCZENIA PRZECIWKO	porządkowi i spokojowi publicznemu (bez wykroczeń z art. 55 kw)	779
	bezpieczeństwu osób i mienia (bez wykroczeń z art. 82 kw)	123
	bezpieczeństwu i porządkowi w ruchu na drogach	20 387
	obyczajności publicznej	2
	urządzeniom użytku publicznego	334
	przepisom o ochronie przyrody	0
	mieniu	991
	przepisom ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi	1 584
	innym przepisom	1 199
	Ogółem:	**2 5177**

Źródło: opracowanie własne na podstawie: Komenda Powiatowa Policji w Legionowie [2016].

W analizowanym roku do najczęściej popełnianych wykroczeń na terenie powiatu legionowskiego należały: przeciwko bezpieczeństwu i porządkowi w komunikacji (ujawniono ich aż 20 387), dotyczące spożywania alkoholu w miejscach publicznych (1 584), a także związane z porządkiem i spokojem publicznym (779).

Jednym z kolejnych obszarów bezpieczeństwa, który wymaga monitorowania jest bezpieczeństwo w ruchu drogowym. W 2016 r. na terenie powiatu legionowskiego doszło do 29 wypadków drogowych. W ich rezultacie zginęły trzy osoby, a 36 zostało rannych. Ich główną przyczyną była nadmierna prędkość, nie ustąpienie pierwszeństwa pieszym, nie ustąpienie pierwszeństwa przejazdu oraz wykroczenia popełniane przez pieszych polegające na wejściu bezpośrednio przed jadący pojazd.

Stosunkowo nowym rozwiązaniem pozwalającym na zaangażowanie się społeczności lokalnej w proces diagnozowania zagrożeń bezpieczeństwa jest wdrożona w drugiej połowie 2016 r. Krajowa Mapa Zagrożeń Bezpieczeństwa (dalej zwana mapą). Na terenie powiatu legionowskiego liczba zgłoszeń na dzień 31 grudnia 2016 r. wynosiła ogółem 745, co świadczy o dużej aktywności społeczności lokalnej. Jednak ze zgromadzonych danych wynika, że tylko 153 zgłoszenia zostały potwierdzone, czyli pozytywnie zweryfikowane, natomiast aż 592 nie udało się zweryfikować. Bardziej szczegółowe dane na ten temat zawiera tabela 3.

Tabela 3. Dane dotyczące najczęściej zgłaszanych zagrożeń przez mieszkańców powiatu legionowskiego w 2016 r.

KATEGORIA ZAGROŻENIA	Zgłoszenia potwierdzone	Zgłoszenia niepotwierdzone
Nielegalne rajdy samochodowe	2	18
Nieprawidłowe parkowanie	92	83
Niewłaściwa infrastruktura drogowa	3	12
Przekraczanie dozwolonej prędkości	52	257
Spożywanie alkoholu w miejscach niedozwolonych	2	118
Zła organizacja ruchu drogowego	1	14
Dzikie wysypiska śmieci	1	11

Źródło: opracowanie własne na podstawie danych uzyskanych z Komendy Powiatowej Policji w Legionowie (za okres od 1 lipca 2016 rok do 31 grudnia 2016 r.).

Aż 41,5% wszystkich zgłoszeń dotyczyło przekraczania dozwolonej prędkości. Wskaźnik potwierdzalności dla tej kategorii zagrożeń ukształtował się na poziomie 16,8%. Warto zaznaczyć, że skorzystać Krajowej Mapy Zagrożeń Bezpieczeństwa może

w zasadzie każdy obywatel, który posiada dostęp do Internetu. Po zaznaczeniu na mapie miejsca i wyborze jednej spośród 25 kategorii zdefiniowanych zagrożeń Policja sprawdza zgłoszenie i na jego podstawie potwierdza lub nie fakt wystąpienia zagrożenia na danym terenie.

Podsumowując problematykę diagnozowania zagrożeń w przestrzeni lokalnej trzeba stwierdzić, że tylko w przypadku bezpieczeństwa w ruchu drogowym KPP dokonała analizy przyczyn zaistniałych zdarzeń drogowych. W odniesieniu do popełnianych przestępstw z siedmiu wybranych kategorii oraz ujawnianych wykroczeń, jak również pozostałych zjawisk kryminogennych brak informacji o ich ewentualnych przyczynach w dokumentach analityczno-sprawozdawczych będących przedmiotem badań.

Projekty profilaktyczne realizowane przez Komendę Powiatową Policji w Legionowie

O randze i znaczeniu prewencji w działaniach Policji najlepiej świadczy fakt, iż profilaktyka została uznana za jeden z priorytetów Komendanta Głównego Policji na lata 2016–2018[3]. Ponadto w dniu 30 kwietnia 2015 r. Komendant Główny Policji zatwierdził nową *Koncepcję działań Policji w zakresie profilaktyki społecznej na lata 2016–2018* [Komenda Główna Policji 2015]. W ramach prac nad tym dokumentem zdiagnozowano obszary dysfunkcyjne, ważne dla profesjonalizacji policyjnej profilaktyki społecznej, jak również wyznaczono cele w horyzoncie trzech lat. Najważniejsza konkluzja przeprowadzonej diagnozy dotyczyła uwzględniania w projektowanych działaniach, poza analizą zagrożeń opartą na statystykach policyjnych, oczekiwań społecznych i wniosków z badań realizowanych przez instytucje pozapolicyjne, w tym podjęcie działań zmierzających do stworzenia obserwatoriów na rzecz profilaktyki społecznej[4].

Z danych Komendy Głównej Policji wynika, że podczas debat społecznych przeprowadzanych z udziałem wspólnot lokalnych w ciągu ostatnich dwóch latach 80% postulatów kierowanych do Policji było związanych z profilaktyką społeczną. Analiza tych postulatów, a także celów zawartych w rządowych, krajowych i resortowych programach oraz wyników badań opinii publicznej pozwoliły na określenie priorytetowych obszarów dla policyjnej profilaktyki społecznej. Aktualnie na szczególną uwagę zasługują działania dotyczące bezpieczeństwa dzieci i młodzieży oraz osób starszych [Kuźnia 2015, s. 75]. Pełen katalog zawiera 22 obszary priorytetowe, a wśród nich: 1) narkotyki, dopalacze, środki odurzające; 2) bezpieczeństwo w ruchu drogo-

[3] Szerzej: Komenda Główna Policji [2016].
[4] Szerzej w: Komenda Główna Policji [2015].

wym; 3) cyberzagrożenia; 4) bezpieczeństwo dzieci i młodzieży – edukacja dla bezpieczeństwa.

W badanym roku KPP realizowała cztery programy profilaktyczne: „Kibic", „Z Borsukiem bezpieczniej", „Bezpieczny i kulturalny pasażer" oraz „Edukacja prawna w szkołach z udziałem warszawskiej Policji". Program profilaktyczno-edukacyjny pn. „Kibic" adresowany był do uczniów klas II szkół gimnazjalnych. Jego głównym celem było kształtowanie nawyków poprawnego oraz właściwego zachowania się kibiców w związku z organizowanymi masowymi imprezami sportowymi, jak również przygotowanie młodzieży do kulturalnego udziału w wydarzeniach sportowych. Podkreślenia wymaga interesująca i motywująca forma jego realizacji. Zgodnie z założeniami do tego projektu profilaktycznego powinien on być przeprowadzany na stadionie sportowym. Edukacja młodzieży odbywa się zatem w warunkach rzeczywistych, co może mieć znaczący wpływ na efektywność procesu kształcenia. Zakres tematyczny tych warsztatów obejmował m.in.:

1) zasady i przepisy obowiązujące na terenie ośrodka sportowego;
2) prawne aspekty negatywnych zachowań podczas masowych imprez sportowych;
3) psychologiczne aspekty zachowań agresywnych i asertywnych, sportowej złości oraz zasady rozpoznawania postaw związanych z przemocą i innymi negatywnymi zachowaniami [http://wprewencji.policja.waw.pl/wp/profilaktyka-spoleczna/programy-i-dzialania-pr/304,Program-profilaktyczno-edukacyjny-pn-KIBIC.html]. Jednorazowo w zajęciach mogła brać udział grupa młodzieży do 30 osób. Liczba opiekunów z kolei była uzależniona od wielkości grupy szkoleniowej i dostosowana do potrzeby zapewnienia bezpieczeństwa oraz prawidłowego zachowania się uczestników.

Program profilaktyczno-edukacyjny pn. „Z Borsukiem bezpieczniej" adresowany był przede wszystkim do pacjentów szpitali dla dzieci, zwłaszcza tych, które doznały różnego rodzaju urazów fizycznych, zarówno z winy osób dorosłych, jak i z braku wystarczającej wiedzy na temat bezpiecznych zachowań. Celem głównym tego projektu była poprawa bezpieczeństwa dzieci na drodze, podczas zabawy, jak również edukacja wiktymologiczna dzieci i młodzieży, aby nie stawały się ofiarami przestępstwa ze strony dorosłych i rówieśników. Program realizowany był w postaci wizyt policjantów wraz z maskotką „Borsukiem", którzy podczas pogadanki zapoznawali dzieci i młodzież z problematyką bezpieczeństwa ogólnego, przy wykorzystaniu elementarza szkoleniowego pn. „Z Borsukiem bezpieczniej". W czasie zajęć omawiano m.in. następującą problematykę:

1) zasad poruszania się po drodze, w tym przechodzenia po pasach;
2) zachowania się podczas przerw i przebywania na terenie szkoły;

3) przebywania samemu w domu i spędzania czasu wolnego [http://wprewencji.policja.waw.pl/wp/profilaktyka-spoleczna/programy-i-działania-pr/56413,Program-profilaktyczno-edukacyjny-pn-Z-Borsukiem-Bezpieczniej.html.]. Pogadankę przeprowadzano w małych grupach, aby umożliwić każdemu dziecku aktywny w niej udział. Podobne spotkania organizowano w placówkach oświatowych, w których miały już charakter zajęć interaktywnych.

Z kolei program profilaktyczno-edukacyjny pn. „Bezpieczny i kulturalny pasażer" skierowany był do uczniów szkół podstawowych, gimnazjalnych i kadry pedagogicznej. Jego celem głównym było kształtowanie umiejętności prawidłowego, bezpiecznego i kulturalnego zachowania się na przystankach oraz w środkach komunikacji publicznej, w szczególności uświadomienie zagrożeń wynikających z nieprzestrzegania obowiązujących zasad w czasie podróżowania komunikacją publiczną. Treści tego programu obejmowały m.in.:

1) zasady świadomego i bezpiecznego uczestnictwa w ruchu drogowym w charakterze pasażera środków komunikacji publicznej;
2) podróżowanie połączone z prezentowaniem postawy życzliwości, uczynności i odpowiedzialności za bezpieczeństwo swoje i innych osób;
3) przygotowanie młodych ludzi do udzielania pierwszej pomocy w komunikacji publicznej [http://wprewencji.policja.waw.pl/wp/profilaktyka-spoleczna/programy-i-dzialania-pr/56355,Program-profilaktyczno-edukacyjny-pn-Bezpieczny-i-kulturalny-pasazer.html]. Struktura programu pozwalała realizować go w małych grupach do 25 osób przy wykorzystaniu publicznych środków transportu, jak również na terenie placówek oświatowych.

Natomiast program informacyjno-edukacyjny pn. „Edukacja prawna w szkołach" adresowany był do szeroko rozumianego środowiska szkolnego tworzonego przez kadrę pedagogiczną, rodziców, dzieci i młodzież, a nawet przedstawicieli samorządu terytorialnego zajmujący się problematyką oświatową. Projekt ten miał na celu kształtowanie bezpieczeństwa w środowisku szkolnym. Uczestnikom warsztatów edukacyjnych była przekazywana wiedza m.in. na temat:

1) regulacji prawnych dotyczących przeciwdziałania niedostosowaniu społecznemu oraz realnemu zagrożeniu bezpieczeństwa i porządku w placówkach oświatowych;
2) odpowiedzialności prawnej nieletnich na podstawie obowiązujących przepisów prawnych;
3) współdziałania placówek oświatowych w sytuacji zagrożenia dzieci i młodzieży demoralizacją i przestępczością oraz zapobiegania zachowaniom ryzykownym [http://wprewencja.policja.waw.pl/wp/profilaktyka-spoleczna/programy-i-dzialania-pr/302,Edukacja-prawna-w-szkolach-z-udzialem-warszawskiej-Policji.html]. W ra-

mach realizacji założeń tego programu opracowano też dwie publikacje: poradnik dla policjantów pt. *Zapobieganie i zwalczanie demoralizacji oraz przestępczości wśród nieletnich* oraz informator dla nauczycieli nt. *Zasad współpracy Policji z placówkami oświatowymi*.

Reasumując należy zaakcentować, iż wszystkie cztery programy profilaktyczne zostały opracowane przez specjalistów z Komendy Stołecznej Policji. Problematyka tych programów nawiązywała do priorytetów profilaktyki społecznej ujętych w *Koncepcji działań Policji w zakresie profilaktyki społecznej na lata 2016–2018* [Komenda Główna Policji 2015]. Jednak w analizowanym okresie KPP nie realizowała chociażby jednego projektu, który byłby opracowany w następstwie przeprowadzenia diagnozy zagrożeń na poziomie lokalnym.

Zakończenie

Bezpieczeństwo lokalne jest i niewątpliwie będzie ważną przestrzenią dla życia indywidualnego jednostek oraz funkcjonowania społeczności lokalnych. Dlatego też wymaga postrzegania go w kategoriach dobra wspólnego, które jest przedmiotem zainteresowania i troski wielu podmiotów, jak również samych mieszkańców. W tym kontekście zasadnym wydaje się stwierdzenie, że podmiotem wiodącym, przynajmniej w sferze realizacyjnej, powinny być jednostki terenowe Policji.

W artykule opisano kształtowanie bezpieczeństwa lokalnego na przykładzie Komendy Powiatowej Policji w Legionowie. Przeprowadzona diagnoza dotyczyła trzech najważniejszych aspektów funkcjonowania każdej jednostki terenowej Policji, tj. zadań przez nią wykonywanych, metod i sposobów identyfikowania zagrożeń dla bezpieczeństwa społeczności lokalnych, a także realizowanych projektów profilaktycznych. Ważną płaszczyzną odniesienia było przedstawienie wybranych rozwiązań wdrożonych w całej Policji i zbadanie ich realizacji w praktyce działania jednostki stanowiącej przedmiot dociekań naukowych.

Na podstawie przeprowadzonych badań można sformułować dwie konkluzje o charakterze generalnym. Po pierwsze, kształtowanie bezpieczeństwa lokalnego powinno polegać przede wszystkim na diagnozowaniu zagrożeń, analizowaniu ich przyczyn i podejmowaniu działań zapobiegawczych, a dopiero potem na wykrywaniu przestępstw i wykroczeń oraz ściganiu ich sprawców. Po drugie, poziom bezpieczeństwa lokalnego zależy w dużym stopniu od zaangażowania się mieszkańców we wszystkie formy działań profilaktycznych, a także ich reagowania na wszelkie naruszenia bezpieczeństwa i porządku publicznego.

Natomiast odnosząc się do praktyki działania trzeba podkreślić, iż misją policji jest zapobieganie popełnianiu przestępstw i wykroczeń, w celu zapewnienia odpowiedniego poziomu bezpieczeństwa i porządku publicznego. Dlatego zasadnym jest uzupełnienie przeprowadzanych przez jednostki terenowe policji okresowych ocen stanu bezpieczeństwa i porządku publicznego o ten istotny obszar ich działalności. Kolejnym rozpoznanym w czasie badań problemem był brak dokonywania analiz dotyczących przyczyn zdiagnozowanych zagrożeń dla bezpieczeństwa lokalnego. Stąd postulat poszerzenia diagnozowania zagrożeń o katalog ich przyczyn, aby skuteczniej oddziaływać na poziom porządku i bezpieczeństwa publicznego. Wówczas byłaby możliwość podejmowania działań ukierunkowanych na konkretne przesłanki inicjujące niekorzystne społecznie zjawiska kryminogenne. Poszukując odpowiedzi na kluczowy problem badawczy „Czy realizowane przez Komendę Powiatową Policji w Legionowie projekty profilaktyczne są adekwatne do zidentyfikowanych zagrożeń oraz oczekiwań społecznych?" należy stwierdzić, że w analizowanym okresie jednostka ta nie realizowała projektu, który byłby opracowany w następstwie przeprowadzenia diagnozy zagrożeń na poziomie lokalnym. Dążąc do ograniczenia występujących zagrożeń trzeba przede wszystkim oddziaływać na wspólnotę lokalną poprzez dedykowane jej akcje profilaktyczne. Przywołane dedykowanie powinno mieć dwojaki charakter – z jednej strony należy eliminować przyczyny zagrożeń, a z drugiej, wykorzystując różne formy oddziaływań, docierać do wyselekcjonowanych adresatów, mogących być potencjalnymi sprawcami lub ofiarami tych zagrożeń. Zatem diagnozowanie zagrożeń powinno być uzupełnione o wskazane rozwiązania, co podniosłoby skuteczność i efektywność lokalnego systemu profilaktyki społecznej.

Reasumując przeprowadzona diagnoza funkcjonowania Komendy Powiatowej Policji w Legionowie pozwala przyjąć tezę, że odgrywa ona znaczącą rolę w kształtowaniu bezpieczeństwa lokalnego. Z tego powodu warto rozważyć zasadność wdrożenia proponowanych usprawnień i rozwiązań, aby jej współuczestnictwo w tym procesie było pełniejsze oraz spowodowało wzrost poczucia bezpieczeństwa społeczności lokalnej powiatu legionowskiego.

Bibliografia

Cylkowski T. (2015), *Rola Policji w systemie bezpieczeństwa wewnętrznego*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje", nr 20, ss. 127–143.

Główny Urząd Statystyczny (2016), *Raport pt. Powierzchnia i ludność w przekroju terytorialnym w 2016 r.*, GUS, Warszawa.

Komenda Główna Policji (2015), *Koncepcja działań informacyjnych Policji na rzecz profilaktyki społecznej 2016–2018. „Porozmawiajmy o prewencji… – aby żyło się bezpieczniej!"* (niepublikowana).

Komenda Główna Policji (2016)*, Priorytety i zadania priorytetowe Komendanta Głównego Policji na lata 2016–2018* (niepublikowane).

Komenda Powiatowa Policji w Legionowie (2016), *Ocena stanu bezpieczeństwa i porządku publicznego na terenie działania Komendy Powiatowej Policji w Legionowie za 2016 rok* (niepublikowana).

Kuźnia A. (2015), *Komentarz – Działania Policji w zakresie profilaktyki społecznej – perspektywy i wyzwania* [w:] Komenda Główna Policji, *Prewencja Policji. Perspektywy i Wyzwania*, Wydawnictwo Centrum Szkolenia Policji, Warszawa.

Serafin T., Parszowski S. (2011), *Bezpieczeństwo społeczności lokalnych. Programy prewencyjne w systemie bezpieczeństwa*, Difin, Warszawa.

Ustawa z dnia 6 kwietnia 1990 r. o Policji [Dz. U. z 2015 r., poz. 355, z późn. zm.].

Zarządzenie nr 1041 Komendanta Głównego Policji z dnia 28 września 2007 r. w sprawie szczegółowych zasad organizacji i zakresu działania komend, komisariatów i innych jednostek organizacyjnych Policji [Dz. Urz. KGP z 2013 r., poz. 50 z późn. zm.].

Netografia

http://wprewencji.policja.waw.pl/wp/profilaktyka-spoleczna/programy-i-dzialania-pr/304, Program-profilaktyczno-edukacyjny-pn-KIBIC.html, dostęp: 17.09.2017.

http://wprewencji.policja.waw.pl/wp/profilaktyka-spoleczna/programy-i-działania-pr/56413, Program-profilaktyczno-edukacyjny-pn-Z-Borsukiem-Bezpieczniej.html, dostęp: 17.09.2017.

http://wprewencji.policja.waw.pl/wp/profilaktyka-spoleczna/programy-i-dzialania-pr/56355, Program-profilaktyczno-edukacyjny-pn-Bezpieczny-i-kulturalny-pasazer.html, dostęp: 17.09.2017.

http://wprewencja.policja.waw.pl/wp/profilaktyka-spoleczna/programy-i-dzialania-pr/302, Edukacja-prawna-w-szkolach-z-udzialem-warszawskiej-Policji.html, dostęp: 17.09.2017.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **181–194**

Olga Menshykova[1]
Lviv State University of Life Safety, Ukraine
Taras Rak[2]
IT Step University Lviv, Ukraine
Yuriy Rudyk [3]
Lviv State University of Life Safety, Ukraine

Expanding of Compliance Assessment for Preventive Measures of Fire Safety as a Local Facilities with High Risk Level in Ukraine

Abstract: This paper presents the application of agent-based quantitative risk assessment with a fundamental review of public attitudes towards firefighting, a qualitative increase in the level of community responsibility for security. This is the goal that must be set, involving volunteers for their self-organization in matters of fire suppression. Involving volunteers in the task of preventing and eliminating fires will be more effective and will have a more productive result. This will minimize the time of arrival of the first fire-fighting unit to a place of fire or emergency, especially in the countryside. In addition, local, communal, volunteer organizations need to be widely involved in significantly enhancing the culture of safety among people, awareness and responsibility, and improving their personal skills and ability to work in extreme situations.
The process of improving the existing system of supervision over control in the field of fire and technological safety, fire prevention and emergency systems is essential. This would be part of the reform of the State Service of Ukraine for Emergency Situations.
Thus, the assessment of compliance with the level of safety in the local communities, the implementation or use of objects with a high degree of risk, which could endanger the consumer, is classified by the legislation of Ukraine to the legislatively regulated sphere and is mandatory.
Key words: technical regulation, risk, fire hazard, compliance assessment systems.

[1] helga.menshikowa@gmail.com
[2] rak.taras74@gmail.com
[3] rudyk@ldubgd.edu.ua

Introduction

The purpose of this article is to highlight the lack of security assessment measures at the local level. This is partly due to the reform of the local government administration initiated in Ukraine and the long-term reform of the security block at government level.

In particular, the administrative reform includes transferring the financing of certain security functions to the local level. The moratorium on the verification of compliance with security requirements by the central government deprives control and eliminates the application of preventive measures.

In Ukraine, there is a significant gap in the perception regarding responsibility for the security of local communities by the officials and authorities at all levels. And the same gap is in the lack of normative regulation of the process of transferring responsibility. No less noticeable is the lack of awareness of safety priority in home or industrial activities by the majority of people.

Therefore, the development and implementation of a clear and adapted to local conditions mechanism for assessing the compliance of security measures taken in an industrial institution, city block, village, and whole city will contribute to maintaining an adequate level of security of the populace and territories. One way to achieve this is to use existing methods and means to assess compliance of high risk industrial plants. The article presents justification and methods of such application in the field of fire safety and prevention.

In Ukraine, the activity of voluntary fire protection is regulated at the legislative and sub-legislative, territorial and local levels, taking into account local conditions and needs. Article 27 of the Civil Protection Code of Ukraine defines the bases for the functioning of voluntary civil protection formations [Code 2012].

Also, a resolution of the Cabinet of Ministers of Ukraine dated July 17, 2013, No. 564 "On Approval of the Procedure for the Functioning of Voluntary Fire Protection" was adopted, which approves the procedure for the operation of units of voluntary fire protection [Res. 2013].

Order of the SSES of Ukraine dated July 11, 2016 No. 331 "On Approval of the Partial Studies Plan and Training Program for the Special Training of Local Fire Guards and Members of Voluntary Fire Protection" permits, at the request of local self-government bodies and economic entities, to carry out on a contractual basis special training of local fire brigade personnel and members of voluntary fire protection based on training stations of emergency-rescue detachments of special purpose (units of technical service) Departments of the SSES of Ukraine in the regions, the

Higher Professional School of the Lviv State University of Life Sciences (Vinnytsia) and the Training Center of the Rescue Service of Civil Protection in accordance with the approved Model Curriculum and the curriculum of special training for local fire brigade personnel and members of voluntary fire protection squad.

According to the proposed definition [Draft 2016], voluntary fire brigade is a fire brigade founded by individuals and/or legal entities of private law, the main statutory goal (purpose) of which is to participate in fire prevention, fire extinguishing. Voluntary fire protection by organizational-legal form is formed as a public organization or a public union.

The urgency of creating such formations is that it is possible to avoid injury to people during fires, prevent significant material damage, if the elimination of fires began at the initial stage of their occurrence. A local level of fire safety can only be increased by territorial communities themselves by creating voluntary fire brigades, as is the case in developed European countries, Canada and the United States of America. It is actually crucial for local objects with high risk degree.

Foreign experience shows that the most effective way of fire protection locally and in the regions is the organization of voluntary fire brigade (hereinafter – VFB). The VFB abroad has historical roots and national peculiarities. In all countries it is created to unite the efforts of citizens (nonprofessionals) to combat fires. It should be emphasized that voluntary fire brigades exceed the number of professional firefighters and together with them create a sufficiently effective fire safety system. In Ukraine, despite the similar principles of creation and operation of voluntary fire units, there is a low level of fire safety at local communities. The reasons are low material and technical provision of fire brigades. For voluntary fire brigades this is one of the main reasons for their small number and low professional readiness.

