Andrzej Żebrowski

Instytut Politologii
Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie

Służby specjalne w zmieniającym się środowisku bezpieczeństwa międzynarodowego w XXI wieku

Wprowadzenie

Przemiany cywilizacyjne w zasadniczy sposób zmieniły otoczenie państw, które podlegają wszechobecnej globalizacji. Jest to proces, który wkracza we wszystkie obszary działania państwa i człowieka. Jest ona źródłem postępu, ale i zacofania. Skala i charakter występujących zagrożeń to poważne wyzwanie dla poszczególnych państw, które podejmują wysiłki w celu ich minimalizacji, lub niedopuszczenia do ich powstania. Jest to trudny i złożony problem, wymagający współpracy nie tylko państw, ale i organizacji międzynarodowych.

Artykuł ten jest poświęcony służbom specjalnym i ich podstawowej funkcji informacyjnej, która stanowi podstawę współpracy międzynarodowej państw członkowskich NATO i Unii Europejskiej, a także bilateralnych porozumień z państwami niebędącymi członkami wskazanych organizacji. Uwzględnione zagrożenia są rozpoznawane i zwalczane przez służby każdego państwa, przy uwzględnieniu własnej specyfiki. W związku z tym problematyka działania służb została ukazana w sposób ogólny, bez odnoszenia się do służb konkretnego państwa.

W prezentowanym materiale poruszone zostały trzy wybrane kwestie. Pierwsza to charakterystyka środowiska bezpieczeństwa międzynarodowego, którego ewolucja stanowi wyznacznik kierunków zainteresowania służb specjalnych. Kolejne zagadnienie to zasilanie informacyjne, które jest kluczem do realizacji zadań w otoczeniu wewnętrznym i zewnętrznym państwa. Ostatnie to funkcjonowanie służb specjalnych zarówno cywilnych, jak i wojskowych.

Charakterystyka środowiska bezpieczeństwa międzynarodowego

Współczesne środowisko międzynarodowe poszukuje nowej pod względem jakościowym formuły bezpieczeństwa. Zachodzące procesy to następstwo zaniku dwubiegunowego podziału świata, przemian cywilizacyjnych (w tym

zderzenie kręgów cywilizacyjnych), gdzie wszechobecna globalizacja zdominowała wszystkie sfery działania państw. Dla jednych są one źródłem postępu i rozwoju, a dla innych źródłem niepewności i biedy.

W ostatniej dekadzie XX wieku byliśmy świadkami ogromnych zmian cywilizacyjnych: technologicznych, politycznych, społecznych i kulturowych. Postęp w technice, procesach wytwarzania, przetwarzania i przekazywania informacji dokonał się na oczach niemal jednego pokolenia i umożliwił budowanie zupełnie nowej jakości życia i pracy. Zmiany te, poza już obecnie oczywistymi, cechuje także[1]:

1) rozwój społeczności otwartej na osiągnięcia i wartości innych narodów, kultur, grup i pojedynczych ludzi,
2) popularyzacja idei wolności, solidarności, tolerancji,
3) ograniczenie suwerenności państwa na rzecz instytucji samorządowych i grup lokalnych, jak również instytucji międzynarodowych,
4) humanizacja stosunków międzyludzkich głównie przez zastępowanie przymusu wolnym i świadomym wyborem,
5) zanikanie tradycyjnych podziałów społecznych i równoczesny wzrost znaczenia ludzi wykształconych – merytokracji.

Powyższe zjawiska to początek:

> transformacji systemowej w Europie i na świecie (ze szczególnym wskazaniem na Azję), która przebiegała w sposób zróżnicowany. Zmieniła ona w istotny sposób otoczenie wewnętrzne i zewnętrzne, gdzie pojawiły się wątpliwości i problemy nie tylko w skali lokalnej czy regionalnej, ale i globalnej. Można nawet przyjąć, że tempa ich rozwoju i skutków nie przewidzieli autorzy scenariusza tej polityki. W związku z tym istnieje uprawniona podstawa do zmiany poglądów i ich dostosowania do współczesnych wyzwań w kwestii bezpieczeństwa państwa, jego zagrożeń, a także gwarancji tego bezpieczeństwa[2].

Procesom tym towarzyszy widoczna współzależność między państwami – występuje silne oddziaływanie państw silnych na sytuację militarną, ekonomiczną i polityczną regionów geograficznie nawet znacznie odległych, co stanowi źródło wzajemnej podejrzliwości. Wynika ona nie tylko z faktów, lecz, w większym zapewne stopniu, z wyobrażeń i przewidywań co do zachowań innych państw na arenie międzynarodowej, przede wszystkim sąsiadów (niekoniecznie bezpośrednich) oraz mocarstw mających pośredni, ale znaczący wpływ na sytuację w polu bezpieczeństwa danego kraju[3].

---

1 A. Piskozub, *Przemiany kulturowe i cywilizacyjne w perspektywie społeczeństwa postindustrialnego i aspekty globalizacji kulturowej – uwarunkowania i wnioski*, [w:] *Polska na drodze do nowoczesnej cywilizacji*, red. J. Dąbrowski, t. 2, PAN, Warszawa 1990, s. 33.

2 A. Żebrowski, *Wywiad i kontrwywiad XXI wieku*, Wyższa Szkoła Ekonomii i Innowacji w Lublinie, Lublin 2010, s. 33.

3 S. Dworecki, *Od konfliktu do wojny*, Buwik, Warszawa 1996, s. 12.

Nietrudno dostrzec, że podstawową przyczyną zachodzących procesów jest jednak globalizacja, która stwarza szanse i zagrożenia dla przyszłości naszego globu, dla ludzkości. Szanse to przede wszystkim[4]:

1) nowe perspektywy rozwoju ekonomicznego (nie dla wszystkich);
2) wzrost znaczenia ponadpaństwowych norm prawnych i egzekwowania ich przestrzegania;
3) perspektywy nowych metod sterowania życiem publicznym w skali światowej, globalnego zarządzania – jak to się coraz częściej określa;
4) perspektywy rozwoju nowych form demokracji bezpośredniej – w szczególności rozwoju społeczeństwa obywatelskiego.

Do zagrożeń związanych z globalizacją zaliczyć można:

1) niepewność związaną z tym, czy potrafimy rozpoznać rodzące się szanse, będące wynikiem rozwoju cywilizacji informacyjnej przekraczającej granice państw i kontynentów; niepewność ta dotyczy również powstania i rozwoju organizmów ponadnarodowych oraz wzrastającej migracji ludności;
2) nasilenie się konfliktów etnicznych, ideologicznych i religijnych, ksenofobii i nietolerancji;
3) zmiany środowiska;
4) obawę, czy przyszłe społeczeństwo globalne będzie społeczeństwem ciepłym czy zimnym (w aspekcie zdolności do udziału w konfliktach i ich charakteru);
5) terroryzm.

Państwa stoją w obliczu wyzwań, które są pochodną globalnych, regionalnych i lokalnych szans i zagrożeń o zróżnicowanym podłożu. Ich cechy charakterystyczne to m.in.: źródło pochodzenia, skala i dynamika, czas, skutki i przewidywalność.

Zagrożenia militarne i pozamilitarne przybierają coraz częściej charakter pozapaństwowy i asymetryczny. Współcześnie coraz częściej już nie państwa zagrażają innym państwom, lecz procesy i zjawiska, jakie występują w zmieniających się społeczeństwach[5]. Właśnie „biedna Północ" występuje przeciwko „bogatej Północy", a systemy totalitarne przeciwko demokracji. Asymetryczność wyraża się swego rodzaju niezgodnością celów, metod lub środków działania, przyjmowanych przez obie strony potencjalnego lub realnego konfliktu[6]. Widoczna powszechna asymetryczność jest wyrazem powszechnie zauważalnego elementu towarzyszącego rozwojowi społecznemu, który w sensie globalnym jawi się w ogromnych dysproporcjach międzypaństwowych, międzyregionalnych czy wręcz coraz bardziej powszechnej asymetrii rozwoju

[4] T. Jemioło, *Globalizacja – szanse i zagrożenia*, Akademia Obrony Narodowej, Warszawa 2000, s. 14.