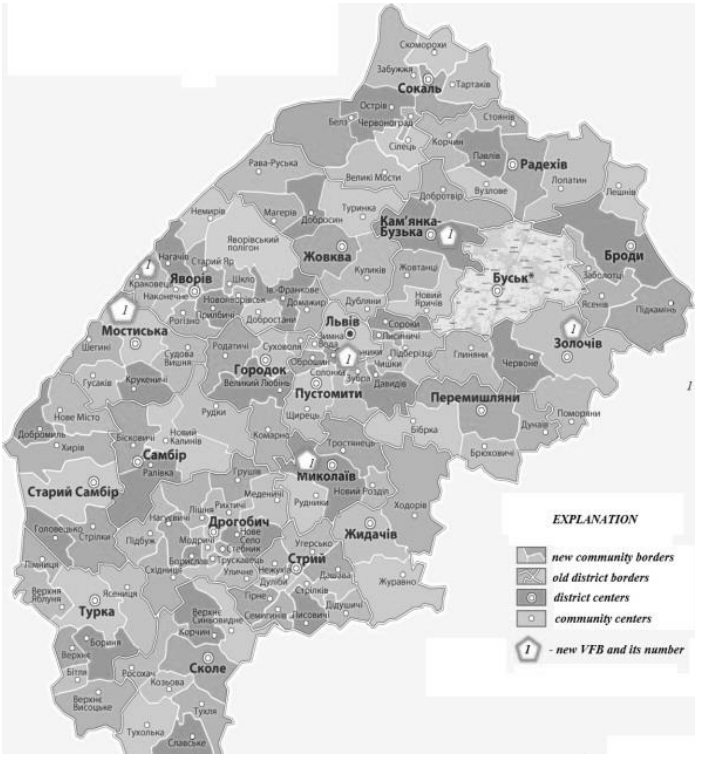
The European fire protection system is based on fire departments of local authorities and voluntary fire brigades. At present, up to 80% of the United Kingdom, Germany, France, and Italy's fire brigades consist of volunteers, indicating the effectiveness of cooperation between professional fire brigades and the community and volunteer organizations in fighting fire and mitigating the effects of emergencies. In Europe, fire brigade volunteers play a more important role than professional firefighters. In each European country there is an approach to the development of voluntary fire protection. In Germany, voluntary fire brigades exist in over 2070 settlements. In Switzerland and Austria, volunteers make up more than 90% of the total number of firefighters, and in Poland there are more than 3.8 thousand voluntary fire brigades. The equipment of voluntary fire brigades is not worse, it is even better than professional ones [Explanatory 2014].

Thus, the aim of the article was to determine functions of the VFB in local communities both for action at the objects with high risk degree and for preventive measures of fire safety on the ground of compliance assessment in technical regulation.

Approachable knowledge

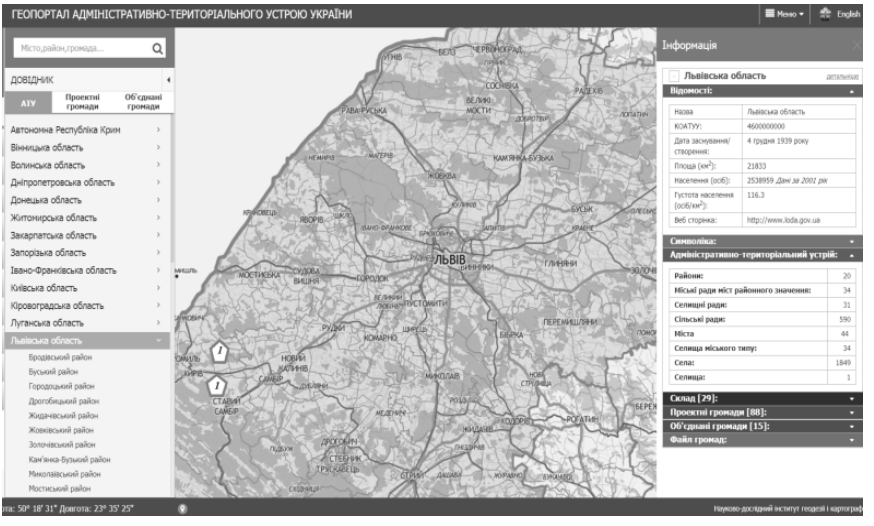
According to the target social program for the development of civil protection of the Lviv region for 2011–2013 and with the forecast for 2015, approved by the session of the Lviv Regional Council dated April 12, 2010, No. 1167, it was planned to create 6 VFB formations, namely in Zolochivsky district (Sasiv village), Kamyanka-Buzky district (Virov village), Mykolayiv district (Ternopillia village), Yavoriv district (Krakovets town), Mostysky district (Cherneve village), Pustomyty district (village Solonka), as shown in pictures 1 and 2.

Picture 1. The map of new VFB, created in Lviv region in 2013



Source: own elaboration.

Picture 2. The map of new VFB, created in Lviv region in 2015



Source: own elaboration.

During 2014–2015, no subdivision of local voluntary fire protection has been created. In connection with the military-political situation in the country, the implementation of the target social program for ensuring fire safety for 2013–2015 on the establishment of subdivisions of local voluntary fire brigades has been suspended.

In accordance with the reform of local self-government and territorial organization of authority, the Decree of the CMU of 11.11.2015 № 1158-p approved a promising plan for the formation of community territories of the Lviv region, according to which the creation of 85 communities is expected.

In 2015, 15 joint territorial communities were created in the Lviv region (Sambir district – 8, Zhydachiv district – 2, Brodivsky district – 1, Mykolayiv district – 1 and Stryj district – 1), in which the first elections were held in October, 2015. On the territory of these communities, there are only two Local FB (Grushatychi and Mizenets villages of Stary Sambir district) with the required 66. As of April 1st, 2016, 16 united territorial communities were created in the territory of the region, in which 64 LFB are planned but not established [Programs Lviv 2017].

By conducting analysis and taking into account the location of the existing state fire and rescue units, local fire brigades, the requirements DBN 360-92** "Urban planning. Planning and development of urban and rural settlements", regarding the normative calculation of the needs of fire depots and the number of fire trucks in settle-

ments, administrative territories and territorial communities were defined, in which additional 762 local fire brigades and 203 units of voluntary fire brigade are required.

According to the regional targeted social security program for the provision of fire safety for 2014-2016, in 2016 funds in the amount of 600 thousand UAH on the formation and functioning of 6 divisions of the VFB were planned [Programs Lviv 2017].

Analyzing the experience of realization of the reform in the Lviv region, it should be noted that on April 8, 2016, the head of the regional state administration and the head of the State Service of Ukraine for Emergencies signed a Memorandum of Cooperation on the organization of measures for civil protection of the population of the combined territorial communities of Lviv region [Programs Ukraine 2017]. In order to ensure an adequate level of safety of the population in the communities, an extensive system of local fire and rescue teams is planned that will be able to arrive at the scene within 20 minutes, while in Europe it is 8 minutes. In addition, within the framework of the reform, it is proposed to organize an active volunteer movement.

As part of the implementation of that Memorandum [Programs Ukraine 2017], a pilot project on organizing measures for civil protection of the population of capable territorial communities was launched. A pilot project started in the Sambir district of Lviv region. The Main Department of the SSE of Ukraine in the Lviv region conducted a dialogue with the leadership of the Babynska, Volya-Baranetska and Chukvyanskaya Territorial Communities on the establishment of local fire brigades. In addition, they allocate special firefighting equipment, fire and rescue equipment, military clothing, helmets that will be transferred to the volunteers in the area. There is also a large-scale work on consulting the representatives of territorial communities in the field of the development of the legal and regulatory component, providing methodical assistance to communities in calculating the optimal number of local civil protection services, which should be established at the level of each united community, taking into account their technogenic load.

Within the frame of the reform of local self-government and decentralization of authorities, the process of reforming the system of the State Service of Ukraine for emergencies is underway. Hence, on September 15, 2016, the Minister of Internal Affairs of Ukraine announced the reform of the SSE of Ukraine. One of the stages of the reform is the decentralization of the system and the creation of integrated fire brigades with the participation of volunteers.

It is worth pointing out that in European countries and the United States, the moral encouragement of volunteer firefighters in the form of awards, honors, and public gratitude is widely used. A feature of the VFB in European countries is that

volunteer firefighters create public associations (unions, associations, etc.) together with professional firefighters and scientific and technical organizations specializing in the development and production of fire-fighting equipment. For Ukraine, in the context of adapting the experience of foreign countries, it is important that the improvement of fire protection lies in the area of authority decentralization and the increase of local self-government bodies through their financial autonomy. Only then can the issue of qualitative provision of the establishment and operation of the VFB be resolved, attract the necessary funds for this and provide appropriate social benefits and preferences to the members of these wives. The development of local self-government will allow us to quickly solve all issues that concern community members and will enable them to influence the level of their well-being. State interference in this process should be minimal.

The reform of decentralization of government will ensure adequate funding for voluntary fire brigade units from local budgets to protect the lives of people and property of territorial communities.

Rescuers conduct work on the creation of voluntary fire brigades based on the actual units of local fire brigade and initiate amendments to the relevant legislation. This will allow local authorities to recruit voluntary fire brigades members who have been trained and tested on the specialty “firefighter-rescuer” on the basis of training units of the territorial divisions of the SSE of Ukraine in accordance with the established procedure.

The state of things

Fire broke out on the night of June 14, 2017 in a 24-storey residential building in the west of London. Grenfell Tower was built in 1978, and it consisted of 127 apartments. Residents say that the fire alarm was not working in the house. It is also noted that British high-rise buildings do not install systems for extinguishing fires.

The inhabitant of Grenfell Tower testifies that the fire stairs were covered by a fire: "There was no fire outlet, because these stairs were in the fire. The house was recently repaired, the outside lining was fit with some plastic from above and replaced the windows, and the fire went under this new lining, which stayed on the wooden slats, and almost all the residents of the house were worried about this, we had a meeting about this repair, and we were afraid that this could happen. We were all impressed by how quickly the fire broke out: first there was nothing – and then everything is burning! At first the fourth floor was on fire but the whole house is very big ...". Another young man who heard screams about the fire in the apartment opposite,

thought to stay in the apartment. Then a fire alarm rang, and they decided that they had to leave. It seems that the firefighters could not get to the fire crane – whether it did not work, or they could not open it... It turned out that the fire started in the kitchen, and then the fire through the window began to spread through the lining, which was only recently put there… and, apparently, the fire outlet also burned, so people from above could not go down, and the firefighters were not able to get up [*Експерт про пожежу в Лондоні: двері мали стримати вогонь* 2017].

Picture 3. Photos of Grenfell tower fire inside and outside

Source: BBC 2017.

According to several eyewitnesses, the fire quickly spread throughout the building after the lining flared up. The fire quickly spread from the fourth floor to the eighth, then to the corner of the building, and then turned over to another corner. The witnesses saw that the high-rise building of the Greenfield Tower was on fire from one side – from top to bottom, but only on the one side, and as the fire flipped over to the other sides.

Nearly 250 London firefighters tried to extinguish the fire for almost ten hours. Forty firefighters and more than 100 physicians worked on the site. To extinguish a fire on high floors, which is not reached by the spray of the fire brigade, fire can only be dealt with by getting to it from below – there are no other ways. As of the evening of June 14, the firemen did not succeed in completely extinguishing the flames. On June 15, rescuers suspended searches because of a high probability of collapse of the building. After all, approaching the edges of a burned building is dangerous. More than 120 families were left without a roof over their head and are housed in public centers [Wikipedia 2017].

The British security standards should allow the occupants of the high-rise building in which the fire occurred wait for the firefighters, or leave the building unhindered, told BBC Robert Tavener, retired fire inspector. Previously, the rules of fire safety of the buildings cover only what happened inside the building, and not outside. If the fire is exterior, then you can go back and walk – ways of leaving, corridors and stairs should be free. Judging by the way the fire was propagating, whether the Grenfell Tower was in line with the fire requirements was rhetorical, the facing could have been made of plastic, but residents could still evacuate when they saw the fire from the outside.

The expert clarifies that according to the British rules, fire safety in buildings provides fireproof hermetic doors in apartments and stairs. The apartment doors restrain the fire for an hour, and if the fire originated in another apartment – and its door also held back the fire – then you have two hours. Doors are tested for compliance with British fire regulations. That people were told to stay in apartments as it is a rule. The design should allow remaining in the apartment for two hours, waiting until the fire fighters are dealing with fire. The same doors must isolate the fire stairs [*London fire: a visual guide to what happened at Grenfell Tower* 2017].

The fire department does not currently confirm that the fire started on the fourth floor caused by the ignition of a refrigerator. The Greenfell Tower Association of Citizens has repeatedly warned the company responsible for the management of the facility about the threat to people's lives due to the unsatisfactory state of fire safety. Experts on fire safety were surprised with the speed at which the fire spread throughout the house. In many reports, interviewed local residents blamed for the spread of fire tile, which the house had completed to cover just over a year ago during a major overhaul of almost 9 million pounds.

Research and outcomes

As it appears, there is a problem of coordination for the local level of measures and actors to prevent fires – the function of monitoring compliance with fire regulations and rules. In Ukraine, as can be seen above, the permanent reform of supervisory bodies, both in consumer policy and in life safety, leaves local communities without proper protection. No draft legislation on this subject is covered in public discussion. If the organization of rescue and extinguishing of fires is still in the process of transformation, the preventive direction of work to prevent the emergence and minimization of the consequences of emergencies remained individual.

Given the passage of qualitatively different changes and types of influence, it is possible to consider fire, chemical leak, radiation and other types of hazards. Causes of hazards can be found both in the object under study and in the surrounding objects. The selection of the assessment procedure may affect the situation in which the possibility of causing damage occurs. Evaluation management can be carried out both from the inside of the object and from outside of its limits; Individual evaluation and management functions can be combined. Different management strategies have a different effect on the object.

To assess the effectiveness of management the concept of "risk" as a measure of hazard under a different management strategy can be introduced, including the risk of lack of management. Risk is a measure of hazard that characterizes the possibility of causing harm and its severity. It is assumed that it is possible to estimate the scale of the damage – its severity. This definition includes, as a separate case, the application in practice of risk assessment methods as a mathematical expectation of a loss [Emelyanenko 2012].

In general, the concepts of “risk” and “hazard” complement each other. Most often, the risk acts as a characteristic of change (risky actions), and hazard – as a characteristic of the state of the object (a hazardous factor). The practice shows that zero risk in the existing technical systems is impossible to provide. The global recognition has received the concept of tolerable (acceptable) risk. The content of this concept is the pursuit of low safety. This permissible risk is provided through the technical, economic, social and political directions of human activity. Tolerable (acceptable) risk of an accident is a risk, the level of which is permissible and justified on the basis of socio-economic considerations.

The high risk degree of the operation of an object is acceptable if, for the benefit of the facility, the society is ready to take this risk. Thus, acceptable risk represents a certain compromise between the level of safety and the possibilities of its achievement. It is now assumed that for the action of man-caused hazards in general, an individual risk is considered acceptable if its value does not exceed 10^{-6}. Risk is the possibility of occurrence and probable magnitude of the consequences of negative influence over a certain period of time. In some countries, the tolerable risks are set by law. The range of acceptable risks varies from a maximum of 10^{-6} per year, to a minimum of 10^{-8} per year. For ecosystems, the tolerable risk is equal to the amount at which 5% of the species of biogeocoenosis can suffer. Ukraine has declared such an approach in technical regulation, but statistics show that the real risk of death is higher by 10–100 times [Rudyk 2010].

Safety is closely linked with the economic aspect of the activity of a particular industrial enterprise, so it cannot rise to infinity. With an increase of safety costs social risk rises, but technical risk decreases. The growth of social risk means that the company is forced to spend money on solutions for questions of reducing the technical risk, while it reduces the payment of social issues. Of course, the overall social risk in society is reduced. This defines the emerging contradictions between the interests of individual enterprises and society.

The Law of Ukraine "On Hazardous Objects" [2001] defines the tolerable risk – a risk that does not exceed the maximum permissible level in the territory of an object of increased hazard and/or its borders. The same law states that risk management refers to the decision-making process and the implementation of measures aimed at ensuring the minimum possible risk.

Knowledge of individual risk does not allow us to judge the scale of disasters. 10 deaths could be recorded in one of 10 accidents or catastrophic accidents. Therefore, the concept of "social risk" is introduced.

Social risk is defined as the dependence of the risk (frequency of occurrence) of events occurring in the damage of a certain number of people exposed to the striking influence of a definite species, when realizing certain hazards from this number of people. It characterizes the scale of catastrophic hazards.

The hazards and risks associated with them are everywhere, but when known measures can be taken, they minimize or eliminate the risk. Walking down the stairs is followed by a risk of falling, but the probability of this is negligible. Ladders are dangerous, the probability of injury is known as a risk.

Risk management is based on achieving a certain level of safety, the balance of benefits and costs within an individual object, territory and the state as a whole. At the same time, risk management mechanisms aimed at reducing their values have not been widely practiced. Thus, quantitative risk assessment is used only in selected areas, namely, in the analysis of the safety of nuclear power plants, the declaration of safety of high-risk objects. The main mechanisms of state regulation in the field of risk management are state standardization, certification, state expertise, state supervision and control, licensing, economic regulation, declaration of safety of dangerous objects and insurance.

These mechanisms are based on the introduction of protective measures in the characteristics of products or systems that remain more effective, as experience shows that even well designed software can be dropped or overcome, or information for improvement may not be applicable.

The provision will be applied to provide safety in all cases of the project, which will not make it possible either to sufficiently reduce the risk or eliminate hazards. Supplementary protective measures involving additional equipment may increase safety.

Relatively low reliability of the effect of information for improvement is expected, which may consist of organizational measures, proper behavior, attentiveness, the use of personal protective equipment (PPE), skill and training, compared with proven technical protective equipment. Information for improvement will not be a substitute for the correct use of safety precautions by project measures, provision or supplementary protective measures.

On the one hand, the degree of risk exposure to achievement of goals, and the other the degree of uncertainty, which is determined by the risk itself, should be distinguished. For example, the risk of using improper quality raw materials which allows to reach the ultimate goal has a very significant impact, but assume that the probability of such a risk is low, then their product will indicate an insignificant level.

Conclusion

A fundamental review of public attitudes towards firefighting, a qualitative increase in the level of community responsibility for safety – these are the goals that must be set, involving volunteers for their self-organization in matters of extinguishing fires. Involving volunteers in the task of preventing fires will be more effective and will have a more productive result. In addition, local, communal, volunteer organizations need to be widely involved in significantly enhancing the culture of safety among people, awareness and responsibility, and improving their personal skills and ability to work in extreme situations.

1. The process of improving the existing system of supervision over control in the field of fire and technological safety, fire prevention and emergency systems is essential. This would be part of the reform of the State Service of Ukraine for Emergency Situations. One of the steps in this reform is the use of existing methods and means of assessing compliance of high-risk facilities at the local level.

   An equally important step is the expansion of the network of local fire brigades in the territorial communities and the involvement of volunteers to provide fire protection. This will minimize the arrival time of the first fire-fighting unit to a place of fire or emergency, especially in the countryside.

   Thus, the reform of the local self-government institution, the transfer of a number of functions from the state to local authorities, an increase in the financial compo-

nent of local budgets necessarily raise the issue of expanding the network of voluntary fire brigades in Ukraine.

2. The risk as a measure of hazard, characterizing the possibility of causing harm and its severity, depends on the severity (financial expression) of the harm that may result from the danger considered; and the probability of occurrence of that harm is a function from vulnerability to hazard, display of a hazardous event, technical and human ability to avoid harm.
3. The compliance assessment of the safety level at the local object, the application or use of high risk degree objects that may endanger the consumer is attributed to the legislation in Ukraine is mandatory for execution.
4. Accepting the definition of safety as the presence of this system in an acceptable risk (insignificant and/or unlikely) we consider it as an indispensable component of quality. Consequently, quality management involves compliance assessment tools.

Quality management is conducted taking into account a certain level of safety, balance of benefits and expenses within the limits of the separate object, territory and the state as a whole. Quantitative risk assessment, which is used only in selected areas, namely during the analysis of safety of nuclear power plants, declaration of safety of high-risk objects, is supplemented by the main mechanisms of state regulation in the field of risk management: standardization, certification, state expertise, state and market supervision and control, licensing, economic regulation, declaration of safety of hazardous objects and insurance.

Bibliography

Draft Law on Voluntary Fire Protection No. 4011a of 15.07.2016, [online] www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59781, access: 15.08.2017.

Emelyanenko S.O. (2012), *Estimation of fire risk for electrotechnical reasons in residential buildings*, [in:] Emelyanenko S.O., Rudyk Yu.I., Kuzyk A.D, "Fire safety", No, 20, pp. 105–110.

Explanatory note to the draft Law on Voluntary Fire Protection No. 4011a dated July 15, 2014, [online] www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59781, access: 15.08.2017.

Programs of the Main Department of SSES in Lviv region, [online] www.lviv.dsns.gov.ua/en/Programi.html, access: 15.08.2017.

Programs of the SSES Ukraine, [online] www.dsns.gov.ua/ua/Pilotni-proekti.html, access: 15.08.2017.

Resolution of the Cabinet of Ministers of Ukraine No. 564 dated 17.07.2013, On Approval of the Procedure for the Functioning of Voluntary Fire Protection.

Rudyk Yu.I. (2010), *Estimation of the fire hazard of the transient resistance growth in electrical connections* [in:] Rudyk Yu.I, Stolyarchuk P.G., "Bulletin of the National University Lviv Polytechnic", No. 665: Automation, Measurement and Control, pp. 101–107.

The Code of Civil Protection of Ukraine, [online] Code number 5403-VI dated 02.10.2012, access: 15.08.2017.

Експерт про пожежу в Лондоні: двері мали стримати вогонь (2017), "BBC News" [online], www.bbc.com/ukrainian/features-40278834, access date: 18.06.2017.

Grenfell Tower Fire, "Wikipedia, The Free Encyclopedia" [online], www.en.wikipedia.org/wiki/Grenfell_Tower_fire, access date: 18.06.2017.

London fire: a visual guide to what happened at Grenfell Tower (2017), "BBC News", [online] www.bbc.com/news/uk-40301289, access: 04.08.2017.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **195–202**

Sławomir Jankiewicz[1]
Wydział Finansów i Bankowości, Wyższa Szkoła Bankowa w Poznaniu

Infrastruktura energetyczna jako istotny element bezpieczeństwa Polski

Energy Infrastructure as an Important Element of Poland's Security

Abstract: Poland, wanting to catch up with highly developed countries, needs to boost economic growth. However, this requires fulfilling many conditions. One of them is providing electricity adapted to the needs of the economy.
The aim of the article was a synthetic analysis of the production and transmission infrastructure (the two most important elements of the system) in the context of Poland's energy security. This allowed us to verify the hypothesis, which was: the current decapitalization of energy assets negatively affects the country's energy security. This poses a potential threat to the pace of economic development. Especially, the change in the factors on which it is based and the increase in wealth will increase the demand for energy.
Key words: economic development, energy policy, power transmission systems.

Wstęp

Polska, pragnąc dogonić kraje wysokorozwinięte, musi zwiększyć tempo rozwoju gospodarczego. Ponadto jego wysoki poziom powinien zostać utrzymany przynajmniej przez całą dekadę, aby możliwe było zbliżenie się poziomem dobrobytu do tzw. starych krajów UE. Wymaga to spełnienia wielu warunków. Jednym z nich jest dostarczenie energii elektrycznej dostosowanej do potrzeb gospodarki. Wiąże się to z zapewnieniem odpowiedniej ilości energii oraz sprostaniem oczekiwaniom w zakresie jej parametrów jakościowych. W przypadku nowoczesnej gospodarki obok energii,

[1] slawomir.jankiewicz@wsb.poznan.pl

której napięcie zasilania (wartość, niesymetria, częstotliwość, kształt przebiegu czasowego) nie ulega dużym wahaniom, istotne jest także utrzymanie ciągłości zasilania (co oznacza, że w normalnych warunkach przerwy są sporadyczne) [International Electrotechnical Commission]. Umożliwia to poprawną pracę nowoczesnych urządzeń, które są wymagające w tym zakresie. Nawet niewielkie zmiany jakości dostarczanej energii mogą wpłynąć na ich awaryjność lub niestabilną pracę (np. przegrzewanie, zwiększone drganie, nieplanowe wyłączenie), co powoduje nadmierne zużycie lub zakłócenie przebiegu procesów i tym samym prowadzi do strat. W ubiegłym roku z powodu tzw. złej jakości energii elektrycznej gospodarka UE straciła według szacunków ok. 150 mld euro.

Energia elektryczna jest ważnym czynnikiem budowy innowacyjnej gospodarki. Z tego też powodu UE przyjęła, że głównym celem wspólnotowej polityki energetycznej jest m.in. zapewnienie bezpieczeństwa dostaw energii [Wersja skonsolidowana Traktatu o Unii Europejskie 2010, art. 194]. Ponieważ na poziomie krajowym bezpieczeństwo energetyczne ma równie istotne znaczenie, odniesienie do tego zagadnienia można znaleźć w Prawie energetycznym, Doktrynie zarządzania bezpieczeństwem energetycznym oraz Polityce energetycznej Polski do 2025 roku [Ministerstwo Gospodarki i Pracy 2004; Ustawa z dnia 10 kwietnia 1997 i Ministerstwo Gospodarki i Pracy 2005].

Zarządzanie bezpieczeństwem energetycznym na poziomie kraju uzależnione jest przede wszystkim od potencjału wytwórczego, stopnia dywersyfikacji produkcji, posiadanych surowców energetycznych oraz technicznych możliwości importu energii elektrycznej i surowców służących do jej produkcji. W przypadku importu szczególnie ważne są możliwości zapewnienia ciągłości dostaw w sytuacjach nadzwyczajnych. Ponadto z punktu widzenia bezpieczeństwa niezbędne jest utrzymywanie niezawodności sieci przesyłowych, by system był gotowy do ciągłej dostawy oraz przetrzymania nagłych i nieprzewidzianych zakłóceń.

Celem artykułu jest syntetyczny opis infrastruktury wytwórczej i przesyłowej (a więc dwóch najważniejszych elementów systemu) w kontekście bezpieczeństwa energetycznego Polski. Pozwoli to na zweryfikowanie hipotezy, że obecna dekapitalizacja majątku energetycznego wpływa negatywnie na bezpieczeństwo energetyczne kraju i stanowi potencjalne zagrożenie dla tempa rozwoju gospodarczego. Szczególnie, że zmiana czynników, na których się on opiera, oraz wzrost zamożności spowodują zwiększenie popytu na energię elektryczną.

Sieci przesyłowe energii elektrycznej jako podstawa zapewnienia bezpieczeństwa w Polsce

Energię elektryczną nie tylko należy wyprodukować, ale i dostarczyć do odbiorcy, kiedy jest na nią zapotrzebowanie. Umożliwia to m.in. system elektroenergetyczny, który obejmuje sieć przesyłową i dystrybucyjną. W Polsce mamy dwie grupy podmiotów, które się tym zajmują – PSE (Polskie Sieci Elektroenergetyczne S.A.) i OSD (Operatorów Systemu Dystrybucyjnego).