[5] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*, Akademia Obrony Narodowej, Warszawa 2003, s. 8.

[6] Tamże.

świata[7]. Należy podkreślić, że przemianom lat 90. ubiegłego stulecia towarzyszyło zjawisko systematycznego powiększania się potencjałów militarnych widoczne w działaniach asymetrycznych, na co wielu polityków i specjalistów nie zwracało uwagi.

Mając na uwadze sfery zagrożeń asymetrycznych, należy zawsze się liczyć z wystąpieniem nagłego ryzyka nie tylko z proliferacją, ale i użyciem broni masowego rażenia (BMR), środków do jej przenoszenia, a także technologii do jej produkcji łącznie z transferem specjalistów. Jest to jedno z najważniejszych wyzwań dla społeczności międzynarodowej.

> Mając na uwadze zarówno efekt psychologiczny, jak i fizyczny, broń masowego rażenia musi być traktowana jako potencjalna broń asymetryczna. Ponadto względna łatwość produkcji środków chemicznych i biologicznych oraz ich potencjał bojowy wpływają na wzrost możliwości ich wytwarzania przez państwa o ograniczonej infrastrukturze, a także organizacje i ugrupowania pozapaństwowe[8].

Należy również uwzględnić coraz liczniejszą grupę państw, które są bliskie wejścia w posiadanie nie tylko wspomnianej broni biologicznej czy chemicznej, ale i atomowej, m.in. przez uruchomienie własnych programów jądrowych. Jeżeli uwzględni się dążenie do wejścia w posiadanie tego rodzaju broni także przez skrajne ugrupowania polityczne, religijne, jak również przestępcze czy terrorystyczne, możliwość jej użycia wykracza poza sferę wyobraźni. Ponadto wiele państw dąży do nabycia nowoczesnych systemów broni konwencjonalnej. Starają się wykorzystać różne źródła, a dążenie do wejścia w jej posiadanie może wywołać nowe konflikty zbrojne.

Oznacza to, że asymetryczny charakter zagrożeń w połączeniu z wszechobecną globalizacją i informatyzacją społeczeństw, a przede wszystkim ich skalą, stawia społeczność międzynarodową w obliczu konieczności przeciwstawienia się tym zagrożeniom, którym towarzyszy niepewność i ryzyko.

Środowisko bezpieczeństwa międzynarodowego na początku XXI wieku charakteryzuje się różnorodnością, złożonością (nieliniowość to ogromna ilość procesów), zmiennością (dynamiczne zmiany o charakterze informacyjnym, cywilizacyjnym, kulturowym itp.), znaczną nieprzewidywalnością (turbulentność związana z dynamiką i nieliniowością procesów)[9]. Okazuje się, że tradycyjne postrzeganie granic nie ma już większego znaczenia, ponieważ są one płynne i porowate, np. granice państw członkowskich Unii Europejskiej. Za taką tezą przemawia m.in. masowe przemieszczanie się ludności z Afryki do Europy Zachodniej. W tym procesie czas uległ tzw. kompresji.