PSE jest spółką państwową, która odpowiada za zapewnienie na poziomie kraju infrastruktury dla hurtowego rynku energii elektrycznej i powiązanie go z zagranicą oraz zabezpieczenie pracy Krajowego Systemu Elektroenergetycznego [Ustawa 1997, art. 9c ust. 2]. PSE zarządza krajową siecią wysokich napięć o łącznej długości prawie 14 tys. km, na którą składa się 246 linii (w tym 1 o napięciu 750 kV, 77 linii o napięciu 400 kV i 168 linii o napięciu 220 kV) i jedno podmorskie połączenie ze Szwecją (o napięciu 450 kV). Pozostałe linie (o łącznej długości ok. 800 tys. km) są własnością OSD [Jankiewicz, Grądzik 2017]. Operatorzy Systemu Dystrybucyjnego są odpowiedzialni m.in. za dbanie o sieć (tj.: eksploatację, konserwację, rozbudowę, zarządzanie przepływem energii). Większościowym właścicielem najważniejszych OSD (PGE Dystrybucja S.A., Enea Operator Sp. z o.o., Tauron Dystrybucja S.A. i Energa-Operator S.A.) jest państwo.

Bezpieczeństwo sieci energii elektrycznej dotyczy zapewnienia ciągłości przepływu bez zmian parametrów technicznych prądu i szybkiego usuwania awarii. W Polsce może być z tym problem, ponieważ majątek sieciowy jest znacznie zdekapitalizowany [Jankiewicz 2013, ss. 27–38; Żmijewski, Sokołowski 2010, ss. 87–94]. Według szacunków średni wiek linii wynosi 40 lat, co oznacza, że jest bliski zużyciu technicznemu. M. Kleiber, J. Steinhoff, K. Żmijewski [2016] szacują, że linie przesyłowe są zdekapitalizowane w 71%, a dystrybucyjne aż w 70–80%. W przypadku sieci wysokich napięć aż 82% linii 220 kV i 25% linii 400 kV ma ponad 30 lat, 20–30 lat ma z kolei 17% z pierwszej i 56% z drugiej grupy [Ministerstwo Gospodarki 2013; Ministerstwo Gospodarki 2014]. Sieci te zostały zbudowane według innych standardów technologicznych i są przystosowane przede wszystkim do podłączenia dużych wytwórców energii elektrycznej. Charakteryzuje je również niska gęstość. Na 1000 km^2 przypada w kraju 41 km sieci (podobnie jak na Węgrzech), a więc mniej niż na Słowacji czy w Czechach i dużo mniej niż w krajach wysokorozwiniętych (np. Szwajcaria – ponad 161 km, Niemcy – 100 km, Francja – 90 km lub Holandia – 80 km [Stankowska 2009 i *Raport o wpływie uregulowań…* 2009]. Polska posiada też znacznie mniejszą liczbę stacji transformatorowych niż kraje lepiej rozwinięte [50hertz 2015].

Wpływa to na znaczne ograniczenie możliwości przesyłania energii elektrycznej i podłączenia do sieci nowoczesnych źródeł wytwarzania (tj. odnawialnych, które są niewielkiej mocy i znacznie rozporoszone), a także zwiększa ryzyko awarii i wydłuża czas naprawy. Ponadto odnotowujemy dużo większe niż średnia unijna straty na przesyle energii elektrycznej (według szacunków Biura Bezpieczeństwa Narodowego w 2011 roku całkowita strata w przesyle energii elektrycznej w Polsce wyniosła 10 774 GWh, co stanowiło 7,3% całej energii wprowadzonej do systemu i kosztowało 2,1 mld zł) [Rudźko 2012].

Wraz ze wzrostem popytu na energię elektryczną i rozwojem OZE (odnawialnych źródeł energii) potrzebne będzie zwiększenie gęstości i unowocześnienie sieci. Konieczne będą inwestycje w tzw. inteligentne sieci elektroenergetyczne, a więc takie, które „są w stanie efektywnie integrować zachowanie i działanie wszystkich podłączonych do nich użytkowników – wytwórców, konsumentów i użytkowników będących zarówno wytwórcami, jak i konsumentami" oraz pozwalają na stworzenie „oszczędnego pod względem gospodarczym i zgodnego z zasadami zrównoważonego rozwoju systemu energetycznego, charakteryzującego się niskim poziomem strat oraz wysoką jakością i bezpieczeństwem dostaw" [Energy… 2011]. Wprawdzie proces inwestycyjny (wymiana starych oraz budowa nowych linii) systematycznie trwa, jednak jest on zbyt powolny. Po pierwsze, brakuje środków na przyspieszenie do poziomu potrzeb (według szacunków w najbliższych kilku latach powinniśmy zainwestować ok. 60 mld zł, z tego ponad 9 mld zł we wprowadzenie inteligentnych liczników) [Żmijewski 2014]. OSD nie są w stanie wygospodarować takich funduszy ze środków własnych, a URE nie wyrazi zgody na ich przerzucenie na społeczeństwo, gdyż wymagałoby to znacznego podwyższenia cen energii, a w efekcie spowodowało osłabienie konkurencji krajowych przedsiębiorstw i wzrost kosztów utrzymania gospodarstw domowych (szczególnie, że dla właściciela – Skarbu Państwa – priorytetem jest maksymalizacja dywidendy, a nie wzrost kapitałów). Nie ma też możliwości pozyskania całego wymaganego kapitału na rynku, co wynika głównie z dużego ryzyka (gdyż jak prognozuje UE, nie wszystkie przedsięwzięcia z tego zakresu będą opłacalne [Komisja Europejska 2006]).

Po drugie, inwestycje ograniczają uwarunkowania prawne. Obecnie uzyskanie pozwoleń na budowę lub uwarunkowań środowiskowych może trwać do 12 lat. Dochodzą do tego problemy z procesami planistycznymi oraz dostępem inwestora do nieruchomości, na której ustawiona jest sieć. Z tego powodu średni czas kompleksowej budowy linii przesyłowej wynosi 7–15 lat.

Bez zmian prawnych i strategii rozwoju sieci Polska może mieć problem z tempem rozwoju gospodarczego.

Dekapitalizacja majątku w wytwarzaniu energii elektrycznej jako problem dla bezpieczeństwa kraju

W Polsce zapotrzebowanie na energię elektryczną w porównaniu z wysokorozwiniętymi krajami jest relatywnie niskie i wynosi per capita ok. 3500 kWh rocznie. Wraz ze wzrostem zamożności będzie ono ulegało zwiększeniu i szacuje się, że w 2030 roku osiągnie wartość ok. 7000–7500 kWh (tj. obecną średnią krajów UE). Możemy także oczekiwać wzrostu zapotrzebowania ze strony przedsiębiorstw, ponieważ innowacyjna gospodarka (a z taką będziemy mieć do czynienia w Polsce, jeżeli chcemy osiągać wysokie tempo rozwoju gospodarczego) jest energochłonna [Jankiewicz 2014]. Oznacza to, że konieczne będzie zwiększenie podaży energii elektrycznej i to nawet w przypadku pozytywnych zmian w zakresie efektywności energetycznej. Według szacunków ekspertów do 2030 roku moc zainstalowana w zakresie podaży energii elektrycznej powinna zwiększyć się o ok. 40% [Jankiewicz 2014; Forum Energii 2017] Jeżeli weźmiemy pod uwagę nie średnioroczne obciążenie systemu elektroenergetycznego, ale zapotrzebowanie w tzw. szczycie (czyli czasie największego popytu) i konieczność utrzymania rezerwy (na nieprzewidziane zmiany obciążenia, awarie czy wyłączenia z powodu remontów), to wzrost ten powinien być jeszcze większy. Niestety może być z tym problem. Wynika to z faktu, że obecne bloki energetyczne są znacznie zdekapitalizowane (ok. 60% elektrowni ma ponad 30 lat, a z tego ponad 30% ma 40 i więcej lat) i w pierwszej kolejności konieczne jest odtworzenie potencjału (do 2030 roku dotyczy to jednostek o łącznej mocy 16 000 MW) [Jankiewicz 2014]. Obecnie planowane i będące w budowie jednostki konwencjonalne będą miały moc tylko ok. 8,5 tys. MW [Agencja Rynku Energii 2016]. Dochodzi do tego – jeżeli zostanie wybudowany – blok atomowy o mocy 3000 MW. To za mało, by zastąpić wycofywane z eksploatacji jednostki, a przecież powinniśmy zwiększyć nasz potencjał. Sytuacja ta będzie miała negatywny wpływ na bezpieczeństwo energetyczne i tym samym na możliwości rozwoju gospodarczego. Zwróciła już na to uwagę Najwyższa Izba Kontroli w 2013 roku, informując, że możliwe są okresowe dysproporcje pomiędzy popytem a podażą na rynku energii elektrycznej już w najbliższych latach. Szczególnie przy ekstremalnych warunkach pogodowych lub w przypadku dynamicznego wzrostu zapotrzebowania na energię w obiektach położonych daleko od elektrowni [NIK 2013].

Powinniśmy więc zwiększyć nakłady na inwestycje w moce wytwórcze, jakkolwiek nie będzie to łatwe. Po pierwsze, przedsiębiorstwa energetyczne nie mają potencjału, by sfinansować je samodzielnie ani by pozyskać potrzebne środki od sektora finansowego (zbyt niska EBITDA). Ponadto okres zwrotu w wytwarzaniu wynosi kilkadziesiąt lat, a więc inwestycje tego typu są ryzykowne, co dodatkowo zniechęca kapitał obcy

do finansowania. Po drugie, firmy z tego sektora zostały zmuszone do ratowania górnictwa, co jeszcze zmniejsza ich możliwości finansowania. Będą ponosić znaczne nakłady na restrukturyzację branży wydobywczej i inwestować przede wszystkim w bloki oparte na węglu jako paliwie (i to niezależnie od ich opłacalności ekonomicznej w odniesieniu do innych źródeł oraz negatywnego wpływu na środowisko). Po trzecie, potencjał finansowy wytwórców jest systematycznie uszczuplany przez konieczność wypłaty dywidendy, której domaga się Skarb Państwa.

Kolejna barierą jest czas potrzebny na wybudowanie bloku energetycznego. Dla jednostek węglowych wynosi on ok. 7 lat, a dla atomowych jest jeszcze dłuższy i, w przypadku Polski, trudny do oszacowania (pierwotnie przyjmowano ok. 10 lat, co oznacza, że taki blok powstanie w 2020 roku; obecnie mówi się o roku 2030, tj. po 20 latach). Należy zwrócić uwagę, że trudności z budową elektrowni atomowych mają też kraje posiadające doświadczenie w tym zakresie. Przykładowo w Finlandii, która pierwsze bloki atomowe wybudowała już w latach 70., ostatnia inwestycja tego typu opóźniona jest o 8 lat (trwa więc już 12 lat) i nie wiadomo kiedy zostanie zakończona. Znacznie przekroczony został także jej budżet (z 3 mld euro urósł do szacowanych obecnie 8,5 mld euro) [Koistinen 2016]. Relatywnie krótki okres budowy charakteryzuje jednostki OZE, które są preferowane z uwagi na ochronę klimatu. Jednak w porównaniu z innymi typami elektrowni charakteryzuje je niska efektywność z uwagi na nierówną pracę, która jest wynikiem uzależnienia od czynników przyrodniczych [*Finansowanie*… 2013]. Przykładowo w 2015 roku w Niemczech (a więc kraju, w którym udział źródeł odnawialnych jest największy) moc zainstalowana w OZE (na poziomie 90 tys. GW) była niewiele niższa od mocy ze źródeł konwencjonalnych (106 tys. GW). Jednak w produkcji energii elektrycznej istniała ponadtrzykrotna różnica między tymi źródłami – tradycyjne wyprodukowały 427 TWh energii elektrycznej, a odnawialne tylko 155 TWh [BfEGTPuE 2016]. OZE wymagają również większych inwestycji po stronie sieci (m.in. z uwagi na konieczność podłączenia rozproszonych źródeł oraz posiadania sieci o większej przepustowości).

Zaprezentowane powyżej dane dotyczące potencjału wytwórczego pokazują, że Polska w najbliższej dekadzie będzie miała problem z podażą energii elektrycznej, jeżeli nie zwiększy inwestycji w moce wytwórcze. Oznacza to, że bezpieczeństwo energetyczne kraju jest zagrożone. Może to wpłynąć negatywnie na rozwój gospodarczy, który jest silnie uzależniony od energii elektrycznej.

Wnioski

Analiza sytuacji w branży energii elektrycznej pokazuje, że klienci oczekują bezawaryjnych dostaw oraz powstrzymania wzrostu jej ceny [PwC, Bank Śląski 2015]. Dla

poprawy sytuacji systemu elektroenergetycznego należy do 2030 roku zainwestować co najmniej 200 mld zł [Rakowski i in. 2008]. Nie da się tego zrobić natychmiast, między innymi z uwagi na koszty i proces technologiczny. Wymaga to również takich zmian w prawie, które uregulowałyby m.in. proces ustanawiania służebności przesyłu oraz wprowadziły parametryczny system wynagrodzeń dla właścicieli nieruchomości, przez które przebiegają korytarze przemysłowe. Ponadto konieczna jest zmiana prawa budowlanego, uwarunkowań środowiskowych i usprawnienie procesów planistycznych.

Myśląc długookresowo o rozwoju gospodarczym kraju, należy zlikwidować najważniejsze bariery rozwoju tego sektora. Konieczne jest też szybkie opracowanie i konsekwentne wdrażanie strategii inwestycyjnej.

Bibliografia

Finansowanie czystej energii: rozwiązania dla Polski (2013), Cambridge Programme for Sustainability Leadership, Centre for Energy Policy Research, Uniwersytet Korwina w Budapeszcie.

Forum Energii (2017), *Polski sektor energetyczny 2050*, Warszawa.

Jankiewicz S., Grądzik P. (2017), *Renewable Energy Sources as a Barrier to the Eu's Common Energy Policy – on the Example of Poland and Germany*, UE we Wrocławiu, Wrocław.

Jankiewicz S. (2014), *Polityka energetyczna państwa a rozwój gospodarczy w Polsce,* [w:] M. Bucka, Z. Mikołajewicz (red.), *Procesy gospodarczego i społecznego rozwoju wobec wyzwań współczesnego świata*, Uniwersytet Opolski, Opole.

Jankiewicz, S. (2013), *Wpływ budowy elektrowni atomowej w Polsce na rynek energii elektrycznej*, [w:] K. Pająk, A. Ziomek, S. Zwierzchlewski (red.), *Ekonomia i zarządzanie energią a rozwój gospodarczy*, Adam Marszałek, Toruń.

Komisja Europejska, Dyrektywa 2005/89/WE Parlamentu Europejskiego i Rady z dnia 18 stycznia 2006 r. dotycząca działań na rzecz zagwarantowania bezpieczeństwa dostaw energii elektrycznej i inwestycji infrastrukturalnych, Dz. U. L 33 z 4 lutego 2006 r.

Ministerstwo Gospodarki (2014), *Bezpieczeństwo Energetyczne i Środowisko – perspektywa do 2020 r*., Warszawa.

Ministerstwo Gospodarki (2013), *Sprawozdanie z wyników monitorowania bezpieczeństwa dostaw energii elektrycznej za okres od dnia 1 stycznia 2011 roku do dnia 31 grudnia 2012 roku*, Warszawa.

Ministerstwo Gospodarki i Pracy (2004), *Doktryna zarządzania bezpieczeństwem energetycznym*, Warszawa.

Ministerstwo Gospodarki i Pracy (2005), Polityka energetyczna Polski do 2025 roku, Warszawa.

NIK (2013), *Funkcjonowanie i bezpieczeństwo elektroenergetycznych sieci przesyłowych*. Informacja o wynikach kontroli NIK, Warszawa.

PwC, Bank Śląski (2015), *Koniec tradycyjnej energetyki? Jak wygrać w dobie zmian*?, Warszawa.

Raport o wpływie uregulowań prawnych na warunki eksploatacji i rozwoju infrastruktury technicznej liniowej sektora paliwowo-energetycznego decydującej o bezpieczeństwie energetycznym kraju (2009), Operator Gazociągów Przesyłowych GAZ-SYSTEM S.A., Izba Gospodarcza Gazownictwa, Polskie Towarzystwo Przesyłu i Rozdziału Energii, PSE Operator S.A., Towarzystwo Rozwoju Infrastruktury ProLinea Izba Gospodarcza CIEPŁOWNICTWO POLSKIE, PERN „Przyjaźń" S.A.

Rozporządzanie Parlamentu Europejskiego i Rady nr 34/2013 z dnia 17 kwietnia 2013 r. w sprawie wytycznych dotyczących transeuropejskiej infrastruktury energetycznej, uchylającej decyzję nr 715/2006/WE oraz zmieniającej rozporządzenia WE nr 713/09, WE nr 714/09 i WE nr 715/09, Dz. U. L. 115 z 25 kwietnia 2013 r., ss. 39–75.

Rudźko R. (2012), *Analiza nt. wielkości strat w przesyle energii elektrycznej w Polsce*, BBN, Warszawa.

Stankowska A. (2009), *Realizacja elektroenergetycznych inwestycji liniowych – wyzwania i bariery inwestycyjne*, „Elektroenergetyka", nr 1.

Ustawa z dnia 10 kwietnia 1997 r. Prawo energetyczne, Dz. U. z 2006 r. Nr 89, poz. 625 z późn. zm.

Wersja skonsolidowana Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Dz. U. UE C 83 z 30 marca 2010 roku, art. 194.

Żmijewski K. (red.) (2014), *Program Gospodarki Niskoemisyjnej na terenach wiejskich*, Warszawa.

Żmijewski K., Sokołowski M. (2010), *Rozwój sieci energetycznych w Polsce w kontekście uregulowań pakietu klimatyczno-energetycznego*, „Acta Energetica", nr 3.

Bibliografia elektroniczna

Agencja Rynku Energii S.A., http://www.rynek-energii-elektrycznej.cire.pl/ st,33,335,tr,145, 0,0,0,0,0,budowane-i-planowane-elektrownie.html, dostęp: 10.04.2016.

Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, *EEG in Zahlen 2014* (2015), http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachg ebiete/Ener gie/Unternehmen_Institutionen/ErneuerbareEnergien/ZahlenDatenInformationen/ EEGinZahlen _2014_BF.pdf?__blob=publicationFile&v=4, dostęp: 28.01.2017.

Energy Roadmap 2050, EUROPEAN COMMISSION, Brussels 2011, http://ec.europa. eu/smart-regulation/impact/ia_carriedout/docs/ia_2011/sec_2011_1565_en. pdf, [10.04.2016].

International Electrotechnical Commission, http://www.electropedia.org/iev/iev.nsf/display? openform&ievref=617-01-05, dostęp: 10.09.2017.

Kleiber M., Steinhoff J., Żmijewski K., *Infrastruktura energetyczna – potrzebny plan Marshalla?*, SRNPRE, www.rada-npre.pl, dostęp: 20.04.2016.

Koistinen O., *Suomenkin uusi ydinvoimala maksaa 8,5 miljardia euroa*, http://www.hs.fi/ talous/a130 5627982885, dostęp: 20.04.2016.

50hertz, http://www.50hertz.com/de/50Hertz/Netzueberblick, dostęp: 20.01.2016.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **203–213**

Magdalena Karolak-Michalska[1]
Wydział Zarządzania i Nauk o Bezpieczeństwie
Społeczna Akademia Nauk

Polityka narodowościowa jako element kształtujący bezpieczeństwo państwa – casus współczesnej Ukrainy

National Policy as an Element Shaping the Security of the Country – a Casus of Modern Ukraine

Abstract: The aim of the article is to broaden the analysis regarding the correlation between the national policy and the security of independent Ukraine. In the first part of the article the author treats about the national policy of Ukraine, notice that the current regulations on the rights of national and ethnic minorities in Ukrainian legislation, including those concerning the Russian minority are not extensive or detailed, which translates into stability of state security. In further research, points out that national policy should correspond with the security policy of Ukraine, be equipped with mechanisms that will eliminate inter-ethnic tensions and emphasize the territorial integrity of the state. The Crimean annexation and the conflict in Donbas show that the situation in Ukraine, in which the Russian minority is involved, requires constant monitoring of state authorities. In the final remarks, the author recommends that the Ukrainian authorities take multi-path actions on the line "national policy-security of the state", oriented not only on normative regulations, but also on cultural activities to understand the cultural and identity differences of the Ukrainian and Russian populations. As a result, such practices are conducive to ensuring the stability of the internal security of the state and the territorial integrity of Ukraine.
Key words: nationality policy, ethnopolitics, security of Ukraine, the Russian minority, ethnicity, conflict in Donbas.

[1] magdalenakarolak-michalska@wp.pl

Wstęp

Obserwacja rzeczywistości społeczno-politycznej rodzi pytania o kondycję bezpieczeństwa państw Europy. Eksperci w szczególności koncentrują się nad obszarem Ukrainy, który na skutek aneksji Krymu i konfliktu w Donbasie jest przedmiotem licznych analiz. Badacze obok czynników politycznych, ekonomicznych, układu sił i strefy wpływów w środowisku międzynarodowym zwracają uwagę na czynnik etniczny, jako determinantę kształtującą bezpieczeństwo państwa wielonarodowego. Choć powstaje coraz więcej analiz w zakresie polityki narodowościowej Ukrainy i obszaru Wspólnoty Niepodległych Państw (WNP), to opracowania te nadal budzą pewien niedosyt badawczy. Brakuje badań ogniskujących się z jednej strony na bezpieczeństwie państwa, z drugiej na etnopolityce Ukrainy. W wspomnieć należy, że od momentu aneksji Krymu jesteśmy świadkami największego wyzwania w sferze bezpieczeństwa transatlantyckiego od zakończenia zimnej wojny, o którym nie sposób dyskutować bez uwzględnienia czynnika etnicznego i różnic narodowo-kulturalnych w społeczeństwie ukraińskim. Tematyka ta wymaga badań, gdyż „konflikt na Ukrainie może doprowadzić do zniszczenia tego, co z wysiłkiem udało się osiągnąć przez ostatnie ćwierćwiecze w ramach budowy struktur kooperatywnego bezpieczeństwa w Europie. Jego dalsza eskalacja może doprowadzić zarówno do nowego podziału kontynentu, jak i długotrwałej konfrontacji pomiędzy Unią Europejską, NATO i Federacją Rosyjską" [Panek 2015, s. 7]. Dodać należy, że Rosja wykorzystuje lokalne separatyzmy i zróżnicowanie etniczne do destabilizacji sytuacji politycznej w państwach powstałych po rozpadzie ZSRR (np. Gruzji). Ukraina jest kolejnym państwem, które zostało poddane rosyjskiej presji z wykorzystaniem konfliktów rozniecanych na tle etnicznym [Furier 2017, s. 19].

Celem niniejszego artykułu jest poszerzenie analiz dotyczących korelacji pomiędzy polityką narodowością a bezpieczeństwem współczesnej Ukrainy. Zakres tematyczny badań dotyczy przestrzeni terytorialno-czasowej jaką jest niepodległa Ukraina. Autorka dokonując badań niniejszej problematyki, stosuje interdyscyplinarne podejście badawcze, integrujące w sobie metody charakterystyczne dla nauk o polityce, stosunków międzynarodowych czy nauk o bezpieczeństwie.

Etnopolityka Ukrainy

Od początku lat 90. XX w. na Ukrainie panuje konsensus głównych sił politycznych, że powinna być ona postrzegana jako państwo „narodu tytularnego oraz mniejszości narodowych i etnicznych". Założenia te znalazły wyraz w ustawodawstwie ukraińskim.

Konstytucja z 1996 roku w art. 11 stwierdza, że „Państwo popiera konsolidację i rozwój narodu ukraińskiego, jego historyczną świadomość, tradycję i kulturę, a także rozwój etniczny, kulturowy, językowy i religijny tożsamości wszystkich rdzennych ludów i mniejszości narodowych Ukrainy" [*Konstituciâ Ukrainy* 1996]. Dalej, w artykule 53, czytamy: „Obywatelom należącym do mniejszości narodowych gwarantuje się prawo nauki w języku ojczystym lub nauki języka ojczystego w państwowych i komunalnych instytucjach nauczania albo w ośrodkach kultury narodowej" [*Konstituciâ Ukrainy* 1996]. Rzetelność naukowa nakazuje doprecyzować, że w polityce językowej Ukrainy zostały sformułowane dwa podejścia: ukraińskie i rosyjskie. Pierwsze zakłada realizację polityki dyskryminacji, która ma wzmacniać znaczenie języka ukraińskiego. Po drugiej stronie znajduje się ta część społeczeństwa, która uważa, że chociaż nie jest bezpośrednio dyskryminowana, to kroki podejmowane przez rząd w Kijowie negatywnie oddziałują na ludność rosyjskojęzyczną i łamią jej prawa [Szeptycki 2015, s. 14]. Dodać w tym miejscu należy, że osiągnięciem władz porewolucyjnej Ukrainy (po 2014 roku) jest fakt, że polityka językowa przestała być głównym przedmiotem sporów, co w przeszłości starała się wykorzystywać Rosja i prorosyjskie środowiska na Ukrainie. Wbrew oskarżeniom władz rosyjskich, zmiany polityczne na Ukrainie po obaleniu Wiktora Janukowycza nie przyniosły prześladowań ludności rosyjskojęzycznej.

Analiza ukraińskiej ustawy zasadniczej, a także aktów prawnych niższego rzędu, prowadzi do wniosku, że zawierają one podstawowe gwarancje w zakresie praw mniejszości narodowych i etnicznych, przy czym przynależność do mniejszości traktują jako sprawę indywidualnego wyboru każdego obywatela. Wśród praw przynależnych mniejszościom, w tym rosyjskiej, znajdują się: prawo do obywatelstwa, wolności myśli i słowa oraz wyrażania poglądów i przekonań; prawo udziału w wyborach (czynne i bierne), a także uczestnictwa we władzy; prawo do tworzenia partii politycznych, zakładania stowarzyszeń i organizacji społecznych, do akcji masowych; prawo używania języka ojczystego i wyboru języka komunikacji, wychowania i nauki; prawo do autonomii narodowo-kulturalnej, swobodnego rozwoju kultury; prawo dostępu do środków masowego przekazu, utworzenia środków komunikacji masowej, uruchomienia działalności wydawniczej, otrzymania, przechowywania i rozprzestrzeniania informacji w języku ojczystym; zakaz dyskryminacji narodowej i językowej; prawo wolności wyznawania religii bądź nie wyznawania żadnej; prawo do wyboru zawodu, do pracy, odpoczynku; prawo do mieszkania, odpowiednich warunków życia, a także ochrony praw ekonomicznych i socjalnych [*Zakon Ukrainy Pro nacional'ni*…1992; *Zakon Ukraini Progromadânstvo*…2001; *Zakon Ukrainy O partiâch*… 2001; Ustawa Podstawy prawne 1992; *Zakon Ukraini Protelebačennâ*… 1993; *Zakon Ukraini Prosvobodu*… 1991].

Szczególne miejsce w regulacji praw mniejszości rosyjskiej na Ukrainie zajmowała Konstytucja Autonomicznej Republiki Krymu (ARK). Władze Krymu miały prawo do samodzielności w kształtowaniu polityki społecznej i kulturalnej, eksploatacji zasobów naturalnych oraz stosunków gospodarczych z zagranicą. Polityka obronna, zagraniczna i monetarna pozostały w gestii władz Ukrainy. Zgodnie z artykułem 10 Konstytucji ARK język rosyjski – jako język większości – stał się językiem autonomii. Przepis ten wprowadzał zasadę rosyjsko-ukraińskiej dwujęzyczności na półwyspie, tym samym „wzmacniając" pozycję języka rosyjskiego na Ukrainie, ale tylko na obszarze Krymu. Ponadto mniejszość rosyjska uzyskała m.in. prawo do: reprezentacji w organach władzy ARK i zakładania organizacji politycznych; ochrony i rozwoju kultury, powoływania organizacji kulturalnych; tworzenia środków masowego przekazu, wydawnictw, muzeów, teatrów; publikowania aktów prawnych na terenie autonomii w języku rosyjskim [*Konstitucîâ Respubliki Krym*… 1998; *Konstitucîâ Ukrainy* 1996].

Prawa mniejszości narodowych na Ukrainie są również przedmiotem umów dwu- i wielostronnych o charakterze międzynarodowym. Uczestnictwo Ukrainy w organizacjach międzynarodowych oraz ratyfikacja umów zawierających klauzule mniejszościowe są istotne dla mniejszości narodowych – poszerzają bowiem katalog ich praw. W kontekście mniejszości rosyjskiej największego znaczenia nabrał Traktat o Przyjaźni, Dobrym Sąsiedztwie i Współpracy pomiędzy Ukrainą i Federacją Rosyjską, który określił indywidualne i zbiorowe prawa mniejszości ukraińskiej w Rosji i rosyjskiej na Ukrainie (art. 12). Strony zagwarantowały mniejszościom ochronę praw etnicznych, językowych, kulturalnych i wyznaniowych. Zobowiązały się zapewnić również możliwość nauki języka rosyjskiego na Ukrainie oraz ukraińskiego w Rosji [*Dogovor o družbe*… 1997]. Traktat ten stanowi „instrument" wspomagający prawa i wolności polityczne Rosjan, odnosząc się do problematyki ich uczestnictwa w życiu publicznym Ukrainy.

Mniejszościom narodowym i etnicznym na Ukrainie przysługują również prawa wynikające ze współpracy państw w wymiarze wielostronnym. W ramach członkostwa w ONZ władze ukraińskie podpisały szereg aktów, które zapewniają ochronę praw osób należących do mniejszości narodowych. Wraz z przynależnością Ukrainy do Organizacji Bezpieczeństwa i Współpracy w Europie, wiążącego charakteru dla państwa nabrał Dokument Spotkania Kopenhaskiego w Sprawie Ludzkiego Wymiaru KBWE z 29 czerwca 1990 roku. Na jego podstawie kwestie dotyczące mniejszości rozstrzygane są w demokratycznych strukturach politycznych opartych na praworządności[Dokument Spotkania1990]. Nadmienić należy, że choć dokumenty OBWE traktowane są jako tzw. *international human rights soft law*, oddziałują w systemie standardów ochrony osób należących do mniejszości narodowych siłą politycznego uznania jej państw-członków.

Ukraina ratyfikowała podstawowe akty prawne Rady Europy, a po uzyskaniu członkostwa zobowiązała się do dostosowania się do norm organizacji w zakresie praw człowieka. Konwencja Ramowa o Ochronie Mniejszości Narodowych (KROMN) z 1 lutego 1995 roku, poszerzyła zakres gwarancji mniejszości narodowych na Ukrainie. Ochrona praw i wolności mniejszości stała się integralną częścią międzynarodowej ochrony praw człowieka, przy zagwarantowaniu równości wobec prawa. Mniejszości narodowe otrzymały m.in. prawo do samokategoryzacji (art. 3). Konwencja zobowiązała Ukrainę do zagwarantowania warunków dla rzeczywistego udziału mniejszości narodowych w życiu kulturalnym, społecznym i ekonomicznym oraz w sprawach publicznych, przy zakazie ingerencji państwa w prawo mniejszości do uczestniczenia w działalności organizacji pozarządowych na szczeblu krajowym i międzynarodowym [*Konvenciâ pro zabezpečennìa*…1995].

W ramach współpracy z Radą Europy Ukraina ratyfikowała także Europejską Kartę Języków Regionalnych i Mniejszościowych. Zgodnie z jej treścią mniejszość rosyjska otrzymała gwarancję, że Ukraina w stosunku do języka rosyjskiego będzie opierać swoją politykę na uznaniu języka rosyjskiego za przejaw bogactwa kulturowego i respektować jego zasięg geograficzny. Ukraina zobowiązała się eliminować zróżnicowanie, wyłączenie, ograniczenie lub uprzywilejowanie dotyczące posługiwania się językiem rosyjskim, a także udostępnić najważniejsze teksty ustaw państwowych w języku rosyjskim [*Evropejska Hartìâ* 1992].

Wynikiem aktywności Ukrainy we Wspólnocie Niepodległych Państw jest m.in. Konwencja o Zagwarantowaniu Praw Osób Należących do Mniejszości Narodowych z 21 października 1994 roku, zgodnie z którą mniejszość narodowa zyskała gwarancję praw obywatelskich, politycznych, socjalnych, ekonomicznych, kulturalnych z międzynarodowymi standardami w dziedzinie praw człowieka [*Konvenciâ ob obespečenii*…1994].W ramach kooperacji państw WNP została także uchwalona Konwencja Państw WNP o Prawach i Podstawowych Wolnościach Człowieka z 26 maja 1995 roku. Państwa zaznaczyły w niej, że dążą do ochrony i przeciwdziałania naruszeniom praw człowieka i podstawowych wolności, tradycji tolerancji i przyjaźni narodów [*Konvenciâ Sodružestva*…1995].

W praktyce, jak wynika z obserwacji własnych i dostępnych badań z lat 1991–2017, mniejszości narodowe na Ukrainie korzystają z przyznanych im praw. Przykładowo Rosjanie piastują stanowiska w organach władzy ustawodawczej, wykonawczej i samorządowej, zakładają partie polityczne, stowarzyszenia i organizacje społeczne. Z kolei w sferze praw kulturalnych korzystają z prawa do używania języka rosyjskiego (np. w 2007 roku ilość książek i broszur wydrukowanych po rosyjsku wynosiła 4 639 (26,21% ogółu), po ukraińsku 11 825 (66,82%) [*Third Report Submitted*… 2009, s. 14–27]).

Wyzwaniem pozostaje pozycja języka rosyjskiego w mediach. Zgodnie z badaniami kampanii „Bojkot rosyjskiego kina" w 2014 roku 39,3% czasu antenowego w telewizji ukraińskiej wypełniały materiały w języku rosyjskim, 29% – w ukraińskim, a 23,5% – w rosyjskim z ukraińskimi napisami [Szeptycki 2017, s. 99].

Z obserwacji własnych przeprowadzonych podczas wyjazdów na Ukrainę w latach 2007–2014 wynika, że regulacje praw mniejszości narodowych i etnicznych w ustawodawstwie ukraińskim, w tym dotyczące mniejszości rosyjskiej, nie mają charakteru rozbudowanego, co przekłada się na kondycję i stabilność bezpieczeństwa wewnętrznego państwa. Wydarzenia na Krymie związane z aktywnością ludności rosyjskiej(w 2001 roku stanowili 58,5% mieszkańców półwyspu) w 2014 roku i jej zaangażowania w referendum przyłączenia półwyspu do Rosji wskazują, że mimo przyznanych ustawowo praw, Rosjanie podjęli działania na rzecz ich poszerzenia, mając przy tym często przeświadczenie, że są dyskryminowani. Sytuacja ta wskazuje na wpływ polityki narodowościowej na poziom bezpieczeństwa obywateli, a także zależność na linii etnopolityka – bezpieczeństwo państwa w kontekście integralności terytorialnej. Ciekawymi w powyższym kontekście wydają się być badania z lat 1997–2005, z których wynika, że w 1997 roku 56% Rosjan na Ukrainie uważało Rosjan i Ukraińców za jeden naród, w 2002 roku myślało tak 76%, a w 2004 roku było ich nawet 79%. Z kolei w 2005 roku 61% Rosjan pozytywnie oceniało ponowne zjednoczenie Ukrainy i Rosji w ramach jednego państwa [Panek 2015, s. 19]. Późniejsze badania z 2008 roku wykazały, że Rosjanie mieszkający w ARK identyfikowali się całkowicie z językiem rosyjskim, w większości z rosyjską tradycją kulturową (69,9%), a w mniejszej części z radziecką tradycją kulturową (15%). Tylko 34,4%uznawało Ukrainę za ojczyznę, 22,4% uważało się za patriotów Ukrainy, a 47,3% było gotowe zamienić obywatelstwo ukraińskie na rosyjskie. Połączenie Krymu z Rosją popierało 75,9% Rosjan krymscy, jednocześnie wykazując negatywny stosunek do NATO i UE [Skrukwa 2017, ss. 216–217].

Śledząc rozwój polityki etnicznej Ukrainy, odnotować należy, że prezydent Leonid Krawczuk wspierał wypracowanie narodowej histeriografii; rosyjska i radziecka polityka wobec Ukrainy były prezentowane przez władze w negatywnym świetle, a ukraińska świadomość narodowa miała się rozwijać w opozycji do Rosji. Prezydent prowadził działania na rzecz wzmocnienia pozycji języka ukraińskiego i ustanowienia narodowego Kościoła prawosławnego. Oba te czynniki były postrzegane jako ważny element polityki budowania narodu. Przy tym Krawczuk opowiadał się bardziej za narodem politycznym, obywatelskim niż etnicznym, co pozwoliłoby uniknąć wykluczenia mniejszości narodowych. Z kolei Leonid Kuczma reprezentował podobne podejście, ale zrezygnował z retoryki antyrosyjskiej i uznał, że budowa narodu będzie procesem długotrwałym. Takie stanowisko było wynikiem troski o relacje z Rosją, a także wizji

państwa charakterystycznej dla poradzieckiej nomenklatury na Ukrainie [Szeptycki 2015, s. 283].

Stosunki międzyetniczne na Ukrainie mogły potencjalnie ulec zmianie po pomarańczowej rewolucji. Sytuacja taka wynikała po pierwsze z faktu, że środowiska mniejszości rosyjskiej w większości nie popierały Wiktora Juszczenki, po drugie, prezydent podjął działania na rzecz wzmocnienia świadomości narodowej –za pomocą polityki historycznej. W praktyce w latach 2005–2010 nie doszło do poważniejszych napięć na tle narodowościowym. Ważnym jest jednak to, że polityka Juszczenki pogłębiła stereotypy myślowe i nasiliła rozłam w społeczeństwie na prorosyjski wschód i proeuropejski zachód. W znacznym stopniu do podziału przyczyniły się media i partie polityczne, które spekulowały na temat problemów dzielących obywateli Ukrainy [Voytyuk 2017, s. 266].

Znaczących zmian w kontekście polityki narodowościowej nie przyniosło również dojście do władzy Wiktora Janukowycza, który zrezygnował z retoryki poprzednika. Doprecyzować należy, że w okresie niepodległości ukraińskiej, do momentu konfliktu w Donbasie, udało się uniknąć przemocy fizycznej w rozwiązywaniu konfliktów o podłożu etnicznym. Jednak brak zgody społecznej dotyczącej pamięci narodowej i kwestii językowych przyczyniał się coraz częściej do podziału niż ukształtowania trwałej stabilizacji wewnętrznej państwa charakteryzującego się dużą różnorodnością. Wraz z odejściem od władzy Janukowycza, aneksją krymską i konfliktem w Donbasie, w którym czynnik etniczny (w 2001 roku Rosjanie stanowili 38% mieszkańców obwodu donieckiego i 39% obwodu ługańskiego [*Nacional'nyj…* 2001]) stanowi jeden z kluczowych elementów eskalujących napięcie i ukazujący słabość etnopolityki, pojawiła się konieczność wypracowania nowego podejścia do polityki narodowościowej Ukrainy. Powinna ona korespondować z polityką bezpieczeństwa, być zaopatrzona w mechanizmy, które będą niwelować napięcia międzyetniczne i kłaść nacisk na zapewnienie integralności terytorialnej państwa.

Prawa mniejszości narodowych na Ukrainie z jednej strony są prawami wszystkich obywateli, z drugiej – w ustawodawstwie ukraińskim występują prawa skierowane na ochronę mniejszości narodowych, w szczególności rosyjskiej. Od początku lat 90. XX wieku ochrona mniejszości w Europie Wschodniej uległa poprawie. Pomimo to nadal występują zagrożenia bezpieczeństwa dla i ze strony mniejszości narodowych. Ich grupę tworzy m.in. wadliwość części decyzji administracji rządowej i samorządowej dotycząca spraw konkretnych obywateli oraz istnienie ksenofobii powodującej wyobcowanie wśród członków mniejszości narodowych.

Polityka narodowościowa, a bezpieczeństwo

Ukraina przez wielu jest uważana za państwo znajdujące się w procesie budowy tożsamości narodowej, postkolonialne lub cywilizacyjnie podzielone. Uzyskanie politycznej niezależności nie było tożsame z przeprowadzeniem reform politycznych i gospodarczych, nie dokonano również faktycznych zmian w kręgach elit władzy [Panek 2015, s. 13; Szeptycki 2015, ss. 283–284], nie nastąpiło więc wypracowanie rozwiązań dotyczących polityki narodowościowej w kontekście bezpieczeństwa terytorialnego państwa. Po proklamowaniu niepodległości Ukraina zaniechała działań skierowanych na wzmocnienie bezpieczeństwa państwa. Przyczyną tego było m.in. przekonanie, że bytowi państwa nic nie zagraża ze strony byłych republik radzieckich [Voytyuk 2017, s. 264].

Brak dostosowanej do realiów ukraińskich koncepcji polityki narodowościowej – jak pokazują wydarzenia na Krymie i konflikt w Donbasie – zaburza stabilizację państwa, bowiem bezpieczeństwo wewnętrzne „zazębia się" z zewnętrznym. Na Ukrainie owym „spoiwem, zazębieniem" jest m.in. mniejszość rosyjska. Z jednej strony jest ona niezadowolona ze statusu prawno-politycznego i uczestniczy w konflikcie wewnętrznym w państwie, wysuwając roszczenia federalizacji Ukrainy, z drugiej zaś stanowi oficjalną przyczynę aneksji krymskiej. Tym samym bezpieczeństwo państwa wymaga rozważenia w kontekście powiązania zachodzących zjawisk, zdarzeń i procesów, w tym także etnopolitycznych.

Mało efektywna polityka narodowościowa władz ukraińskich, spekulacje na temat kwestii językowych i różnic regionalnych spowodowały wzrost prorosyjskich nastrojów w regionie wschodniej Ukrainy. Przy tym zróżnicowanie etniczne Donbasu nie było jedyną przyczyną formowania się tam tendencji separatystycznych. Kluczowy wpływ na kształtowanie świadomości etnicznej, kulturowej, językowej oraz tożsamości mieszkańców Donabsu miała radziecka, a później rosyjska propaganda oraz słabe zaangażowanie w problemy regionu władz ukraińskich. Dodatkowo rosyjskie media przez 25 lat wpływały na opinię publiczną w Donbasie zaś władze ukraińskie zupełnie to lekceważyły tego znaczenie. Brak odpowiedniej polityki narodowościowej Ukrainy i należytej uwagi dla problemów regionu stały się ważnymi przyczynami wybuchu działań wojennych w Donbasie [Voytyuk 2017, ss. 264–265].

Z badań wynika, że zgrupowania separatystów są sukcesywnie powiększane, głównie przez Rosjan, Czeczenów czy Osetejczyków. Istotnym jest, że to etniczni Rosjanie (samozwańczy premierzy – Aleksandr Borodaj i Marat Baszarow) nieakceptujący pozycji prawno-politycznej ludności rosyjskiej na Ukrainie, zajmują kluczowe stanowiska w politycznych i wojskowych strukturach dowodzenia samozwańczych republik

(Donieckiej i Ługańskiej) [Panek 2015, s. 49; Otłowski 2014]. Do końca 2016 roku w konflikcie donbaskim zginęło ok. 10 tys. osób [Szeptycki 2017, ss. 89–92], a sam konflikt jest uznany przez 52% ankietowanych za jeden z najważniejszych problemów Ukrainy [*Public Opinion…* 2016]. W świetle badań z 2016 roku 63% obywateli Ukrainy uważa, że toczy się wojna rosyjsko-ukraińska, a 65% sądzi, że na Ukrainie obecne są wojska rosyjskie [Shpiker 2017]. Nie ulega wątpliwości, że utrata kontroli nad Donbasem przez władze ukraińskie – m.in. na skutek nieudolnej i nie będącej odpowiedzią na potrzeby lokalnej ludności polityki narodowościowej przez władze państwowe – zachęciła do działania prorosyjskich separatystów.

Dążenie do stanu bezpieczeństwa na Ukrainie polega, w najprostszym ujęciu, na likwidacji lub minimalizacji zagrożeń, w tym tych związanych z procesami etnopolitycznymi. Nie wszystkie zagrożenia można jednak zlikwidować, tak więc zapewnienie bezpieczeństwa oznacza ograniczenie podatności państwa na występujące lub potencjalne zagrożenia, które mogą ograniczyć swobodę rozwoju państwa [Poseł-Częścik 2003, s.178]. Ważne jest zatem racjonalne i kompleksowe podejście do problemu bezpieczeństwa jako sumy wysiłków i ich skutków podejmowanych w ramach polityk szczegółowych, w tym narodowościowej, które są prowadzone przez właściwych ministrów i w konsekwencji sprzyjają kreacji warunków bezpieczeństwa bytu, rozwoju, wzmacniają obronność. Jeśli jednak polityki te są prowadzone w sposób niewłaściwy obracają się przeciwko tym wartościom, a co za tym idzie osłabiają państwo, m.in. poprzez brak przezorności i wprowadzenia odpowiednich mechanizmów wobec wybuchu ewentualnych konfliktów etnicznych.

Zakończenie

Polityka bezpieczeństwa Ukrainy w sposób szczególny powinna uwzględniać sytuację etniczną państwa, a także zwracać uwagę na kondycję etnopolityki. W powyższym kontekście dotychczasowe zmiany w systemie bezpieczeństwa Ukrainy można oceniać jako niewystarczające, przebiegające w sposób przypadkowy i podporządkowany celom politycznym partii walczących o władzę. Wprowadzający zmiany (władza ustawodawcza i wykonawcza) nie dokonują zmian fundamentalnych, uznając realizowane reformy sił zbrojnych czy służb specjalnych za wystarczające i pomijają wprowadzenie istotnych modyfikacji w realizacji polityki narodowościowej.

Obserwując współczesne, po 1991 roku, zarządzanie bezpieczeństwem państwa ukraińskiego w ramach transformacji polityczno-gospodarczej, można je traktować jako podejmowane w odpowiedzi na pojawiające się potrzeby. Nie należy przez dłuższy czas poddawać tego obszaru działań państwa krótkofalowym zmianom, nie

uwzględniając specyfiki etnicznej państwa, głównie mniejszości rosyjskiej, która od momentu uzyskania niepodległości przez Ukrainę wykazuje dążenia do poszerzenia swoich praw i uznania lokalnych Rosjan za drugi naród tytularny w państwie. Dotychczasowe działania władz ukraińskich naruszają bezpieczeństwo wewnętrzne i zewnętrzne państwa również w kontekście przeciwdziałania konfliktom etnicznym.

W ustawodawstwie ukraińskim nie ma inflacji prawa dotyczącego mniejszości narodowych i etnicznych. Nie występuje również zbytnia szczegółowość przepisów prawnych traktujących na ten temat. Tym samym na Ukrainie istnieje potrzeba podjęcia działań legislacyjnych odnoszących się do respektowania praw mniejszości narodowych, w tym związanych ze statusem języka rosyjskiego. Polityka narodowościowa władz Ukrainy powinna skoncentrować się na porozumieniu międzyetnicznym i zapobieganiu konfliktom etnicznym na terytorium kraju, a także na zagwarantowaniu harmonijnego rozwoju stosunków między narodem tytularnym i mniejszościami. Ponadto działania władz powinny skoncentrować się na demokratyzacji i poprawie warunków życia, a także aktywizacji wszystkich grup w budowę społeczeństwa obywatelskiego oraz zagwarantowania ochrony tożsamości etniczno-kulturowej mieszkańców Ukrainy. Można zaryzykować stwierdzenie, że dla wzmocnienia bezpieczeństwa wewnętrznego ukraińska polityka narodowościowa powinna skupić się na dążeniu państwa do stworzenia odpowiednich mechanizmów i instytucji, zapobiegających tendencjom etnokratycznym ze strony większości i nadmiernej polityzacji etniczności mniejszości. Zaistniała sytuacja na Ukrainie, w którą zaangażowana i uwikłana jest mniejszość rosyjska wymaga zespolenia działań w obszarze polityki narodowościowej i bezpieczeństwa, a także stałego monitoringu sytuacji.

Bibliografia

Dogovor o družbe, sotrudničestve i partnerstve meždu Rossijskoj Federaciej i Ukrainoj ot 31.05.1997 g (1997), [online], www.kremlin.ru, dostęp: 12.05.2017.

Dokument Spotkania Kopenhaskiego w Sprawie Ludzkiego Wymiaru KBWE z 29.06.1990 roku (1990), [online], www.biuro.sejm.gov.pl/teksty, dostęp: 14.05.2017.

Evropejska Hartìâ Rehional'nih Mov abo Menšin vìd 5.11.1992 r. (1992), [online], www.rada.gov.ua, dostęp: 14.11.2017.

Furier A. (2017), *Transformacja polityczna wschodnich sąsiadów Polski a ukraińska niepodległość – polska perspektywa badań,* [w:] A. Furier (red.), *Ukraina. Czas przemian po rewolucji godności*, Fundacja na Rzecz Czystej Energii, Poznań.

Konstituciâ Respubliki Krym ot 21 noâbrâ 1998 goda (1998), [online], www.portal.rada.gov.ua, dostęp: 14 listopada 2017.

Konstituciâ Ukrainy (1996), Kiev.

Konvenciâ ob obespečenii prav lic prinadležaûŝih k nacional'nym men'šistvam ot 21.10.1994 g (1994), [online], www.cis.minsk.by dostęp: 19.05.2017.

Konvenciâ pro zabezpečennìa prav osib, ŝčo naležat' do nacìonal'nih menšin vìd 1.02.1995 r (1995), [online], www.rada.gov.ua, dostęp: 17.05.2017.

Konvenciâ Sodružestva Nezavisimih Gosudarstv o pravah i osnovyh svobodah čeloveka ot26.05.1995 g (1995), [online], www.cis.minsk.by, dostęp: 12.05.2017.

Nacional'nyj Sostav Ukrainy (2001), [online], www.ukrcesnsus.gov.ua, dostęp: 17.01.2016.

Otłowski T. (2014), *Ukraina-Rosja – konfliktu ciąg dalszy*, Policy Paper nr 8, FAE, Warszawa.

Panek B. (2015), *Polityka Federacji Rosyjskiej w regionie Europy, Azji i Pacyfiku*, Difin, Warszawa.

Poseł-Częścik E. (2003), *Kryteria bezpieczeństwa państwa,* [w:] S. Dębski, B. Górka-Winter (red.), *Kryteria bezpieczeństwa międzynarodowego państwa,* PISM, Warszawa.

Public Opinion Survey Residents of Ukraine (2016), 28 maja – 14 czerwca, [online], www.iri.org, dostęp: 20.11.2017.

Shpiker M. (2017), *Is there a war going on between Russia and Ukraine?,* 15 marca, [online],www.kiis.com.ua, dostęp: 16.11.2017.

Skrukwa G. (2017), *Krym w niepodległej Ukrainie: ojczyzna Tatarów krymskich i obiekt rosyjskich aspiracji,* [w:] Furier A. (red.), *Ukraina. Czas przemian po rewolucji godności*, Fundacja na Rzecz Czystej Energii Poznań.

Szeptycki A. (2015), *Ukraina wobec Rosji. Studium zależności*, Warszawa.

Szeptycki A. (2017), *Ukraina wobec Rosji: trudna droga ku niezależności,* [w:] A. Furier (red.), *Ukraina. Czas przemian po rewolucji godności*, Fundacja na Rzecz Czystej Energii, Poznań.

Third Report Submitted by Ukraine Pursuant to Article 25, *Paragraph 1 of the Framework Convention For the Protection of National Minorities* (2009), Rada Europy, Strasburg.

Ustawa Podstawy prawne Ukrainy w sprawach kultury z 14 lutego 1992 roku (1992), [online], www.portal.rada.gov.ua, dostęp: 14.11.2017.

Voytyuk O. (2017), *Kilka uwag na temat świadomości narodowej mieszkańców Donbasu,* [w:] A. Furier (red.), *Ukraina. Czas przemian po rewolucji godności*, Fundacja na Rzecz Czystej Energii, Poznań.