Okazuje się, że w tych złożonych warunkach ma miejsce stopniowa zmiana układu sił między cywilizacjami, co oznacza słabnącą pozycję Zachodu, które-

---

7 Tamże.

8 Tamże, s. 43.

9 M.S. Witecka, *Zagrożenia asymetryczne a technologie informacyjne*, „Zeszyt Problemowy TWO" 2011, nr 4, s. 9.

go wpływy słabną. Cywilizacje azjatyckie rosną w siłę polityczną, ekonomiczną i militarną. Natomiast cywilizacje islamu charakteryzuje demograficzna eksplozja, która jest źródłem wielu zagrożeń. Obserwujemy zjawisko zbliżania się państw podobnych kulturowo, które jednoczą się wokół państw będących ośrodkami danego kręgu cywilizacyjnego. Stanowi to poważne zagrożenie dla innych kręgów cywilizacyjnych. Widoczne są już napięcia, które występują przede wszystkim wzdłuż linii błędów i obszarów zainteresowań państw mających swoje strategiczne interesy np. w kręgu cywilizacyjnym islamu. Przykładowo, masowe migracje, konflikty religijne i etniczne czy działalność grup terrorystycznych nie mają granic terytorialnych, a często trudno zidentyfikować podmiot, któremu należałoby się przeciwstawić[10].

Wielopłaszczyznowe zmiany, jakie następują na świecie, wspomniana globalizacja, nasilanie się konfliktów o zróżnicowanym podłożu, w tym zbrojnych, w wielu państwach na Dalekim Wschodzie czy kontynencie afrykańskim, a także wzrost fundamentalizmu, fanatyzmu religijnego skutkują m.in. zwiększonym przemieszczaniem się ludności.

Powyższym procesom towarzyszy:

> degradacja moralna w rozwiniętych technologicznie społeczeństwach dobrobytu, które są obserwatorem buntu zepchniętych na margines świata, konserwatywnych, broniących moralności i wiary, zgorszonych mieszkańców muzułmańskiego Bliskiego Wschodu, podsycany przez próby naruszenia *status quo* ich świata, m.in. poprzez implementację demokratycznych i zachodnich standardów w islamskich krajach. Sprzeciw wobec *westernizacji i macdonaldyzacji* świata przybiera gwałtowne, radykalne formy. Ekstremiści i fundamentaliści wykorzystują przeciwko społeczeństwu cywilizacji zachodniej jej własne, gloryfikowane zdobycze – demokrację i rozwiniętą technikę – używając ich jako broni[11].

Sprzeciw w zachodnim kręgu cywilizacyjnym przyjmuje różne formy, w tym najbardziej skrajne, z użyciem przemocy włącznie (np. terroryzm, cyberterroryzm).

Znamiennym zjawiskiem wśród społeczeństw rozwiniętych jest to, że jednostki nieodnajdujące się we współczesnym świecie w poszukiwaniu wartości zwracają się ku islamowi, gdzie odnajdują niezmienną od wieków tradycję, konserwatywną moralność oraz siłę, która pozwala na przeciwstawianie się oszalałemu zachodniemu światu[12].

Masowe migracje m.in. oznaczają, że „świat się skurczył", a konglomerat mniejszości narodowych i grup etnicznych różniących się kulturą, językiem, religią, stanem posiadania stanowi problem dla zachodniego środowiska bezpieczeństwa międzynarodowego. Wspominane grupy w pewnych okolicznościach stanowią bazę ekspansji politycznej (w tym wrogich idei), gospodar-

[10] M. Kozub, *Strategiczne środowisko bezpieczeństwa w pierwszych latach XXI wieku*, Akademia Obrony Narodowej, Warszawa 2009, s. 128.

[11] M.S. Witecka, *Zagrożenia asymetryczne*..., s. 45.

[12] Tamże.

czej i kulturowej. Mogą być także kartą przetargową w rozmowach między państwami, stanowić nieocenione dobro, ale i źródło zagrożeń dla bezpieczeństwa państwa pobytu spowodowane m.in. działalnością terrorystyczną, czy też zorganizowanych grup przestępczych. Niejednokrotnie stanowią tzw. bombę z opóźnionym zapłonem. Przykładowo, powstanie i aktywność zbrojna Państwa Islamskiego stanowi poważne zagrożenie dla regionu, a także innych państw będących jego przeciwnikami.