Zakon Ukrainy Pro nacional'ni menšini v Ukraini vid 25.06.1992 r. (1992), [online], www.portal.rada.gov.ua, dostęp: 14.11.2017.

Zakon Ukraini Pro gromadânstvo Ukraini 18.01.2001 r. (2001), [online], www.portal.rada.gov.ua, dostęp: 14.11.2017.

Zakon Ukrainy O partiâch Ukraini vid 5.04.2001 r. (2001), [online], www.portal.rada.gov.ua, dostęp: 14.11.2017.

Zakon Ukraini Pro telebačennâ i radiomovlennâ vid 21.12.1993 r. (1993), [online], www.portal.rada.gov.ua, dostęp: 14.11.2017.

Zakon Ukraini Pro svobodu sovistita religijni organizacii vid 23.04.1991 r. (1991), [online], www.portal.rada.gov.ua, dostęp: 14.11.2017.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **215–226**

Tomasz Szubrycht[1]
Akademia Marynarki Wojennej

Wybrane problemy zaangażowania polskich okrętów w działania stałych zespołów okrętów (część I)

Selected Problems of Polish Ship's Engagement in the Activities of Standing Maritime Groups (Part I)

Abstract: The first part of the paper concerns the involvement of Polish Navy ships in the Standing NATO Maritime Group presents the areas of possible activity of Polish Navy. Based on conceptual modernization programs presented in the article, the group of navy vessels has been dedicated to Standing NATO Maritime Groups participation.
Key words: Standing NATO Maritime Group, Polish Navy, Allied actions on the seas
Maritime potential of the Navy.

Wstęp

Podejmując problematykę oceny poziomu zaangażowania państwa nadmorskiego w działalność operacyjną realizowaną w ramach stałych zespołów NATO, należy pamiętać, że aktywność marynarki wojennej dowolnego państwa obejmuje zarówno działania o charakterze narodowym, jak i międzynarodowym. Do działań międzynarodowych zaliczyć należy m.in.: ćwiczenia, działalność szkoleniową, codzienną działalność operacyjną oraz dyplomację morską. Za główne determinanty kształtujące proporcje między działaniami narodowymi i międzynarodowymi należy uznać: decyzje polityczne dotyczące poziomu zaangażowania w działania międzynarodowe, potencjał ilościowo-jakościowy marynarki wojennej państwa oraz koszty związane

[1] t.szubrycht@amw.gdynia.pl

z udziałem w przedsięwzięciach o charakterze międzynarodowym (działania w ramach stałych zespołów NATO, udział w ćwiczeniach międzynarodowych oraz operacjach sojuszniczych i międzynarodowych). Warto zatem znaleźć odpowiedź na pytanie, jaki powinien być maksymalny, optymalny i minimalny poziom zaangażowania Marynarki Wojennej RP w działania w ramach stałych zespołów NATO.

Wewnętrzne i zewnętrzne uwarunkowania zaangażowania polskich okrętów w działaniach stałych zespołów

Wydaje się, iż nie trzeba nikogo przekonywać, że Polska nie tylko powinna, lecz wręcz musi uczestniczyć we wspólnym wysiłku sił morskich państw Sojuszu. Zaangażowanie to powinno mieć charakter wieloaspektowy i obejmować m.in.: udział w operacjach i ćwiczeniach sojuszniczych, wydzielanie okrętów do stałych zespołów, delegowanie oficerów do struktur sojuszniczych, wymianę oficerów, współpracę szkoleniową i naukowo-badawczą oraz dyplomację morską. Ze względu na podjętą w niniejszej publikacji problematykę w dalszych analizach skupiono się tylko na jednym, wybranym aspekcie zaangażowania sojuszniczego, a mianowicie na problematyce wydzielania okrętów do stałych zespołów okrętów NATO.

Należy pamiętać, że decyzje dotyczące poziomu zaangażowania polskiej marynarki wojennej w szeroko pojmowany wysiłek operacyjny sił morskich państw Sojuszu są podejmowane na szczeblu politycznym. Rolą przedstawicieli marynarki wojennej jest zaproponowanie wariantów i różnego poziomu tego zaangażowania. Warianty te powinny uwzględniać: aktualne możliwości Marynarki Wojennej RP (np. liczbę okrętów, które można wydzielić do działań w ramach stałych zespołów), prognozowane możliwości zwiększenia lub zmniejszenia dotychczasowego zaangażowania oraz oszacowanie potencjalnych kosztów działalności okrętów w stałych zespołach NATO. Co więcej, należy jednocześnie pamiętać, że poziom zaangażowania marynarki wojennej musi wynikać z przyjętej dla całych Sił Zbrojnych RP strategii zaangażowania w działania podejmowane w ramach Sojuszu Północnoatlantyckiego.

Na wstępie podjętych rozważań celowe wydaje się również przypomnienie, że w opublikowanej w lutym 2017 *Strategicznej koncepcji bezpieczeństwa morskiego Rzeczypospolitej Polskiej* uwzględnione zostały dwa bardzo istotne aspekty, a mianowicie: akweny o żywotnym znaczeniu dla Polski oraz obszary potencjalnych działań Marynarki Wojennej RP[2]. W dokumencie tym za akweny o żywotnym znaczeniu dla Polski uznano:

[2] Rejony potencjalnych działań MW RP (*primary deployment area*) to akweny morskie, na których, ze względu na: żywotne interesy państwa, zobowiązania sojusznicze lub koalicyjne oraz aspiracje (polityczne, militarne lub gospodarcze) państwa, występuje największe prawdopodobieństwo działań sił morskich. Zob. *Strategiczna koncepcja bezpieczeństwa morskiego Rzeczypospolitej Polskiej* 2017, s. 76.

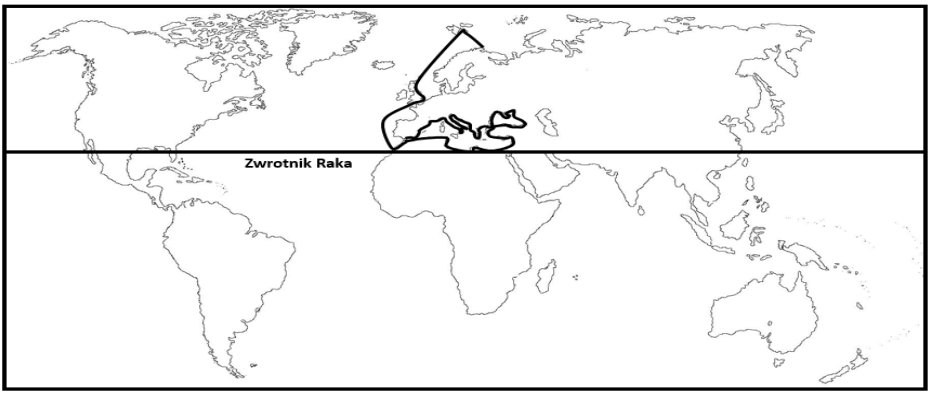
- Morze Bałtyckie wraz z Cieśninami Bałtyckimi,
- Morza Północne,
- Morze Norweskie,
- Morze Śródziemne z przylegającymi do tego akwenu obszarami atlantyckimi,
- Morze Czarne,
- wody wokół Arktyki.

W *Strategicznej koncepcji bezpieczeństwa morskiego Rzeczypospolitej Polskiej* zawarte zostało ponadto stwierdzenie odnoszące się do akwenów o żywotnym znaczeniu dla państwa „[…] Są to akweny, gdzie realizowana jest największa część polskich interesów morskich, zarówno w przestrzeni polityczno-militarnej, gospodarczej, jak i społeczno-kulturowej. W rejonach tych, szczególnie na akwenach morskich podległych polskiej jurysdykcji, SM RP winny prowadzić systematyczne działania narodowe, sojusznicze i koalicyjne, zwiększające bezpieczeństwo. Powinny one aktywnie uczestniczyć w inicjatywach NATO, UE lub regionalnych koalicji międzynarodowych, realizowanych na europejskich obszarach morskich szczególnie narażonych na występowanie stałych lub czasowych zagrożeń dla pokoju i porządku prawnego. Wspólne działania na rzecz ochrony morskiej granicy państw UE i NATO powinny być prowadzone w sposób ciągły. Dodatkowo, SM RP powinny wspierać polskie instytucje naukowo-badawcze, szczególnie te realizujące projekty na obszarze arktycznym i antarktycznym. Dzięki nim nauka polska ma możliwość promowania się na zewnątrz, co wiąże się ze wzrostem pozycji Polski na arenie międzynarodowej i może przynieść wymierne korzyści gospodarcze (np. dostęp do surowców). MW RP powinna brać udział w przedsięwzięciach państw NATO i UE zabezpieczających wspólne strategiczne interesy bezpieczeństwa morskiego, prowadzonych na wodach pozaeuropejskich (w tym tzw. *out-of-area operations*), na tamtejszych akwenach o żywotnym znaczeniu dla Polski" [*Strategiczna koncepcja*… 2017, s. 16].

Za rejony potencjalnych działań Marynarki Wojennej RP uznano natomiast akweny morskie położone na północ od Zwrotnika Raka (wynika to bezpośrednio z zapisów art. 6 Traktatu Północnoatlantyckiego). Nie oznacza to jednak, że polskie okręty nie będą prowadziły działań na innych akwenach, co wynika m.in. z przyjętej definicji rejonów potencjalnych działań.

Poniżej na rys. 1 przedstawione zostały akweny o żywotnym znaczeniu dla Polski oraz rejony potencjalnych działań polskiej marynarki wojennej.

Rysunek 1. Akweny o żywotnym znaczeniu dla Polski oraz rejony potencjalnych działań MW RP



Źródło: opracowanie własne.

Jak zatem można zauważyć, akweny o żywotnym znaczeniu dla Polski oraz rejony potencjalnych działań MW RP w znacznym stopniu pokrywają się z akwenami, na których działania prowadzą stałe zespoły okrętów NATO[3].

Przed stałymi zespołami okrętów Sojuszu, tak w przeszłości, jak i współcześnie, stawiano zadania wynikające m.in. z potencjału, charakteru oraz specyfiki sił morskich. Do zadań tych należy zaliczyć:

- zapewnienie stałej morskiej obecności na akwenach o żywotnym znaczeniu dla Sojuszu; poprzez prezentację bandery w ramach jednolitych zespołów okrętów demonstrowana jest solidarność sojusznicza;
- zapewnienie NATO-wskiego *force in being*[4] [Szubrycht 2008], sił zdolnych do natychmiastowego reagowania w sytuacjach kryzysowych, w przypadku wystąpienia różnych napięć w stosunkach międzynarodowych lub ograniczonej agresji;

[3] Zespół SNMG1 w latach zimnej wojny prowadził działalność operacyjną wzdłuż północno-zachodnich wybrzeży Europy z zadaniem obrony akwenów Północnego Atlantyku. Akweny, na których w czasie zimnej wojny działania prowadził zespół SNMG2, obejmowały Morze Śródziemne i inne akweny oblewające południową flankę Sojuszu. Po zakończeniu zimnej wojny akweny potencjalnych działań zespołu SNMG1 i SNMG2 zostały znacznie rozszerzone. Zespół SNMCMG1 operuje głównie na wodach Europy Północnej (Morzu Północnym, Cieśninach Bałtyckich, Morzu Bałtyckim i na wodach kanału La Manche), natomiast stały zespół przeciwminowy SNMCMG2 na wodach oblewających Europę Południową.

[4] *Force in being* – koncepcja opierająca się na założeniu, że sam fakt istnienia sił morskich państwa (państw) krępuje, a w pewnych okolicznościach nawet paraliżuje, operacje silniejszego przeciwnika, przez stałe zagrożenie możliwością stoczenia bitwy morskiej w sprzyjających dla niej warunkach. Pojęcia tego użył po raz pierwszy, podczas wojny z Francją, w 1690 roku, angielski admirał A. Herbert. W tym okresie Francja posiadała silniejszą flotę niż Brytyjczycy, dlatego też Anglia przyjęła strategię zachowawczą, polegającą na utrzymaniu w nienaruszonym stanie własnych sił morskich poprzez unikanie rozstrzygającej bitwy

– utrzymanie zdolności do tworzenia większych i bardziej licznych zespołów okrętów, jeśli zaistnieje taka konieczność;
– systematyczne wnoszenie wkładu w zwiększenie NATO-wskich zdolności bojowych, poprzez intensywny udział w wielonarodowych ćwiczeniach i codziennej działalności operacyjnej na morzu.

Przystępując do opracowywania różnych wariantów poziomu polskiego zaangażowania w działania w ramach stałych zespołów okrętów, warto mieć na uwadze następujące słowa J. Ginsberta „[…] nie wygrywa się wojny na morzu cudzymi rękoma! Słaby sprzymierzeniec, którego tylko bronić trzeba, a który nic z siebie dać nie potrafi, jest zawsze sprzymierzeńcem uciążliwym, którego broni się niechętnie, a od którego w zamian za pomoc żąda się pewnych, nieraz dotkliwych świadczeń – jeśli w ogóle występuje się w jego obronie" [Ginsbert 1938, s. 142]. Albo też inne, wygłoszone na uroczystości zaprzysiężenia prezydenta USA Johna Fitzgeralda Kennedy'ego. Po modyfikacji mogą mieć następujące brzmienie: „nie pytaj, co NATO może zrobić dla ciebie, ale co Ty możesz zrobić dla NATO".

Rozważania odnoszące się do poziomu zaangażowania polskich okrętów w działania stałych zespołów należy rozpocząć od poszukania odpowiedzi na pytanie, które z polskich okrętów mogą efektywnie realizować zadania w ramach stałych zespołów okrętów Sojuszu.

W roku 2017 polska marynarka wojenna dysponowała 6 okrętami, które mogą realizować zadania w składzie stałych zespołów okrętów. Są to: dwie fregaty rakietowe typu Oliver Hazard Perry, trzy niszczyciele min projektu 206FM oraz okręt dowodzenia ORP Kontradmirał Ksawery Czernicki. Okręty te zostały wybudowane lub zmodernizowane wiele lat temu. Niszczyciele min projektu 206FM pochodzą z połowy lat 60. ubiegłego wieku, a od ich gruntownej przebudowy i modernizacji minęło 17 lat. Fregaty rakietowe t. Oliver Hazard Perry rozpoczęły służbę w US Navy na początku lat 80. ubiegłego wieku. Najmłodszym okrętem jest okręt dowodzenia ORP Kontradmirał Ksawery Czernicki, który wszedł do służby w Marynarce Wojennej RP w roku 2001.

Należy podkreślić, że zgodnie z zaprezentowaną w marcu 2012 *Koncepcją Rozwoju Marynarki Wojennej* oraz zaproponowanym harmonogramem modernizacji technicznej, który nadal formalnie obowiązuje, obecnie eksploatowane niszczyciele min wycofane zostaną z linii w roku 2019, natomiast fregaty rakietowe t. Oliver Hazard Perry planowano wycofać z linii w roku 2016 [*Koncepcja rozwoju MW* 2012]. Realizacja zaplanowanych działań sprawiłaby, że w roku 2019 Marynarka Wojenna RP dysponowałaby tylko dwoma okrętami, które mogłyby zostać wydzielone do składu stałych ze-

morskiej z flotą francuską. Na tej koncepcji opierała się również niemiecka doktryna Hochseeflotte w czasie I wojny światowej.

społów (okręt dowodzenia ORP Kontradmirał Ksawery Czernicki oraz budowany niszczyciel min Kormoran II). Tym samym w najbardziej pesymistycznym wariancie nasze możliwości w ujęciu ilościowym byłyby mniejsze niż państw bałtyckich (Estonii, Litwy czy Łotwy).

W tabeli 1 przedstawiono zdolności Marynarki Wojennej RP do wydzielania okrętów do stałych zespołów w latach 2016–2026 (dane opracowane na podstawie ogłoszonej w marcu 2012 przez Sztab Generalny *Koncepcji rozwoju Marynarki Wojennej*).

Tabela 1. Prognoza potencjału okrętowego Marynarki Wojennej RP zdolnego realizować zadania w ramach stałych zespołów okrętów [wg *Koncepcji rozwoju Marynarki Wojennej*]

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026
	SNMG										
fregata t. OHP	2	0	0	0	0	0	0	0	0	0	0
okręt obrony wybrzeża	0	0	0	1	1	1	2	2	2	3	3
fregata Kaszub	1	1	0	0	0	0	0	0	0	0	0
	SNMCMG										
niszczyciel min pr. 206FM	3	3	3	3	0	0	0	0	0	0	0
okręt patrolowy Czapla	0	1	1	1	1	2	2	2	2	3	3
niszczyciel min Kormoran II	0	1	1	1	1	2	2	2	3	3	3
ORP Ksawery Czernicki	1	1	1	1	1	1	1	1	1	1	1
Razem	7	7	6	7	4	6	7	5	8	10	10

Źródło: opracowanie własne na podstawie [http://mw.mil.pl/zasoby/archiwum/upload/koncepcja_MW.pdf].

Jednak już w sierpniu 2013 roku zaprezentowana w marcu 2012 *Koncepcja rozwoju Marynarki Wojennej* uległa modyfikacji. Podjęto decyzję o remoncie dokowym i eksploatacyjnym fregaty t. Oliver Hazard Perry. Remonty te pozwolą na przedłużenie

eksploatacji okrętu do roku 2025. Zaplanowano, że do 31.03.2016 w oparciu o istniejącą platformę (okręt pr. 621) zostanie zakończona budowa nowego okrętu patrolowego ORP Ślązak[5]. Zaplanowano również, że w latach 2015–2026 wybudowane zostaną trzy okręty patrolowe z funkcją zwalczania min Czapla[6]. W planach przyjęto, że niszczyciele min projektu 206FM zostaną wycofane z linii do roku 2019 (jednak w związku z ostatnimi decyzjami okręty te jeszcze przez następne lata pozostaną w służbie).

Kolejne lata pokazały, że realizacja przyjętych założeń modernizacji marynarki wojennej jest znacznie opóźniona. W konsekwencji Marynarka Wojenna RP systematycznie traci zdolności operacyjne. Należy pamiętać, iż od momentu zdefiniowania założeń taktyczno-technicznych i opracowania dokumentacji technicznej do momentu wcielenia okrętu do linii mija zwykle kilka lat (patrz tabela 2).

Przedstawione w tabeli przykłady odnoszą się do różnych państw. Nie są w pełni reprezentatywne, mogą dać jednak wyobrażenie, jak długi jest czas od momentu położenia stępki do momentu wcielenia okrętu do linii. Oczywiście w tabeli powyżej nie uwzględniono czasu, który jest niezbędny do opracowania projektu danego okrętu. Jak wynika z danych zawartych w tabeli 2, średni czas od położenia stępki do wcielenia do linii dla wybranych okrętów wynosi: dla niszczycieli prawie 80 miesięcy (6 lat i 8 miesięcy), dla fregaty prawie 65 miesięcy (5 lat i pięć miesięcy), natomiast dla niszczyciela min prawie 66 miesięcy (5 lat i 6 miesięcy).

Przedstawione dane powinny uzmysłowić wszystkim, że od momentu podjęcia decyzji o budowie okrętu do jego wejścia do służby mija zwykle kilkadziesiąt miesięcy. Mówiąc o programach modernizacyjnych marynarki wojennej, nie wolno zapominać o najważniejszych „aktywach" morskiego rodzaju sił zbrojnych, a mianowicie o załogach okrętów. Należy pamiętać, że równie długo może trwać szkolenie załogi okrętu, by osiągnęła wymagany poziom wyszkolenia. Mając to na uwadze, każde państwo podejmuje różne kroki, które pozwalają na zachowanie potencjału ludzkiego do momentu pozyskania nowych okrętów.

[5] Zaproponowany termin nie został dotrzymany, nadal trwa budowa ORP Ślązaka.
[6] Jeszcze nie rozpoczęto budowy okrętów patrolowych z funkcją zwalczania min Czapla.

Tabela 2. Dane dotyczące budowy i wcielenia do linii wybranych klas, typów okrętów różnych państw

Klasa, typ okrętu	Data położenia stępki	Wodowanie	Wcielenie do linii	Czas od położenia stępki do wcielenia do linii
niszczyciel				
Arleigh Burke (USA)	06.12.1988	18.08.1989	04.07.1991	32 miesiące
Sejong Daewang (Korea Płd.)	12.11.2004	25.05.2007	22.12.2008	49 miesięcy
Daring – t. 45 (W. Brytania)	28.03.2003	01.02.2006	20.04.2012	109 miesięcy
Kolkata – pr. 15A/15B (Indie)	26.08.2003	30.03.2006	18.08.2014	132 miesięcy
fregata				
Gepard – pr. 11661K (Rosja)	15.08.1992	12.07.1993	12.06.2002	118 miesięcy
Sachsen – t. 124 (Niemcy)	01.02.1999	01.12.1999	04.11.2004	69 miesięcy
Jiangwei II – t. 053H3 (Chiny)	04. 10. 1996	10.08.1997	20. 11.1998	26 miesięcy
De Zeven Provincien (Holandia)	01.09.1998	08.04.2000	26.04.2002	44 miesięcy
niszczyciel min				
Eridan – Tripartite (Francja)	20.12.1977	02.02.1979	16.04.1984	76 miesięcy
Aydin – t. MHV 54-014 (Turcja)	25.07.2001	10.05.2004	24.01.2007	66 miesięcy
Alexander – pr. 12700 (Rosja)	22.09.2011	27.06.2014	09.12.2016	62 miesiące
Katanpää (Finlandia)	11.06.2007	18.06.2009	04.05.2012	58 miesięcy

Źródło: opracowanie własne na podstawie [Janes Fighting Ships 2016/2017].

Poniżej w tabeli 3 przedstawiono prognozę rozwoju potencjału ilościowo-jakościowego polskich okrętów mogących realizować zadania w ramach stałych zespołów okrętów, po zmianach zawartych w *Planie modernizacji technicznej Sił Zbrojnych w latach 2013–2022*.

Tabela 3. Prognoza potencjału okrętowego Marynarki Wojennej RP, zdolnego realizować zadania w ramach stałych zespołów okrętów [wg *Planu modernizacji technicznej Sił Zbrojnych w latach 2013–2022*]

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025	2026
	SNMG										
fregata t. OHP	**2**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**0**
okręt obrony wybrzeża	**0**	**0**	**0**	**1**	**1**	**1**	**2**	**2**	**2**	**3**	**3**
fregata Kaszub	**1**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
ORP Ślązak	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
	SNMCMG										
niszczyciel min pr. 206FM	**3**	**3**	**3**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
okręt patrolowy Czapla	**0**	**1**	**1**	**1**	**1**	**2**	**0**	**2**	**2**	**2**	**3**
niszczyciel min Kormoran II	**0**	**1**	**1**	**1**	**1**	**2**	**2**	**2**	**3**	**3**	**3**
ORP Ksawery Czernicki	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
Razem	**8**	**9**	**8**	**6**	**6**	**8**	**7**	**9**	**7**	**8**	**8**
wg *Koncepcji rozwoju Marynarki Wojennej*	**7**	**7**	**6**	**7**	**4**	**6**	**7**	**5**	**8**	**10**	**10**

Źródło: opracowanie własne na podstawie [http://dgrsz.mon.gov.pl/y/pliki/rozne/2013/09/programuzbrojenia_5_sierpnia.pdf].

Porównując potencjał ilościowy polskiej marynarki wojennej zaproponowany w *Planie modernizacji technicznej Sił Zbrojnych w latach 2013–2022* oraz *Koncepcji rozwoju Marynarki Wojennej***,** można zauważyć, że od roku 2024 w zaproponowanej *Koncepcji*

rozwoju Marynarki Wojennej zaplanowano większą liczbę okrętów, które mogą być wydzielone do działań w ramach stałych zespołów okrętów. Smutkiem napawa jednak fakt, że pojawiają się istotne opóźnienia w programie modernizacji marynarki wojennej i przy wcielaniu do linii nowych okrętów. Należy również podkreślić, iż realizacja ogłoszonych programów modernizacyjnych sił zbrojnych jest istotnym elementem budowy wiarygodności nie tylko sojuszniczej, ale również międzynarodowej[7] naszego kraju.

Uwzględniając uwarunkowania polityczne i geograficzne, istniejące oraz potencjalne wyzwania i zagrożenia bezpieczeństwa, jak również posiadany potencjał militarny, w analizach odnoszących się do bezpieczeństwa naszego kraju należy uwypuklić wypowiadane i potwierdzane w praktyce deklaracje polityczne, iż gwarantem bezpieczeństwa naszego kraju jest przynależność do Sojuszu Północnoatlantyckiego. Jednak ze względu na te deklaracje należy pamiętać, że kluczowymi determinantami naszego bezpieczeństwa narodowego są własny – narodowy – potencjał zbrojny i przynależność do NATO. Zatem nasze członkostwo w Sojuszu nie powinno ograniczać się do wypełniania zapisów art. 5 i 6 Traktatu Północnoatlantyckiego, ale coraz większą wagę powinniśmy przywiązywać do zapisów art. 3, który ma następujące brzmienie „[…] **Dla skuteczniejszego osiągnięcia celów niniejszego traktatu, Strony**, **każda z osobna i wszystkie razem, poprzez stałą i skuteczną** samopomoc **i pomoc wzajemną, będą utrzymywały i rozwijały** swoją indywidualną [wytłuszczenie – autora] i **zbiorową** zdolność do odparcia zbrojnej napaści" [*Traktat Północnoatlantycki*].

Warto w tym miejscu przytoczyć uzupełnienie Traktatu Północnoatlantyckiego, które ma następujące brzmienie: „[…] Po zaznajomieniu się z powyższym traktatem, w imieniu Rzeczypospolitej Polskiej oświadczam, że:

- został on uznany za słuszny zarówno w całości, jak i każde z postanowień w nim zawartych;
- Rzeczpospolita Polska postanawia przystąpić do tego traktatu;
- postanowienia traktatu są ratyfikowane, przyjęte, potwierdzone i będą niezmiennie zachowywane.

Na dowód czego wydany został akt niniejszy, opatrzony pieczęcią Rzeczypospolitej Polskiej. Dodano w Warszawie dnia 26 lutego 1999 r.".

Ze względu na to, że kwestia uczestniczenia polskich okrętów w stałych zespołach nie powinna podlegać dyskusji, nasuwa się w tym miejscu pytanie: działania, w ramach których stałych zespołów powinny być wiodące przy określaniu poziomu zaangażowania Marynarki Wojennej?

[7] Według *Wielkiego słownika języka polskiego* wiarygodność jest to cecha kogoś lub czegoś nie budzącego wątpliwości i takiego, któremu można zaufać [http://wsjp.pl/index.php?id_hasla=5318]. W bankowości natomiast wiarygodność to pojęcie określające poziom rzetelności klientów co do terminowego wywiązywania się z przyjętych zobowiązań.

Rysunek 2. Okręt dowodzenia ORP Kontradmirał Ksawery Czernicki wraz z okrętami zespołu SNMCMG2 na redzie Odessy

Źródło: [http://www.prawica.net/6902].

Wydaje się, że dotychczas zgromadzone doświadczenia oraz posiadany potencjał ilościowo-jakościowy predestynuje Polskę do działań w ramach stałych zespołów przeciwminowych (SNMCMG1 i SNMCMG2). Nie oznacza to jednak, że powinniśmy zrezygnować z wydzielania okrętów do stałych zespołów SNMG1 i SNMG2. W tym miejscu należy podkreślić, iż działania w ramach zespołów SNMG są bardziej spektakularne i mają większy wymiar polityczno-militarny niż działania w ramach zespołów SNMCMG, co ma kilka przyczyn, wśród których do najważniejszych należą następujące:

- wielkość okrętów wchodzących w skład stałego zespołu SNMG1 i SNMG2 (okręty klasy niszczyciel lub fregata, a tylko wyjątkowo wydzielane są korwety);
- potencjał bojowy okrętów wydzielanych do tych zespołów (SNMG1 i SNMG2), zarówno w wymiarze projekcji siły, jak i defensywnym;
- zdolność okrętów klasy niszczyciel i fregata do realizacji zadań o różnym charakterze;
- większa dzielność morska i autonomiczność.

Obok zagadnień potencjałowych nie bez znaczenia jest również wymiar ekonomiczny. Otóż należy pamiętać, że koszt wydzielenia okrętów klasy niszczyciel lub fregata do stałych zespołów jest kilkunastokrotnie mniejszy niż koszt porównywalnego udziału w operacji lądowej. Jak wynika z analizy, koszt udziału kontyngentu morskiego, w porównaniu z lądowym, wynosi 1:25, a w przypadku okrętów przeciwminowych jest jeszcze bardziej korzystny. Efektem analiz zaproponowanych rozwiązań powinna

być decyzja określająca poziom zaangażowania Marynarki Wojennej RP w działania poszczególnych stałych sojuszniczych zespołów okrętów.

Zakończenie

Wyniki przeprowadzonego procesu badawczego zawarte w części pierwszej stanowią materiał wyjściowy dla dalszych analiz, których celem jest wypracowanie dla decydentów politycznych rekomendacji odnoszących się do maksymalnego, optymalnego i minimalnego poziomu zaangażowania Marynarki Wojennej RP w działania realizowane w ramach stałych zespołów NATO. Decyzja określająca pożądany, ze względu na polski interes narodowy, poziom zaangażowania polskich okrętów w działania realizowane w ramach stałych NATO-wskich zespołów okrętów (SNMCMG i SNMG) powinna mieć bezpośredni wpływ na program modernizacji Marynarki Wojennej RP. Przedstawione w części pierwszej i części drugiej analizy mogą mieć istotny wpływ na podjęcie strategicznych decyzji dotyczących przyszłości marynarki wojennej w perspektywie najbliższych dekad.

Bibliografia

Ginsbert J. (1938), *Czy Bałtyk jest morzem zamkniętym?*, Oddz. Propagandy Floty Wojennej Ligi Morskiej i Kolonialnej, Warszawa.

Janes Fighting Ships 2016/2017.

Koncepcja rozwoju Marynarki Wojennej (2012), Ministerstwo Obrony Narodowej, [online] http://mw.mil.pl/zasoby/archiwum/upload/koncepcja_MW.pdf, dostęp: 30.05.2017.

ORP Czernicki z sojusznikami w Odessie, [online] http://www.prawica.net/6902, dostęp: 22.05.2017.

Plan Modernizacji Technicznej Sił Zbrojnych w latach 2013–2022, Ministerstwo Obrony Narodowej, [online] http://dgrsz.mon.gov.pl/y/pliki/rozne/2013/09/program_uzbrojenia_5_sierpnia.pdf, dostęp: 28.05.2017.

Strategiczna koncepcja bezpieczeństwa morskiego Rzeczypospolitej Polskiej (2017), Warszawa-Gdynia.

Szubrycht T. (2008), *Leksykon bezpieczeństwa morskiego*, AMW, Gdynia.

Traktat Północnoatlantycki, Biuro Bezpieczeństwa Narodowego, [online]

https://www.bbn.gov.pl/download/1/15754/TraktatPolnocnoatlantycki.pdf, dostęp: 3.06.2017.

Wielki słownik języka polskiego, [online] http://wsjp.pl/index.php?id_hasla=5318, dostęp: 28.05.2017.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **227–239**

Tomasz Szubrycht[1]
Akademia Marynarki Wojennej

Wybrane problemy zaangażowania polskich okrętów w działania stałych zespołów okrętów (część II)

Selected Problems of Polish Ship's Engagement in the Activities of Standing Maritime Groups (Part II)

Abstract: The second part of the paper considers the issue of Polish Navy engagement in the standing maritime groups activities. The paper discusses the levels of different NATO countries of involvement in allied activities at sea. Indicates the proposed variants of national involvement in standing maritime groups.
Key words: Standing NATO Maritime Group, Polish Navy, Allied actions on the seas Maritime potential of the Navy.

Wstęp

Konsekwencją dokonanych analiz przedstawionych w artykule *Wybrane problemy zaangażowania polskich okrętów w działania stałych zespołów okrętów (część 1)* powinna być próba znalezienia odpowiedzi na pytanie, czy polskie okręty powinny działać tylko w składzie zespołów SNMG1 i SNMCMG1, czy również SNMG2 i SNMCMG2.

Wydaje się, że ze względów politycznych polskie okręty powinny uczestniczyć w działaniach zarówno zespołów SNMG, jak i SNMCMG. Oczywiście największy wysiłek operacyjny należałoby skupić na działaniach w ramach SNMCMG1 oraz SNMG1. W dwóch pozostałych stałych zespołach działalność operacyjna powinna być na niższym poziomie. Nasze zaangażowanie w działaniach na południowej flance NATO ma

[1] t.szubrycht@amw.gdynia.pl

wymiar nie tylko militarny, ale również (a może przede wszystkim) polityczny. Jeśli będziemy obecni na południowej flance NATO, to możemy oczekiwać wzajemności, czyli obecności państw Sojuszu na wschodniej flance NATO[2]. W tym miejscu warto ponownie przytoczyć zapisy art. 3 „[…] **Dla skuteczniejszego osiągnięcia celów niniejszego traktatu, Strony, każda z osobna i wszystkie razem, poprzez stałą i skuteczną** samopomoc i **pomoc wzajemną**, **będą utrzymywały i rozwijały** swoją indywidualną [wytłuszczenie – autora] i **zbiorową** zdolność do odparcia zbrojnej napaści" [*Traktat Północnoatlantycki*].

Wydaje się jednak, że zapisy zawarte w art. 3 powinny być wypełniane przez państwa członkowskie nie tylko w przypadku konieczności odparcia zbrojnej napaści. Sojusznicze wsparcie powinno być udzielane państwom członkowskim także w sytuacjach kryzysu lub w celu minimalizowania wyzwań i pozamilitarnych zagrożeń bezpieczeństwa. Wsparcie takie jest istotnym elementem budowania wiarygodności sojuszniczej. Za przykład budowania takiej właśnie wiarygodności sojuszniczej uznać należy obecność państw Sojuszu na wschodniej flance NATO.

Polski poziom zaangażowania w działania stałych zespołów okrętów NATO

Przystępując do wypracowania polskiego poziomu zaangażowania w działania stałych zespołów NATO, warto się zastanowić, które z państw Sojuszu może stanowić punkt odniesienia (być państwem referencyjnym) dla polskiego poziomu zaangażowania w działania stałych zespołów.

Z 29 państw członkowskich Sojuszu pięć z oczywistych względów zostanie wyłączone z analizy (Czechy, Luksemburg, Słowacja, Węgry, jako państwa nieposiadające dostępu do morza, oraz Islandia, która nie posiada marynarki wojennej). Pozostałe 24 państwa zostały podzielone na cztery grupy. Zaproponowany podział jest wynikiem oceny potencjału ilościowo-jakościowego marynarki wojennej danego państwa, poziomu jego morskich ambicji, a także roli i znaczenia gospodarki morskiej oraz tradycji morskich państwa.

Do pierwszej grupy należy zaliczyć państwa, których marynarki wojenne dysponują bardzo znaczącym potencjałem ilościowo-jakościowym. Do grupy tej możemy zaliczyć: Francję, Niemcy, Turcję, USA, Wielką Brytanię. Drugą grupę stanowią następujące państwa: Włochy, Kanada, Hiszpania, Grecja oraz Holandia.

[2] Warto przypomnieć, że 11 spośród europejskich państw NATO należy zaliczyć do południowej flanki NATO. Są to: Albania, Chorwacja, Czarnogóra, Francja, Grecja, Hiszpania, Portugalia, Słowenia, Turcja, Wielka Brytania (Gibraltar) i Włochy.

Polska zaliczana jest do państw nadbrzeżnych średniej wielkości[3] [Szubrycht 2009, s. 188]. Za siły morskie średniej wielkości uznawane są również siły morskie następujących państw NATO: Belgii, Bułgarii, Danii, Grecji, Holandii, Norwegii, Portugalii oraz Rumunii. Biorąc pod uwagę potencjał ilościowo-jakościowy marynarek wojennych, Grecja i Holandia powinny być zaliczone do grupy trzeciej, jednak ze względu na znaczenie gospodarki morskiej, tradycje morskie, świadomość morską społeczeństwa oraz poziom zaangażowania w działania morskie Sojuszu zaliczone je do drugiej grupy. Do trzeciej grupy państw należą z kolei: Belgia, Bułgaria, Dania, Norwegia, Polska, Portugalia oraz Rumunia. Do ostatniej, czwartej, grupy należą: Albania, Czarnogóra[4], Chorwacja, Estonia, Litwa, Łotwa oraz Słowenia. Siły morskie tych państw zaliczane są do małych.

Rozpatrując poziom zaangażowania w działania stałych zespołów, należy określić, które z państw można uznać za państwo referencyjne dla Polski. Takiego państwa trzeba szukać w grupie trzeciej (do której należą: Belgia, Bułgaria, Dania, Norwegia, Portugalia oraz Rumunia). Warto podkreślić, że aktywność w działaniach stałych zespołów marynarki wojennej Bułgarii i Rumunii ma tylko symboliczny wymiar. O wiele większe zaangażowanie w tym zakresie wykazują państwa bałtyckie (Estonia, Litwa i Łotwa), których okręty aktywnie uczestniczą w działalności operacyjnej stałych zespołów przeciwminowych. Aktywność międzynarodowa tych państw nie sprowadza się jednak wyłącznie do działań w ramach zespołów. Oficerowie z państw bałtyckich wchodzą również w skład sztabu zespołu przeciwminowego, a w 2017 roku zespołem SNMCMG1 dowodził estoński oficer kmdr por. Johan Elias SELJAMAA. Warto zaznaczyć, że to właśnie aktywność marynarek wojennych państw bałtyckich jest dominującym wkładem tych państw we wspólny wysiłek militarny Sojuszu.

Pozostaje zatem decyzja, które z czterech państw – Belgię, Danię, Norwegię czy Portugalię – uznać za państwo referencyjne dla Polski. Przystępując do analizy, przyjęto założenie, że jeśli nie będzie możliwości jednoznacznego określenia państwa referencyjnego, to należy określić przynajmniej przybliżony poziom zaangażowania naszego państwa w działania stałych zespołów, który byłby adekwatny do potencjału i aspiracji Polski. Warto przypomnieć, że w latach zimnej wojny w planach Sojuszu siły morskie dwóch państw (Danii i Norwegii) dedykowane były głównie do działań na Bałtyku.

[3] Państwo nadbrzeżne średniej wielkości to *państwo z dostępem do morza, nie będące mocarstwem ani państwem małym. Ma ono możliwości lub aspiracje realizowania interesów morskich na akwenach wykraczających poza granice wód znajdujących się pod jego jurysdykcją tak, aby pretendować do zajęcia wyższej pozycji w stosunkach międzynarodowych. Nie jest ono jednak w stanie rozciągnąć swych wpływów morskich na cały region.*

[4] Czarnogóra stała się członkiem Sojuszu 5 czerwca 2017 roku.

Poniżej w tabeli przedstawiono liczbę dni działalności okrętów wybranych państw NATO w stałych zespołach w latach 2002–2013. Poniższa tabela została opracowana na podstawie danych uzyskanych z *Allied Maritime Command Headquarters*.

Tabela 1. Liczba dni działalności okrętów wybranych państw NATO w stałych zespołach okrętów latach 2002–2013

Państwo	Łączna liczba dni	Średnioroczna liczba dni	Sumaryczna liczba okrętów w roku 2008	Średnioroczna liczba dni przypadająca na jeden okręt
Niemcy	13 020	1 085	52	20,9
Turcja	7 487	624	48	13,0
Wielka Brytania	6 998	583	52	11.2
Włochy	6 185	515	38	13,6
Holandia	6 054	505	21	24,0
USA	5 534	461	138	3,3
Grecja	5 208	434	34	12,8
Norwegia	**5 143**	**429**	**11**	**39,0**
Hiszpania	4 883	407	30	13,6
Belgia	**2 930**	**244**	**8**	**30,5**
Dania	**2 279**	**190**	**9**	**21,1**
Polska	**1 790**	**149**	**8**	**18,6**
Portugalia	**1 302**	**109**	**13**	**8,4**
Kanada	1 270	106	29	3,7
Estonia	1 237	103	7	14,7

Źródło: [Szubrycht 2017].

Jak wynika z danych zawartych w tabeli 4, średnioroczna liczba dni działalności w stałych zespołach przypadająca na jeden okręt dla wszystkich państw Sojuszu uwzględnionych w analizach wynosi 15,9 dnia. Natomiast jeśli uwzględnimy tylko europejskie państwa NATO, to wielkość ta wynosi 18,6 dni. Jest to dokładnie tyle, ile wynosi wartość średnioroczna dla Marynarki Wojennej RP [Szubrycht 2017].

Jednak w przypadku Polski aż 50,8% naszego zaangażowania w działania stałych zespołów przypada na ORP Kontradmirał Ksawery Czernicki[5]. Zatem należy stwierdzić, iż tak wysoką pozycję nasz kraj zawdzięcza wydzielaniu do składu zespołu SNMCMG

[5] ORP Kontradmirał Xawery Czernicki w latach 2010/2011 realizował zadania w ramach SNMCMG1 przez 545 dni, natomiast w roku 2013 wydzielony był do tego samego zespołu na okres 364 dni.

okrętu dowodzenia ORP Kontradmirał Ksawery Czernicki. Pozostałe okręty prowadziły działania w składzie stałych zespołów w wymiarze 881 dni (daje to następującą średnioroczną liczbę dni przypadającą na jeden okręt – 10,5 dnia). Działania polskich okrętów w ramach zespołu SNMG1 miały więc wymiar symboliczny.

Rysunek 1. Fregata rakietowa ORP Gen. T. Kościuszko wychodzi z portu La Valletta (3 września 2016 r.)

Źródło: [*Strategiczna koncepcja bezpieczeństwa morskiego Rzeczypospolitej Polskiej* 2017, s. 18].

Za szczególnie interesującą uznać należy średnioroczną liczbę dni przypadającą na jeden okręt marynarki wojennej Estonii, która wynosiła aż 14,7 dnia. Estonia zaliczana jest do państw nadbrzeżnych małych, zatem wynik 14,7 dnia należy uznać za imponujący. Jest on większy od tego, który osiągnęły: Turcja, Wielka Brytania, Włochy, USA, Grecja, Hiszpania, Portugalia czy Kanada.

Kluczowa, z punktu widzenia podjętych rozważań, wydaje się odpowiedź na pytanie, czy polskie zaangażowanie na poziomie 1 790, czyli na średniorocznym poziomie 149 dni, jest adekwatne do naszych ambicji i możliwości.

Jeśli w rozważaniach pominiemy okręt dowodzenia ORP Kontradmirał Ksawery Czernicki, wówczas okaże się, że średnioroczne zaangażowanie Polski wynosić będzie już tylko 73,4 dnia. Oczywiście osoby niechętne Marynarce Wojennej twierdzić będą, że jest to poziom jeśli nie za wysoki, to przynajmniej wystarczający. Zwolennicy „Polski morskiej" będą z kolei stać na stanowisku, że jest on zbyt mały. Prawda jak zwykle leży gdzieś pośrodku. Wydaje, się że nasze zaangażowanie powinno plasować się na po-

ziomie zbliżonym do Danii, czyli zamknąć się w przedziale między 190 a 240 dni. Zatem Danię można uznać za państwo referencyjne dla naszego kraju.

Minimalny poziom polskiego zaangażowania nie powinien być jednak mniejszy niż 149 dni**,** czyli pozostać na dotychczasowym poziomie. Jednym z ważnych argumentów za zwiększeniem naszego poziomu zaangażowania jest zwiększająca się obecność naszych sojuszników na wschodniej flance NATO. Oczywiście poziom zaangażowania okrętów musi być bardziej zrównoważony i nie może opierać się właściwie na jednym okręcie. Wymaga to pozyskania nowych okrętów, które mogą prowadzić działania w ramach stałych zespołów NATO.

W państwach Sojuszu przyjmuje się założenie, że tylko jeden na trzy (a w niektórych państwach, np. w Kanadzie – nawet jeden na cztery) okręty jest dostępny w dowolnym momencie do realizacji zadań. Ta zależność nazywana jest często współczynnikiem operacyjnego wykorzystania. W rozważaniach taktycznych w Polsce przyjmuje się, że współczynnik operacyjnego wykorzystania wynoszący 1:3 powinien być uwzględniony w określaniu liczby okrętów poszczególnych klas, jakie powinno posiadać państwo.

Konsekwencją przyjętego poziomu ambicji morskich jest konieczność posiadania adekwatnego potencjału ilościowo-jakościowego. Będąc odpowiedzialnym, należy przy przeprowadzanych analizach przyjąć pewne samoograniczenie. Truizmem wydaje się stwierdzenie, że posiadane siły morskie muszą być efektywnie wykorzystywane jako narzędzie realizacji polityki państwa. Nie zawsze oznacza to konieczność rozbudowy potencjału ilościowo-jakościowego. Konieczne jest jednak efektywne wykorzystanie sił w ramach tzw. cyklu operacyjnego.

Preferowany w NATO cykl operacyjny działań okrętów wynosi 24 miesiące (8 kwartałów). W odniesieniu do czterech okrętów przedstawia się on następująco: trzy okręty realizują zadania w cyklu 2-3-3 kwartały (realizacja zadań w ramach: działań międzynarodowych – narodowych – remontów i odtwarzania gotowości bojowej), natomiast cykl czwartego okrętu wynosi 2-2-4 kwartały. Tym samym łącznie okręty mogą przez 8 kwartałów prowadzić działania w ramach aktywności międzynarodowej, przez 11 kwartałów mogą prowadzić działania w wymiarze narodowym (ćwiczenia, codzienna działalność operacyjna, szkolenia), a 13 kwartałów przeznaczyć na odtwarzanie gotowości bojowej i remonty. Tym samym tylko 25% czasu okręty przeznaczają na zadania o charakterze międzynarodowym, 34,4% na misje narodowe, a 40,6% na odtwarzanie gotowości bojowej i remonty.

W innym wariancie dla czterech okrętów mogą one działać w cyklu 2-4-2, natomiast czwarty okręt w cyklu 2-2-4 kwartały. Tym samym uzyskano następujący wynik: 8 kwartałów w ramach działań międzynarodowych – 25%, 14 kwartałów na prowa-

dzenie działań w ramach aktywności narodowej (ćwiczenia, codzienna działalność operacyjna, szkolenia) – 41,7% oraz 10 kwartałów w ramach odtwarzania gotowości bojowej i remontów – 33,3%.

Przyjęcie preferowanego w NATO cyklu operacyjnego pozwala na wydzielenie jednego okrętu do działań międzynarodowych przez cały 24-miesięczny okres.

Natomiast w przypadku trzech okrętów można przyjąć następujący wariant. Dwa okręty będą działać w cyklu 2-4-2 kwartały, natomiast trzeci w cyklu 2-2-4. Oznacza to, że 6 kwartałów okręty mogą prowadzić działania w wymiarze międzynarodowym – 25%, 10 kwartałów w ramach działań narodowych – 41,7% i 8 kwartałów w ramach odtwarzania gotowości bojowej i remontów – 33,3%. Jednak w przypadku przyjęcia tego wariantu przez jeden kwartał w okresie 24 miesięcy nie będzie możliwości wydzielenia okrętów do działań o charakterze międzynarodowym.

W przypadku Marynarki Wojennej RP bardziej efektywny wydaje się odmienny narodowy cykl operacyjny, który nie jest uzależniony od liczby okrętów. Dla każdego okrętu przedstawia się on następująco – 2-4-2 kwartały, a w wariancie większego umiędzynarodowienia – 3-3-2 kwartały.

Poniżej w tabeli 2 przedstawiono wyniki prezentujące liczbę kwartałów, w których okręty mogą realizować zadania w ramach działań międzynarodowych, narodowych oraz liczbę kwartałów, w których mogą być przeprowadzane remonty i odtwarzanie gotowości bojowej. W nawiasie zamieszczono liczbę kwartałów w wariancie większego umiędzynarodowienia dla cyklu operacyjnego przyjętego w MW RP.

Częstym zarzutem pod adresem przedstawicieli marynarki wojennej przekonujących o konieczności rozbudowy potencjału ilościowo-jakościowego jest zarzut mocarstwowości. Pojawia się on w wypowiedziach oponentów, którzy nie rozumieją i nie doceniają wagi oraz znaczenia dla współczesnego państwa bezpieczeństwa morskiego i interesów morskich. Zarzut ten dotyczy nie tylko zbyt dużych wymagań w stosunku do liczby i klas okrętów, którymi powinna dysponować marynarka wojenna, ale również zbyt dużego zaangażowania w działania o charakterze międzynarodowym oraz błędnego zawężania problematyki morskiej i bezpieczeństwa morskiego państwa wyłącznie do Morza Bałtyckiego.

Przedstawione w tabeli 2 i 3 dane obrazują, iż prawie we wszystkich przyjętych wariantach i cyklach operacyjnych dominujące są działania o charakterze narodowym. Nie można zatem twierdzić, że zaangażowanie w działania o charakterze międzynarodowym jest realizowane kosztem bezpieczeństwa państwa zaangażowanego m.in. w wydzielanie okrętów do stałych zespołów okrętów. Tylko w jednym przypadku – przyjęcia w cyklu operacyjnym wariantu obowiązującego w Marynarce Wojennej RP

większego umiędzynarodowienia – istnieje równowaga pomiędzy działaniami o charakterze narodowym i międzynarodowym.

Tabela 2. Liczba kwartałów realizacji zadań w ramach działań międzynarodowych, narodowych oraz remontów i odtwarzania gotowości bojowej

	Działania międzynarodowe		Działania narodowe		Remonty i odtwarzanie gotowości bojowej	
	NATO	MW RP	NATO	MW RP	NATO	MW RP
Wydzielanie okrętów tylko do jednego stałego zespołu (SNMG lub SNMCMG)						
wariant 4 okręty	**8**	**8 (12)**	**14**	**16 (12)**	**10**	**8**
wariant 3 okręty	**6**	**6 (9)**	**10**	**12 (9)**	**8**	**6**
wariant 2 okręty	**4**	**4 (6)**	**8**	**8 (6)**	**4**	**4**
Jednoczesne wydzielanie okrętów do stałego zespołu SNMG i SNMCMG						
wariant 4 okręty	**16**	**16 (24)**	**28**	**32 (24)**	**20**	**16**
wariant 3 okręty	**12**	**12 (18)**	**20**	**24 (18)**	**16**	**12**
wariant 2 okręty	**8**	**6 (12)**	**16**	**16 (12)**	**8**	**8**
wariant mieszany (2 i 4)	**12**	**12 (18)**	**22**	**24 (18)**	**14**	**12**
wariant mieszany (3 i 4)	**14**	**14 (21)**	**24**	**28 (21)**	**18**	**14**
wariant mieszany (2 i 3)	**10**	**10 (15)**	**18**	**20 (15)**	**12**	**10**

Źródło: opracowanie własne.

Tabela 3. Relacje między działaniami międzynarodowymi – narodowym oraz remontami i odtwarzaniem gotowości bojowej dla analizowanych wariantów w różnych cyklach operacyjnych

	Wariant 4 okręty	**Wariant 3 okręty**	**Wariant 2 okręty**	**Wariant mieszany (2 i 4)**	**Wariant mieszany (3 i 4)**	**Wariant mieszany (2 i 3)**
Cykl operacyjny wg NATO	1:1.75:1.25	1:1.67:1.33	1:2:1	1:1,83:1.17	1:1.71:1.29	1:1.8:1.2
Cykl operacyjny wg MW RP	dla wszystkich wariantów wynosi 1 : 2 : 1 w przypadku podjęcia decyzji o większym umiędzynarodowieniu wynosi 1.5 : 1.5 : 1					

Źródło: opracowanie własne.

W trakcie analizy rodzi się również pytanie, jakie powinny być relacje czasu pełnienia służby polskich okrętów w składzie stałych zespołów SNMG i SNMCMG. Jeśli cho-

dzi o potencjał ilościowo-jakościowy, jaki powinna pozyskać MW RP w najbliższej przyszłości w wyniku wdrożenia przyjętego programu modernizacji Marynarki Wojennej, to celowe wydaje się zachowanie następujących relacji poziomu polskiego zaangażowania – od 30 do 40% zaangażowania w działalność zespołów SMNG oraz od 60 do 70% w działania w ramach zespołu SNMCMG.

Na korzyść większego zaangażowania się Marynarki Wojennej RP w działania w ramach stałych zespołów przeciwminowych (SNMCMG) przemawiają m.in. następujące fakty:

- duże doświadczenie w działaniach przeciwminowych realizowanych w wymiarze sojuszniczym;
- posiadanie okrętu dowodzenia ORP Kontradmirał Ksawery Czernicki pozwalającego na efektywne dowodzenie zespołem przeciwminowym;
- doświadczenie w dowodzeniu stałym zespołem przeciwminowym, dzięki czemu realne staje się dowodzenie kolejnymi zespołami przeciwminowymi, a tym samym istnieje możliwość wykorzystania szansy, by dowodzenie zespołem przeciwminowym stało się polską specjalizacją w ramach NATO;
- większy potencjał ilościowo-jakościowy sił przeciwminowych polskiej marynarki wojennej;
- niższe koszty udziału okrętów w zespole przeciwminowym.

Przedstawione w niniejszym artykule analizy pozwalają na zaproponowanie maksymalnego, optymalnego i minimalnego poziomu zaangażowania Marynarki Wojennej RP w działania realizowane w ramach stałych zespołów okrętów (tabela 4). Przedstawione propozycje ujęte zostały w cyklu 24-miesięcznym (8 kwartałów). Uwzględniając ograniczenia ilościowo-jakościowe Marynarki Wojennej RP, należy zauważyć, że nasz kraj tylko w wyjątkowych sytuacjach będzie zdolny do jednoczesnego wydzielenia więcej niż jednego okręt do stałego zespołu. W przypadku polskich okrętów czas wydzielenia do stałych zespołów powinien wynosić do 6 miesięcy, a optymalny wydaje się okres 3 miesięcy.

Przyjęcie wariantu maksymalnego zaangażowania Marynarki Wojennej w działania realizowane w cyklu dwuletnim w ramach stałych zespołów zapewni wydzielenie okrętów na okres 20 miesięcy (patrz tabela 5). Proponuje się niewydzielanie okrętów do stałych zespołów w grudniu i styczniu[6]. Wynika to z przeprowadzonej analizy aktywności działań i widocznego ograniczania wydzielania okrętów do stałych zespołów przez państwa Sojuszu w tych miesiącach.

[6] Jak wynika z uzyskanych danych, liczba wydzielanych okrętów do stałych zespołów w miesiącach letnich oraz w styczniu i grudniu jest najmniejsza. Największa aktywność widoczna jest natomiast wiosną i jesienią.

Tabela 4. Proponowany maksymalny, optymalny i minimalny poziomu zaangażowania Marynarki Wojenne RP w działania realizowane w ramach stałych zespołów okrętów

		1	2	3	4	5	6	7	8	9	10	11	12
I	SNMCMG												
	SNMG												
II	SNMCMG												
	SNMG												
III	SNMCMG												
	SNMG												

		1	2	3	4	5	6	7	8	9	10	11	12
I	SNMCMG												
	SNMG												
II	SNMCMG												
	SNMG												
III	SNMCMG												
	SNMG												

okręty MW RP nie są wydzielane do stałego zespołu

okręty MW RP są wydzielane do stałego zespołu

I - **Wariant maksymalny; II - Wariant optymalny; III - Wariant minimalny.**

Źródło: opracowanie własne.

W wariancie tym możliwe jest pokrycie cyklu dwuletniego w 83%, przy czym okręty mogą realizować zadania w ramach zespołu SNMCMG przez 12 miesięcy, a w ramach SNMG przez 8 miesięcy.

Przyjęcie wariantu optymalnego zaangażowania w działania realizowane w ramach stałych zespołów wynosi 16 miesięcy, odpowiednio w ramach zespołu SNMCMG 10 miesięcy oraz SNMG – 6 miesięcy. Pozwoli to na pokrycie w 67% przyjętego cyklu.

W przypadku przyjęcia wariantu minimalnego zaangażowania polskie okręty prowadziłyby działania przez 10 miesięcy, co pozwoliłoby na pokrycie dwuletniego cyklu

działań zespołów w 42%. Polskie okręty prowadziłyby działania w ramach zespołu SNMCMG przez 7 miesięcy, natomiast w ramach zespołu SNMG przez 3 miesiące.

Tabela 5. Wariantowe propozycje średniorocznego zaangażowanie polskich okrętów w działania stałych zespołów okrętów

Wariant zaangażowania	Stały zespół okrętów	Średnioroczna liczba dni działania w zespole	Łączna średnioroczna liczba dni działania w zespole	Relacja działań w ramach SNMG do SNMCMG
maksymalny	SNMCMG	182	**303**	**40 do 60**
	SNMG	121		
optymalny	SNMCMG	153	**243**	**37 do 63**
	SNMG	90		
minimalny	SNMCMG	107	**152**	**30 do 70**
	SNMG	45		

Źródło: opracowanie własne.

W przypadku przyjęcia wariantu minimalnego zaangażowanie polskie pozostanie na dotychczasowym poziomie. Będzie ono większe od zaangażowania takich państw, jak: Portugalia, Kanada czy Estonia, mniejsze jednak od zaangażowania Danii, Belgii czy Hiszpanii. Jeśli uwzględnimy średnioroczną liczbę dni, w których polskie okręty prowadzą działania w ramach stałych zespołów, nasz kraj nadal będzie zajmował 12 miejsce wśród państw Sojuszu.

Przyjęcie wariantu optymalnego sprawia, że poziom polskiego zaangażowania zwiększy się o 63%. Jeśli uwzględnimy parametr średniorocznej liczby dni operowania w składach stałych zespołów, Polska przesunie się na 10 miejsce (pozycję tę będzie zajmowała wspólnie z Belgią). Będzie to zaangażowanie większe niż Danii, Portugalii, Kanady czy Estonii, mniejsze jednak od zaangażowania Hiszpanii.

W wariancie maksymalnym polskie zaangażowanie zwiększy się o 103% i będzie większe niż zaangażowanie takich państw Sojuszu, jak: Belgia, Dania, Portugalia, Kanada czy Estonia, nadal będzie mniejsze niż zaangażowanie Hiszpanii. Jeśli uwzględnimy średnioroczną liczbę dni działania w ramach stałych zespołów, Polska zajmować będzie 10 miejsce wśród państw NATO.

Przyjmując założenia wariantu maksymalnego, marynarka wojenna powinna dysponować 6–8 okrętami, które mogą być wydzielone do stałego zespołu przeciwminowego, oraz 3–4 okrętami, które mogą prowadzić działania w ramach zespołu SNMG.

W przypadku przyjęcia wariantu optymalnego powinniśmy dysponować 6–7 okrętami wojny przeciwminowej oraz 2–3 okrętami, które mogą być wydzielone do zespołu SNMG. Jeśli natomiast przyjęty zostanie wariant minimalny, to wówczas niezbędne jest posiadanie 4–5 okrętów, które mogą być wydzielone do zespołów SNMCMG, oraz 2 okrętów, które mogą prowadzić działania w składzie zespołów SNMG.

Zakończenie

Na zakończenie przedstawionych analiz konieczne wydaje się podkreślenie, że działania w ramach stałych zespołów wymagają trzech fundamentalnych elementów:
- stosownych decyzji szczebla politycznego;
- adekwatnego do przyjętego wariantu zaangażowania potencjału ilościowo-jakościowego okrętów;
- finansowego zabezpieczenia działań realizowanych w ramach stałych zespołów.

Nie wolno również zapomnieć o ciągłym uświadamianiu społeczeństwu konieczności ponoszenia wysiłku związanego z wydzielaniem okrętów do stałych zespołów okrętów. Okręty te, mimo że operują na akwenach oddalonych od polskiego wybrzeża, wnoszą istotny wkład w bezpieczeństwo naszej Ojczyzny.

Na zakończenie przedstawionych analiz i rozważań warto przedstawić statystykę odnoszącą się do podsumowania dowodzenia zespołem SNMCMG2. W dniach 05.01–10.07.2017 zespołem dowodził polski oficer kmdr por. Aleksander Urbanowicz. Poniżej przedstawiono tylko wybrane dane dotyczące działalności okrętów stałego zespołu przeciwminowego:
- zespół przebył prawie 12,5 tysiąca mil morskich;
- wykrył i zniszczył łącznie 40 min morskich (pozostałości po I i II wojnie światowej);
- przeprowadził 556 godzin ćwiczeń w ramach obrony przeciwminowej;
- brał udział w 5 ćwiczeniach narodowych i międzynarodowych;
- w czasie różnych ćwiczeń i szkoleń na morzu pod dowództwem polskiego oficera znajdowało się 45 okrętów z kilkunastu państw, których załogi liczyły 2237 marynarzy;
- w czasie wizyt w 22 portach okręty zespołu odwiedziło 12 ambasadorów innych państw oraz 7,5 tysiąca zwiedzających;
- załogi okrętów zespołu uczestniczyły w licznych uroczystościach i przedsięwzięciach promujących NATO.

Należy zatem stwierdzić, iż działania w ramach SNMCMG2 miały nie tylko wymiar szkoleniowy, ale były również istotnym elementem dyplomacji morskiej oraz promocji naszego kraju i Marynarki Wojennej RP.

Bibliografia

Strategiczna koncepcja bezpieczeństwa morskiego Rzeczypospolitej Polskiej (2017), Warszawa-Gdynia.

Szubrycht T. (2009), *Zrównoważenie sił morskich w polityce morskiej europejskich państw NATO*, rozprawa habilitacyjna, AON, Warszawa.

Szubrycht T. (2017), *Działania okrętów wybranych państw sojuszu w stałych zespołach okrętów*, „Przedsiębiorczość i Zarządzanie", t. XVIII, z. 5, cz. III.

Traktat Północnoatlantycki, Biuro Bezpieczeństwa Narodowego, [online] https://www.bbn.gov.pl/download/1/15754/TraktatPolnocnoatlantycki.pdf, dostęp: 3.06. 2017.

PRZEDSIĘBIORCZOŚĆ I ZARZĄDZANIE 2018
Wydawnictwo SAN | ISSN 2543-8190
Tom **XIX** | Zeszyt **1** | Część 3 | ss. **241–254**

Jan Waluszewski[1]
Społeczna Akademia Nauk

Wojna hybrydowa a art. 5 Traktatu Północnoatlantyckiego

Hybrid War and Art. 5 of North Atlantic Treaty

Abstract: Author presents a definition of hybrid war as well as its very essence and characteristics. Moreover, author attempts at answering the question which hybrid activities go beyond war threshold and can lead to the use of sanctions provided by Art.5 of North Atlantic Treaty. What is more, he indicates that legal solutions based on experiences of world wars do not constitute sufficient protection from threats of hybrid nature.
Key words: hybrid war, international security, NATO, art. 5 of North Atlantic Treaty, subliminal aggression.

Wprowadzenie

W publicystyce, a także w wypowiedziach naukowych, popularny w ostatnich latach stał się termin „wojna hybrydowa". Pojawił się on na początku lat dziewięćdziesiątych ubiegłego wieku w USA w specjalistycznych opracowaniach dotyczących konfliktów zbrojnych, które w ten sposób określano (brytyjskie wojny interwencyjne w okresie dekolonizacji, operacje amerykańskiej piechoty morskiej czy wojny w Czeczenii) [Piotrowski 2015, ss. 10–16].

Rozpowszechnienie terminu wojna hybrydowa nastąpiło jednakże dopiero w związku z agresją rosyjską na Krymie wiosną 2014 r. oraz walkami toczącymi się od tej pory na terenie wschodniej Ukrainy. Od tego czasu zarówno teoretycy polemolo-

[1] jwaluszewski@san.edu.pl

dzy, jak i różne organizacje zajmujące się problematyką wojny, w tym instytucje rządowe, przedstawiły szereg określeń czy definicji zjawiska jakim jest wojna hybrydowa, zestawiając ją często z innymi formami wojen nowego typu.

W niniejszym opracowaniu rozważam w jakim zakresie sformułowane dotychczas sposoby rozumienia terminu „wojna hybrydowa" mogą być przydatne przy wykładni art. 5 Traktatu Północnoatlantyckiego [Dz. U. 2000, nr 87, poz. 970]. Zagadnienie to jest istotne dla odpowiedzi na pytanie czy może być on zastosowany w przypadku stwierdzenia, iż jedna lub więcej ze stron Traktatu znajduje się w stanie wojny hybrydowej.

Twórcy Traktatu Północnoatlantyckiego, sporządzonego dnia 4 kwietnia 1949 r., przyjęte w nim uregulowania odnosili do doświadczeń wynikających z drugiej wojny światowej, która zgodnie z tofflerowską teorią fal cywilizacyjnych i związaną z nią koncepcją odpowiadających im typów wojen, stanowiła apogeum wojen drugiej fali, czyli wojen masowych ery industrialnej [Toffler, Toffler 2006; Mattis, Hoffman 2005; Balcerowicz 2010, ss. 182–185].

Powstaje zatem pytanie, na ile rozwiązania prawne przyjęte na podstawie doświadczeń odnoszących się do dezaktualizującego się już obecnie sposobu prowadzenia wojen stanowią zabezpieczenie dla stron Traktatu Północnoatlantyckiego, zwłaszcza w kontekście pojawiających się współcześnie wojen nowego typu. Celem artykułu jest odpowiedź na to pytanie, może ona również stanowić podstawę do stawiania wniosków *de lege ferenda* dotyczących zmian przypisów tworzących międzynarodowy system bezpieczeństwa.

Definicja wojny hybrydowej

Podejmując próbę zdefiniowania danego terminu, czyli określenia znaczenia tego wyrażenia, należy ustalić jaki jest tego cel i jaki charakter ma mieć proponowana definicja. Z punktu widzenia tematu niniejszego artykuł podstawowe znaczenie ma kwestia czy przedstawiona definicja ma być definicją sprawozdawczą (informuje o zastanym znaczeniu danego wyrażenia), czy też projektującą (wprowadzającą do danego języka nowy wyraz (zwrot) bądź też ze względu na jakiś określony cel zmienia zastane w danym języku znaczenie konkretnego wyrazu (zwrotu)) [Trypuz 2013, s. 11–14].

Koncepcja wojny hybrydowej stworzona została na gruncie amerykańskiej myśli wojskowej i została użyta w licznych dokumentach rządowych opracowywanych przez siły zbrojne Stanów Zjednoczonych. Przykładem może być choćby określanie pojęcia zagrożeń hybrydowych zawarte w Army Doctrine Publication [*ADRP 3-0 Operations* 2016, ss. 1–3]. Zgodnie z nim, zagrożenie hybrydowe stanowi różnorodne

i dynamiczne połączenie sił regularnych, nieregularnych i terrorystycznych czy elementów przestępczych zjednoczonych w celu osiągnięcia wspólnych korzyści. Zagrożenia hybrydowe łączą konwencjonalne siły zbrojne przestrzegające prawa, tradycji i zwyczajów wojskowych z siłami nieregularnymi, działającymi bez ograniczeń co do stosowanej przemocy i wyboru celu. Co ciekawe termin *hybrid warfare* (wojna hybrydowa) nie został oficjalnie zdefiniowany przez Departament Obrony Stanów Zjednoczonych i w najbliższej przyszłości już nie zostanie, ponieważ Departament nie uzgodnił istnienia tej formy wojny [Hybrid Warfare 2010, s. 11; Nielsen 2014, s. 5].

Niezależnie od tych wahań amerykańskich instytucji wojskowych, definicję zagrożeń hybrydowych (*hybrid threats*) przedstawiło Naczelne Dowództwo Sił NATO [*BI-SC input*… 2010, s. 2]. Zgodnie z nią zagrożeniami hybrydowymi są zagrożenia stwarzane przez przeciwników posiadających zdolność do jednoczesnego stosowania konwencjonalnych i niekonwencjonalnych środków dla osiągnięcia swoich celów.

Również w Polsce znaleźć możemy oficjalną, ale nieustawową (nielegalną) definicję wojny hybrydowej. Minisłownik opracowany przez Biuro Bezpieczeństwa Narodowego definiuje wojnę hybrydową jako wojnę łączącą w sobie jednocześnie różne możliwe środki i metody przemocy, zwłaszcza zbrojne działania regularne i nieregularne, operacje w cyberprzestrzeni oraz działania ekonomiczne, psychologiczne, kampanie informacyjne (propaganda) itp. [(Mini)słownik BBN 2015, s. 8].

O wiele szerzej i bardziej wszechstronnie pojęcie wojen i zagrożeń hybrydowych opisywane jest w literaturze przedmiotu, obejmującej zarówno wypowiedzi o charakterze naukowym jak i publicystycznym.

Powszechnie przyjmuje się, że sformułowania wojna hybrydowa po raz pierwszy użył komandor Robert Walker w niepublikowanej pracy dyplomowej opisującej specjalne operacje Korpusu Piechoty Morskiej Stanów Zjednoczonych [Walker 1998; Hoffman 2007, s. 9]. Kolejnym prekursorem terminu wojna hybrydowa był płk William Nemeth, który w swojej pracy dyplomowej o wojnie w Czeczenii przedstawił ją jako klasyczny przypadek wojny hrybrydowej [Nemeth 2002].

Za głównego autora i propagatora koncepcji wojen hybrydowych uchodzi jednak Frank G. Hoffman. Po raz pierwszy przedstawił on koncepcję wojny hybrydowej w artykule napisanym wspólnie z generałem Jamesem Mattisem [Mattis, Hoffman 2005, s. 2]

Rozwiniętą definicję terminu wojny hybrydowej F. Hoffman przedstawił w pracy „*Conflict in the 21st Century: The Rise of Hybrid Warfare*" [Hoffman 2007, s. 29]. Podaję ją w przekładzie M. Piotrowskiego [Piotrowski 2015, s. 13], który tłumaczy ją następująco: „Wojny hybrydowe są różnopostaciowe ze swojej nazwy i z ich antagonistów […], mogą być prowadzone zarówno przez państwa, jak i wielu aktorów pozapaństwo-

wych, […] łączą w sobie szereg różnych sposobów walki. Wiele tych działań prowadzą odrębne jednostki lub nawet ta sama jednostka, jednakże zazwyczaj są one operacyjnie oraz taktycznie kierowane i skoordynowane w ramach jednego pola walki dla osiągnięcia synergicznych efektów. Efekty te można osiągnąć na wszystkich szczeblach wojny".

W tej samej pracy M. Piotrowski omawia jeszcze drugie ze stosowanych przez F.G. Hoffmana pojęć – zagrożenia hybrydowe [Piotrowski 2015, s. 14]. Słusznie zauważa przy tym, że zdecydowanie lepszym tłumaczeniem tego terminu na język polski byłoby, zamiast „zagrożenia hybrydowe" – „przeciwnik hybrydowy".

Również w literaturze polskiej znaleźć można szereg ciekawych i przydatnych definicji wojny hybrydowej. Jedną z nich przedstawił A. Gruszczak [2011, ss. 13–14], który stwierdził, że wspólnym elementem powołanych przez niego definicji wojen hybrydowych jest „dążenie stron konfliktu do zbliżenia stosowanych przez nie metod, środków oraz sposobów prowadzenia operacji militarnych i pozamilitarnych w celu maksymalizacji efektu synergii, pozwalającego na osiągnięcie względnie trwałej przewagi nad przeciwnikiem, umożliwiającej strukturalną transformację przestrzeni konfrontacji". Cechą hybrydowości współczesnych wojen – zdaniem tego autora – jest współistnienie dwóch zasadniczych płaszczyzn konfliktu: terytorialnej i wirtualnej. Dwa modele wojny hybrydowej opisał Ł. Skoneczny [2015, ss. 45–49] na przykładzie konfliktu ukraińskiego oraz wojny z Państwem Islamskim, natomiast istotę działań hybrydowych wyrazili M. Banasik i R. Parafianowicz [Banasik, Parafianowicz 2015, s. 14] stwierdzając, iż polega ona na „wielowymiarowym, jednoczesnym oddziaływaniu w sferze militarnej z zastosowaniem klasycznych i nieregularnych działań zbrojnych, w sferze informacyjnej, cybernetycznej i ekonomicznej. Głównym polem bitwy będzie umysł pojedynczego człowieka, wybranych grup społecznych i elit władzy, dlatego wojna nowej generacji będzie nierozerwalnie związana z działaniami dezinformacyjnymi i psychologicznymi".

Przedstawione wyżej definicje wojny hybrydowej, z wyjątkiem ostatniej, tworzone były w oparciu o badania i opisy historycznie bądź też współcześnie występujących konfliktów międzynarodowych i wewnętrznych. Z punktu widzenia dalszych rozważań warto jednak przedstawić próby definiowania wojny hybrydowej w sposób syntetyczny bez posługiwania się szerszym lub węższym opisem konkretnych zjawisk.
Autorzy tych definicji ujmują wojnę hybrydową nie od strony metod i środków jakimi jest prowadzona, lecz od strony płaszczyzn czy obszarów w jakich się toczy. J.J. McCuen [2008, s. 107] podniósł, że chociaż konwencjonalna w formie, wojna hybrydowa rozgrywana jest w trzech płaszczyznach: wśród ludności znajdującej się w strefie konfliktu, w świadomości obywateli państwa prowadzącego wojnę oraz w opinii społecz-

ności międzynarodowej. Podobnie M. Wrzosek [2015, ss. 37–45] który opisując wojnę hybrydową toczącą się na Ukrainie, przedstawia ją w trzech wymiarach: regularnych i nieregularnych działań zbrojnych, operacji psychologicznych i propagandy na arenie międzynarodowej.

Jeszcze dalej idzie J.R. Davis Jr. [Davis Jr. 2014, s. 12], który w swojej monografii dowodzi, że wojna hybrydowa nie stanowi zupełnie innej lub nowej formy działań zbrojnych. Istotą jego koncepcji wojny hybrydowej jest nowe podejście do prowadzenia wojny, przyjęte przez jej uczestnika.

Należy również zaznaczyć, że są autorzy, którzy twierdzą, że nie ma potrzeby wyróżniania, a zatem i definiowania wojny hybrydowej jako wojny nowego typu. Podnoszą oni, że konflikty zbrojne zawsze prowadzone były wszelkimi dostępnymi środkami i metodami, zwłaszcza przy nierównorzędnej pozycji przeciwników [Puyvelde 2015; Balcerowicz 2017, s. 18].

Nie podzielając tak skrajnego stanowiska należy raczej zgodzić się ze stwierdzeniem J. Chambersa [2016, s. 43] że zagrożenia hybrydowe i szara strefa występują w działaniach wojennych od stuleci. Natomiast rozwijająca się obecnie dyskusja pomiędzy wojskowymi, naukowcami i politykami na ten temat podkreśla ich odnowione znaczenie.

Wykładnia art. 5 Traktatu Północnoatlantyckiego

Traktat Północnoatlantycki zwany także traktatem Waszyngtońskim został podpisany w Waszyngtonie 4 kwietnia 1949 r. Początkowo sygnowało go 12 państw, a obecnie utworzona na jego podstawie Organizacja Traktatu Północnoatlantyckiego (ang. North Atlantic Treaty Organization – NATO) liczy 29 członków. Polska jest jej członkiem od lutego 1999 r. [Dz.U. 1999, nr 13, poz. 111].

NATO jest sojuszem polityczno-wojskowym o celach obronnych. Jego podstawową funkcją jest (zbiorcza) wzajemna obrona państw członkowskich za pomocą środków cywilnych i wojskowych. Stanowi on również miejsce współpracy i konsultacji w wielu innych dziedzinach służących bezpieczeństwu państw członkowskich. NATO działa także na rzecz zapobiegania konfliktom i ich rozwiązywania zgodnie z zasadami Karty Narodów Zjednoczonych [Kupiecki 2016, s. 219].

Kluczowe znaczenie dla podstawowej funkcji Sojuszu tj. wzajemnej obrony państwa członkowskich posiada art. 5 Traktatu Północnoatlantyckiego. Stanowi on, co następuje: „Art. 5. Strony zgadzają się, że zbrojna napaść na jedną lub więcej z nich w Europie lub Ameryce Północnej będzie uznana za napaść przeciwko nim wszystkim i dlatego zgadzają się, że jeżeli taka zbrojna napaść nastąpi, to każda z nich, w ramach

wykonywania prawa do indywidualnej lub zbiorowej samoobrony, uznanego na mocy artykułu 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom napadniętym, podejmując niezwłocznie, samodzielnie jak i w porozumieniu z innymi Stronami, działania, jakie uzna za konieczne, łącznie z użyciem siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego.

O każdej takiej zbrojnej napaści i o wszystkich podjętych w jej wyniku środkach zostanie bezzwłocznie powiadomiona Rada Bezpieczeństwa. Środki takie zostaną zaniechane, gdy tylko Rada Bezpieczeństwa podejmie działania konieczne do przywrócenia i utrzymania międzynarodowego pokoju i bezpieczeństwa" [Traktat Północnoatlantycki 2000].

Art. 5 Traktatu zawiera stwierdzenie, że strony Traktatu „zgadzają się, że **zbrojna napaść** na jedną lub więcej z nich (...) będzie uznana za napaść przeciwko nim wszystkim" [Traktat Północnoatlantycki 2000]. W tej części przepisu art. 5 zawarta jest hipoteza wynikającej z niego normy prawnej. Kluczowym terminem dla określenia jakie okoliczności faktyczne muszą zaistnieć aby strony Traktatu zgodziły się, iż wystąpiła przesłanka do zachowań opisanych w dyspozycji art. 5 Traktatu jest sformułowanie „zbrojna napaść".

Termin „zbrojna napaść" jest terminem z języka prawnego, używanego w aktach normatywnych. Występuje on w art. 51 Karty Narodów Zjednoczonych [Karta Narodów Zjednoczonych 1947] oraz w art. 5 Traktatu Północnoatlantyckiego. Jednakże, jak zauważa M. Kołodziejczak [Kołodziejczak 2015, s. 74] termin nie został oficjalnie zdefiniowany, czyli brak jest jego definicji legalnej[2].

Analizując dla potrzeb wykładni art. 5 Traktatu Północnoatlantyckiego znaczenie, a zwłaszcza zakres terminu „zbrojna napaść" warto umieścić go w kontekście rozważań na temat pojęcia wojny. Bardzo obszerne i wszechstronne wywody na ten temat przedstawia J. Reginia-Zacharski [2010/2011].

Przedstawia on definicje wojny oraz konfliktu zbrojnego formułowane przez specjalistów polemologów oraz różne instytucje badawcze. Charakterystyczną cechą większości tych definicji jest ich typologiczny charakter. Przedstawiają one konflikt zbrojny jako cykl zdarzeń, działań i zachowań, którego zwieńczeniem może, aczkol-

[2] Należy jednak zwrócić uwagę, że Polska jest stroną podpisanej w Londynie w dniu 3 lipca 1933 r. konwencji o określeniu napaści. Konwencję tą, przygotowaną z inicjatywy Związku Radzieckiego, który w następnych latach okazał się jednym z największych agresorów w skali światowej, podpisało kilka państw. Nie została ona jednak powszechnie przyjęta przez społeczność międzynarodową, a późniejsze działania w kierunku przyjęcia definicji pojęcia agresji nie zostały uwieńczone powodzeniem. Na XXIX sesji Zgromadzenia Ogólnego ONZ przyjęta została, w dniu 14 grudnia 1974 r., rezolucja nr 3314 (XXIX) zawierająca definicję agresji [Resolution 3314 (XXIX)1974] jednakże w świetle przeważających w doktrynie prawa międzynarodowego poglądów, nie jest ona prawnie wiążąca [Kołodziejczak 2015, s. 73].

wiek nie musi, być wojna. Pomimo, że wojna jest zjawiskiem, które towarzyszy ludzkości od zarania dziejów, jej definicja także przysparza trudności.

Najprostsze, ale niezbyt przydatne dla opisu współcześnie występujących zjawisk, jest formalnoprawne określenie wojny, jako przeciwstawnej stanowi pokoju. Polega ona na walce zbrojnej pomiędzy państwami oraz na innych wrogich działaniach kierowanych przez nie przeciwko sobie. Dlatego, z punktu widzenia przedmiotu niniejszego opracowania, interesujący będzie zakres zjawisk występujących pomiędzy wojną zdefiniowaną, w wyżej przedstawiony, formalny sposób, a stanem pokoju.

Wracając do analizy pojęcia „zbrojna napaść" zawartego w hipotezie art. 5 Traktatu Północnoatlantyckiego zwrócić należy uwagę na określenie pojęcia napaść zbrojna zawarte w wyroku Międzynarodowego Trybunału Sprawiedliwości z 27 czerwca 1986 r. w sprawie Nikaragui [Wyrok Międzynarodowego Trybunału Sprawiedliwości z 27.06.1986 r., s. 93]. Trybunał stwierdził w nim, że: „zbrojny atak musi być rozumiany, jako obejmujący nie tylko działania regularnych sił zbrojnych przekraczających granice międzypaństwowe, ale także wysyłanie przez państwo lub w jego imieniu zbrojnych zespołów, grup niezarejestrowanych lub najemników, które atakują siły zbrojne innego państwa z nasileniem odpowiadającym zbrojnemu atakowi przeprowadzonemu przez regularne siły zbrojne lub z ich znacznym udziałem". Trybunał odwołał się w tym stwierdzeniu do określenia agresji zawartego w art. 3 Rezolucji 3314 (XXIX) w sprawie definicji agresji z dnia 14 grudnia 1974 r. [Resolution 3314 (XXIX) 1974, ss. 142–144] .

Jak wskazuje P. Milik [2014, s. 2] po zamachach terrorystycznych z dnia 11 września 2001 r. w Stanach Zjednoczonych, społeczność międzynarodowa uznała, że zbrojna napaść może być dokonana nie tylko przy użyciu środków militarnych, ale także przy wykorzystaniu innych środków o charakterze cywilnym w celu spowodowania zamachu terrorystycznego o szerokim działaniu (samoloty cywilne, ciężarówki lub autobusy użyte jako środki napaści).

Dla sprecyzowania zakresu terminu zbrojna napaść, koniecznego przy ustalaniu hipotezy normy prawnej wynikającej z art. 5 Traktatu Północnoatlantyckiego warto sięgnąć do koncepcji agresji podprogowej, w Polsce rozwijanej przede wszystkim przez prof. Stanisława Kozieja [Koziej 2016]. Zdefiniował on „agresję poniżej progu wojny (agresję podprogową)" jako działania wojenne, których rozmach i skala są celowo ograniczane i utrzymywane przez agresora na poziomie poniżej dającego się w miarę jednoznacznie zidentyfikować progu regularnej, otwartej wojny. Celem agresji podprogowej jest osiągnięcie przyjętych celów z jednoczesnym powodowaniem trudności w uzyskaniu konsensusu decyzyjnego w międzynarodowych organizacjach bezpieczeństwa [Koziej 2015, s. 2].

W cytowanej definicji agresji podprogowej prof. S. Koziej zwraca uwagę, że jednym z celów agresji jest utrudnianie uzyskania zgodnego stanowiska w kwestii reakcji na tą agresję czego, w przypadku będącym przedmiotem naszych rozważań, dotyczy możliwości zastosowania art. 5 Traktatu Północnoatlantyckiego.

Na podstawie dotychczasowych wywodów, a także posługując się opisem faz wojny hybrydowej przedstawionym przez D. Niedzielskiego [Niedzielski 2016, s. 38] można przedstawić sekwencję zjawisk (działań, zachowań, sytuacji) objętych pojęciem wojny hybrydowej. Według tego autora w wojnie hybrydowej można wyróżnić trwającą prawie przez cały okres trwania konfliktu, fazę **kształtowania**, polegającą na wpływaniu na opinię społeczną przeciwnika w celu stworzenia warunków sprzyjających osiąganiu własnych celów. Następne fazy to: **infiltracja** – nasycanie społeczeństwa przeciwnika elementami popierającymi lub propagującymi działania własne, w tym również pracownikami wywiadu, szkolenie i wyposażanie grup sabotażowych kierowanych przeciwko wybranym strukturom przeciwnika (ugrupowaniom politycznym, wojsku, policji). Faza ta może trwać od kilku miesięcy do kilku lat, aż do osiągnięcia gotowości do przejścia do fazy konfliktu.

Konflikt – prowadzenie bezpośrednich działań w celu zmuszenia przeciwnika do zachowań uniemożliwiających osiągnięcie celów atakującego.

Powrót do normalizacji – budowanie w zaatakowanym państwie systemu wspierającego realizację celów atakującego.

Niewątpliwie wejście wojny hybrydowej w fazę konfliktu lub, według prof. S. Kozieja, przekroczenie progu wojny wypełnia hipotezę art. 5 Traktatu Północnoatlantyckiego i uzasadnia zastosowanie jego dyspozycji. Powstaje natomiast pytanie czy zjawiska występujące we wcześniejszych fazach wojny hybrydowej mogą stanowić podstawę do podjęcia działań przewidzianych w powyższym przepisie. Inaczej mówiąc, czy art. 5 Traktatu Północnoatlantyckiego będzie miał zastosowanie, gdy działania agresora w stosunku do państwa członkowskiego NATO nie przekroczą opisanego przez S. Kozieja progu wojny, czyli będą mieściły się w obszarze agresji podprogowej.

Wydaje się, że z uwagi na ogromny ciężar odpowiedzialności związany z decyzją o zastosowaniu art. 5 Traktatu, niezależnie od tego czy podjęte w ramach prawa do samoobrony działania będą polegały na użyciu siły zbrojnej, członkowie NATO będą powstrzymywali się z podjęciem decyzji o jego zastosowaniu, aż do chwili stwierdzenia, że próg wojny został przekroczony.

Ponadto należy zwrócić uwagę, iż nawet w przypadku uznania przez zamierzające interweniować w ramach samoobrony państwa członkowskie NATO, że wypełniona została hipoteza art. 5 Traktatu Północnoatlantyckiego, czyli nastąpiła zbrojna napaść

na innego członka NATO, dyspozycja zawarta w tym przepisie pozwala interweniującym członkom/stronom Traktatu podjąć działania „jakie uznają za konieczne".

Zwrócił na to uwagę, cytowany przez T. Pisulę profesor James Roberts w artykule *Czy Ameryka poważy się na wojnę z Rosją?* [Pisula 2014, s. 3]. Roberts twierdzi, że w przypadku ewentualnej agresji wobec któregoś z państw Europy Wschodniej, działania jakie uznają za konieczne Stany Zjednoczony będą polegały na ostrej retoryce i minimalnych sankcjach. Lęk przed wojną z Rosją jest w amerykańskim establishmencie na tyle duży, że będzie gotowy poświęcić jakiś mały i daleki kraj, np. Estonię, aby nie narazić się na starcie z Rosją.

Zakończenie

Sześćset lat przed narodzinami Chrystusa, w Chinach, wędrowny doradca, filozof i uczony Sun Tzu stworzył traktat „Sztuka wojny", w którym w 13 rozdziałach przedstawił rozważania na temat teorii wojny. Traktat ten jest do tej pory wykładany w akademiach wojskowych, gdyż zawarte w nim twierdzenia nie straciły na aktualności, pomimo całkowitej zmiany stosunków politycznych, społecznych i ekonomicznych oraz ogromnego postępu technologicznego. Jednym z nich jest zawarte w rozdziale trzecim „Sztuki wojny" stwierdzenie, że najlepszym sposobem walki jest prowadzenie wojny bez ponoszenia strat własnych oraz bez wyrządzania strat wrogowi: „Dlatego osiągnięcie po sto zwycięstw w stu bitwach nie jest szczytem doskonałości. Prawdziwym szczytem doskonałości jest pokonanie armii wroga bez podejmowania walki" [Sun Tzu, Sun Pin 2013, s. 19].

Inny wielki teoretyk wojskowości, żyjący około dwa i pół tysiąca lat później, generał Carl von Clausewitz (1780–1831), którego teoria strategii studiowana jest w akademiach wojskowych, a także w szkołach menedżerskich, w swoim głównym dziele „O wojnie" pisał: „Wojna jest więc aktem przemocy, mającym na celu zmuszenie przeciwnika do spełnienia naszej woli" [Clausewitz 2006, s. 16]. W innym miejscu stwierdził, że: „wojna jest niczym innym, jak dalszym ciągiem polityki przy użyciu innych środków" [Clausewitz 2006, s. 468].

Trudno nie przyznać, że przywołane wyżej myśli wielkich strategów pobrzmiewają we współczesnej rosyjskiej doktrynie wojennej, zwanej „doktryną Gierasimowa". Zakłada ona, że reguły wojny uległy zmianie, że zatarła się linia między wojną a pokojem oraz że zwiększyło się znaczenie niemilitarnych środków osiągania militarnych i strategicznych celów, które w wielu przypadkach są skuteczniejsze niż środki militarne [Asymmetric Warfare Group 2016, s. 3].

Coraz istotniejsze jest wykorzystanie różnorodnych instrumentów politycznych, ekonomicznych i humanitarnych w połączeniu z manipulowaniem nastrojami ludności zamieszkującej teren konfliktu [Skoneczny 2015, s. 43]. Może to doprowadzić do tego, że cele polityczne i strategiczne osiągnięte zostaną bez posługiwania się środkami militarnymi, a przynajmniej bez stosowania ich na poziomie powyżej progu wojny.

W takiej sytuacji powstaje pytanie, czy państwa strony Traktatu Północnoatlantyckiego, uznają, że powyższe działania dają podstawę do zastosowania art. 5 Traktatu Północnoatlantyckiego. Pozytywna odpowiedź na to pytanie może być trudna, gdyż opisane wyżej działania nie dają się zakwalifikować jako „napaść zbrojna". A jak wynika z językowej wykładni art. 5 Traktatu dopiero zbrojna napaść na któregokolwiek z członków NATO, uruchamia zastosowanie środków przewidzianych w art. 5

Art. 5 Traktatu Północnoatlantyckiego w przypadku zbrojnej napaści na jednego z członków Traktatu przewiduje możliwość różnych działań w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego, a użycie siły jest środkiem najdalej idącym. Jednakże warunkiem podjęcia tych wszystkich działań jest napaść zbrojna na jednego z członków NATO.

Wydaje się, że reakcja na agresję o charakterze podprogowym, skierowaną przeciwko jednemu z członków Sojuszu, może być prowadzona w oparciu o jedną z dwóch możliwych interpretacji przepisów Traktatu Północnoatlantyckiego.

Po pierwsze stosując bardzo szeroką wykładnię art. 5 Traktatu można przyjąć, że pewne działania prowadzone w ramach wojny hybrydowej stanowią zbrojną napaść na członka NATO. Próbę taką podjęto w związku z nasilonymi agresywnymi działaniami Rosji w cyberprzestrzeni.

Cyberatak na Estonię w 2007 roku, atak na elektrownię na Ukrainie w 2015 r., działania rosyjskich hakerów w czasie kampanii wyborczych w Stanach Zjednoczonych w 2016 roku oraz we Francji i Niemczech w 2017 r., a także ostatnia akcja dotycząca telefonów komórkowych żołnierzy NATO stacjonujących w Polsce i krajach nadbałtyckich uzasadniają reakcję państw NATO.

Takie stanowisko zaprezentował Sekretarz Generalny NATO Jens Stoltenberg w marcu 2015 r. na seminarium dotyczącym transformacji NATO, gdzie stwierdził, że atak cybernetyczny może wywołać odpowiedź zgodnie z zasadami artykułu 5 Traktatu Północnoatlantyckiego [Pawłowski 2015, s. 1].

Formalna podstawa dla działań NATO w związku z atakami w cyberprzestrzeni sformułowana została w Deklaracji końcowej szczytu NATO w Warszawie, gdzie uznano cyberprzestrzeń za obszar działań, w którym NATO musi bronić się tak samo skutecznie jak w powietrzu, na lądzie i na morzu. Zdecydowano tam o wzmocnieniu cy-

berobrony sieci i infrastruktury krajów członkowskich NATO opierając ją o pogłębioną współpracę z Unią Europejską [*Deklaracja końcowa szczytu NATO w Warszawie* 2016, s. 205 i nast.].

W kolejnym punkcie tej Deklaracji uczestnicy szczytu oświadczyli, że podjęli również kroki w celu zapewnienia sobie zdolności do skutecznego reagowania na wyzwania jakie stawia przed nimi wojna hybrydowa.

To ostatnie oświadczenie wskazuje na drugą możliwość interpretacji przepisów Traktatu Północnoatlantyckiego. Przewidują one bowiem, w szczególności w art. 3 i art. 4, możliwość podejmowania samodzielnie przez poszczególne państwa bądź też we współpracy z innymi członkami Sojuszu działań zmierzających do utrzymania i rozwijania swoich indywidualnych i zbiorowych zdolności do odparcia zbrojnej napaści. Oznacza to możliwość podejmowania indywidualnych oraz zbiorowych działań poniżej progu wojny, a zatem bez stosowania dyspozycji wynikającej z art. 5 Traktatu Północnoatlantyckiego.

Pomimo iż nie da się uniknąć występowania we współczesnych czasach wojen i konfliktów zbrojnych o różnym stopniu intensywności, wydaje się, że coraz większego znaczenia nabiera rywalizacja prowadzona pomiędzy państwami, czy też grupami państw, na poziomie poniżej progu wojny. Jej celem jest, zgodnie z wskazaniami Sun Tzu i Carla von Clausewitza, osiągnięcie takiej przewagi nad przeciwnikiem, która spowoduje, że będzie on postępował zgodnie z politycznymi i ekonomicznymi interesami działającego państwa lub grupy państw.

Takie działania o charakterze hybrydowym mają doprowadzić do destabilizacji systemu politycznego zaatakowanego państwa, osłabienia jego gospodarki, zburzenia panującego w nim ładu społecznego i osłabienia jego pozycji międzynarodowej. W rezultacie mają one doprowadzić do podporządkowania się tego państwa i społeczeństwa woli agresora.

Jak wynika z wyżej przedstawionych rozważań, instrumenty prawa międzynarodowego zbudowane na podstawie doświadczeń uzyskanych w wyniku toczonych w XX wieku wojen starego typu, takie jak system bezpieczeństwa zbiorowego oparty na Karcie Narodów Zjednoczonych i Traktacie Północnoatlantyckim, nie zapewniają jego uczestnikom wystarczającej ochrony przed wojną hybrydową i jej konsekwencjami.

Bibliografia

ADRP 3-0 Operations (2016), Headquarters Department of the Army [online], http://www.apd.army.mil/epubs/DR_pubs/DR_a/pdf/web/ADRP%203-0%20FINAL%20WEB.pdf, dostęp: 9.07.2017.

Asymmetric Warfare Group (2016), Russian New Generation Warfare [online], https://info.publicintelligence.net/AWG-RussianNewWarfareHandbook.pdf, dostęp: 1.10.2017.

Balcerowicz B. (2010), *Siły zbrojne w stanie pokoju, kryzysu, wojny*, Wydawnictwo Naukowe Scholar, Warszawa.

Balcerowicz B. (2017), *O przyszłych wojnach*, „Kwartalnik Bellona", nr 1/2017, ss. 11–19.

Banasik M., Parafianowicz R. (2015), *Teoria i praktyka działań hybrydowych*, „Zeszyty Naukowe Akademii Obrony Narodowej", nr 2(99), ss. 5–15.

BI-SC input to a new nato capstone concept for the military contribution to countering hybrid threats (2010), Allied Command Transformation [online], http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf, dostęp: 9.07.2017.

Chambers J. (2016), *Countering Gray-Zone Hybrid Threats: An MWI Report*, Modern War Institute at West Point.

Clausewitz C. von (2006), *O wojnie*, Mireki, Kraków.

Davis Jr J.R. (2014), *The hybrid mindset and operationalizing innovation: toward a theory of hybrid*, School of Advanced Military Studies, United States Army Command and General Staff College, Fort Leavenworth, Kansas.

Deklaracja końcowa szczytu NATO w Warszawie (2016), „Bezpieczeństwo Narodowe", Biuro Bezpieczeństwa Narodowego, 2016/I–IV.

Gruszczak A. (2011), *Hybrydowość współczesnych wojen – analiza krytyczna,* [w:] W. Sokała, B. Zapała (red.), *Asymetria i hybrydowość. Stare armie wobec nowych konfliktów*, Biuro Bezpieczeństwa Narodowego RP – Instytut Nauk Politycznych Uniwersytetu Jana Kochanowskiego, Kielce.

Hoffman F.G. (2007) *Conflict in the 21st Century: The Rise of Hybrid Warfare*, Potomac Institute for Policy Studies, Arlington, Virginia.

Hybrid Warfare: Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities (2010), The U.S. Government Accountability Office [online], www.gao.gov/assets/100/97053.pdf, dostęp: 9.07.2017.

Karta Narodów Zjednoczonych (Dz. U. z 1947 r., nr 23, poz. 90).

Kołodziejczak M. (2015), *Analiza pojęcia wojny, agresji i napaści zbrojnej oraz przykłady ich użycia w aktach prawnych obowiązujących w Rzeczypospolitej Polskiej*, „Obronność", Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej, nr 2(14), ss. 70–79.

Koziej S. (2015), *Agresja poniżej progu wojny (agresja podprogowa)*, [online], http://koziej.pl/wp-content/uploads/2015/11/Agresja-podprogowa.pdf, dostęp14.08.2017.

Koziej S. (2016), *Hybrydowa zimna wojna w Europie*, Pulaski Policy Papers, Fundacja im. Kazimierza Pułaskiego [online], https://pulaski.pl/wp-content/uploads/2015/02/Pulaski_Policy_Papers_Nr_20_16.pdf, dostęp: 14.08.2017.

Kupiecki R. (2016), *Organizacja Traktatu Północnoatlantyckiego*, Ministerstwo Spraw Zagranicznych [online],http://www.msz.gov.pl/resource/99ad1565-6b31-43fb-a930-e3aef272c42c:JCR, dostęp: 16.08.2017.

Mattis J., Hoffman F.G. (2005), *Future Warfare: The Rise of Hybrid Wars*, „Proceedings Magazine", U.S. Naval Institute, tom 132/11/1, 233, [online], http://www.usni.org/magazines/proceedings/archive/story.asp?print=…, dostęp: 18.08.2017.

McCuen J. (2008), *Hybrid Wars*, „Military Review", vol. 88, no. 2, ss. 107–113.

Milik P. (2014), *Dopuszczalne przypadki użycia sił zbrojnych w świetle prawa międzynarodowego*, „Portal Spraw Zagranicznych" [online], http://www.psz.pl/117-polityka/dopuszczalne-przypadki-uzycia-sil-zbrojnych-w-swietle-prawa-miedzynarodowego, dostęp: 14.08.2017.

(Mini)słownik BBN (2015), *Propozycje nowych terminów z dziedziny bezpieczeństwa*, Biuro Bezpieczeństwa Narodowego [online], www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html, dostęp: 9.07.2017.

Nemeth W.J. (2002), *Future war and Chechnya: a case for hybrid warfare*, Naval Postgraduate School Monterey [online], https://calhoun.nps.edu/bitstream/handle/10945/5865/02Jun_Nemeth.pdf?sequence=1&isAllowed=y, dostęp: 9.07.2017.

Niedzielski D. (2016), *Zagrożenia hybrydowe. Podstawowe informacje i zdolności Sił Zbrojnych RP*, „Kwartalnik Bellona", nr 2/2016 (685), ss.35–46

Nielsen J.N. (2014), *Hybrid Warfare*, „Grand Strategy. The View from Oregon" [online], https://geopolicraticus.wordpress.com/2014/10/07/hybrid-warfare, dostęp 9.07.2017.

Pawłowski J. (2015), *NATO odeprze atak cybernetyczny. „Odpowiedź zgodnie z Artykułem 5"*, Serwis Internetowy Defence24.pl [online], http://www.defence24.pl/208877,nato-odeprze-atak-cybernetyczny-odpowiedz-zgodnie-z-artykulem-5, dostęp: 6.06.2017.

Piotrowski M.A. (2015), *Konflikt nigdy nie jest prosty: amerykańska teoria i doktryna wojen oraz przeciwników hybrydowych*, „Sprawy Międzynarodowe", nr 2, ss. 7–38

Pisula T. (2014), *Co nam gwarantuje artykuł 5*, Serwis Internetowy Niezależna.pl [online], http://niezalezna.pl/60164-polska-i-nato-co-nam-gwarantuje-artykul-5, dostęp: 1.10.2017.

Puyvelde D. Van (2015), *Hybrid war – does it even exist?*, NATO Review magazine [online], http://www.nato.int/docu/review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/, dostęp: 8.07.2017.

Reginia-Zacharski J. (2010/2011), *Analityczne definicje wojny*, „Studia Geopolitica", Rocznik Polskiego Towarzystwa Geopolitycznego, Rok(1), [online], www.geopolityka.org/analizy/jacek-reginia-zacharski-analityczne-definicje-wojny, dostęp: 10.07.2017.

Resolution 3314 (XXIX) (1974), ONZ.

Skoneczny Ł. (2015), *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia*, Przegląd Bezpieczeństwa Wewnętrznego, Wydanie Specjalne, Agencja Bezpieczeństwa Wewnętrznego, ss. 39–50.

Sun Tzu, Sun Pin (2013), *Sztuka wojny*, tłum. R.D. Sawyer, Helion S.A. Gliwice.

Trypuz R. (2013), *Logika. Definicje. Wykład*, KUL [online], http://trypuz.pl/slajdy/definicje.pdf, dostęp: 30.01.2018.

Toffler A.,Toffler H. (2006), *Wojna i antywojna*, Kurpisz S.A., Poznań.

Traktat Północnoatlantycki (2000) (Dz. U. 2000, nr 87, poz. 970).

Ustawa z dnia 17 lutego 1999 o ratyfikacji Traktatu Północnoatlantyckiego, sporządzonego w Waszyngtonie dnia 4 kwietnia 1949 r. (Dz.U. 1999, nr 13, poz. 111).

Walker R. (1998), *SPEC FI: the United States Marine Corps and Special Operations*, Naval Postgraduate School, Monterey, [online], https://calhoun.nps.edu/bitstream/handle/10945/8989/specfiunitedstat00walk.pdf?sequence=1, dostęp: 9.07.2017.

Wrzosek M. (2015), *Trzy wymiary wojny hybrydowej na Ukrainie*, „Kwartalnik Bellona", nr 3, ss. 33–46.

Wyrok Międzynarodowego Trybunału Sprawiedliwości z 27.06.1986 r., [online], www.icj-cij.org/070-19860627-JUD-01-00-EN.pdf, dostęp: 15.07.2017.

SPOŁECZNA AKADEMIA NAUK

Studia I i II stopnia

(LICENCJACKIE, INŻYNIERSKIE, MAGISTERSKIE, JEDNOLITE MAGISTERSKIE)

SPOŁECZNE I HUMANISTYCZNE

- Bezpieczeństwo narodowe
- Dziennikarstwo i komunikacja społeczna
- Europeistyka
- Filologia angielska
- Japonistyka
- Pedagogika
- Pedagogika specjalna
- Pedagogika resocjalizacyjna
- Psychologia
- Socjologia
- Socjokryminologia
- Stosunki międzynarodowe
- Turystyka i rekreacja

EKONOMICZNE

- Finanse i rachunkowość
- Logistyka
- Zarządzanie
- Ekonomia

ARTYSTYCZNE

- Film i sztuki audiowizualne
- Grafika

MEDYCZNE

- Fizjoterapia
- Kosmetologia
- Zdrowie publiczne

PRAWNE

- Prawo
- Administracja

TECHNICZNE

- Architektura i urbanistyka
- Geodezja i kartografia
- Informatyka

Studia podyplomowe

www.podyplomowe.san.edu.pl

PAO: Studia przez internet

www.pao.pl

Studia III stopnia

(SEMINARIUM DOKTORANCKIE)

- Informatyka
- Zarządzanie
- Językoznawstwo

www.san.edu.pl

CLARK UNIVERSITY

Studia w języku angielskim:

*** Bachelor & Master**

- International Business Management
- International Business Communication
- International Tourism and Hospital Management
- IT Management

*** American Master from Clark University**

- Master of Science in Professional Communication
- Master of Public Administration
- Master of Science in Information Technology

*** MBA@SAN z dyplomem Master Clark University Ma**

www.clarkuniversity.eu

ISSN 2543-8190