Tym procesom towarzyszy terroryzm. To jedno z kluczowych zagrożeń m.in. na gruncie społeczno-kulturowym. Obecne ataki terrorystyczne kierowane są na przypadkowe ofiary – najczęściej ludność cywilną. Powiązania istniejące między organizacjami terrorystycznymi reprezentującymi różne ideologie czy wyznania religijne ulegają umiędzynarodowieniu, co stanowi wyzwanie dla globalnej społeczności żyjącej w permanentnym zagrożeniu.

Terroryści w swojej działalności wykorzystują obecną sytuację międzynarodową, trwającą konfrontację polityczną, ideologiczną, religijną, gospodarczą i militarną między państwami. Ponadto wykorzystują tzw. zderzenie cywilizacji, gdzie świat Zachodu i islamu są uczestnikami kooperacji negatywnej. Radykalni islamiści oferują swym współwyznawcom udział w wyimaginowanej walce w imię religii[13], która dla terrorystów zaczęła stanowić hasło usprawiedliwiające wszelkie działania i do nich nawołujące[14]. Terroryzm ma międzynarodowy wymiar i wpisuje się w globalne zagrożenie, z którym coraz trudniej walczyć.

Przewartościowania, jakie zachodzą w środowisku bezpieczeństwa narodowego i międzynarodowego, mają poważny wpływ na zmiany w następujących obszarach[15]:

1) interesach podmiotu narodowego i międzynarodowego oraz wynikające z nich cele strategiczne i operacyjne w dziedzinie bezpieczeństwa;
2) warunkach bezpieczeństwa, czyli szans i zagrożeń dla realizacji interesów oraz osiągania celów w dziedzinie bezpieczeństwa; te ostatnie występują w formie zjawisk określanych kryzysami i konfliktami;
3) strategicznych (długofalowych) i operacyjnych (bieżących) koncepcjach (zasadach i sposobach) działań zmierzających do osiągnięcia przyjętych celów w danych warunkach;
4) systemach bezpieczeństwa, czyli zasobach podmiotów wydzielonych do realizacji przyjętych koncepcji i zadań, odpowiednio do zadań zorganizowanych i przygotowanych.

Każde państwo funkcjonuje w określonym środowisku bezpieczeństwa międzynarodowego, które jest źródłem wspomnianych szans i zagrożeń prze-

[13] S. Simon, *Islam i Zachód – kurs na zderzenie*, „Newsweek Polska" 2005, nr 3, s. 66–68.

[14] *Encyklopedia terroryzmu*, Bellona, Warszawa 2004, s. 212.

[15] S. Koziej, *Współczesne problemy bezpieczeństwa międzynarodowego i narodowego* (*studium analityczne*), PWSBiA, Warszawa 2003, s. 9.

kładających się na jego bezpieczeństwo wewnętrzne. Oznacza to, że państwo w procesie realizacji swoich funkcji musi uwzględniać[16]:

1) swoje otoczenie zewnętrzne, tj. położenie geopolityczne i charakter stosunków z państwami sąsiednimi oraz zasady postępowania regulujące stosunki między państwami;
2) ustrój państwa, tj. zbiór zasad postępowania regulujących działanie i współdziałanie struktur państwowych, ich wewnętrzną spójność i skuteczność;
3) swoje otoczenie wewnętrzne, tj. poziom rozwoju i stan gospodarki, kulturę polityczną społeczeństwa oraz cechy demograficzne.

Występujące między powyższymi czynnikami ścisłe relacje i wzajemne przenikanie wymagają kompleksowego spojrzenia na problemy bezpieczeństwa i podmioty uprawnione do jego budowania w celu stanowienia silnego i niepodległego państwa, zdolnego do skutecznej ochrony swojej suwerenności oraz bezpieczeństwa obywateli[17].

Bezpieczeństwo narodowe i międzynarodowe ulega ciągłym przewartościowaniom, z czym wiąże się jego różnorodność, co sprawia, że nabiera szczególnego znaczenia. Dominacja przede wszystkim bezpieczeństwa sektorowego, w tym: gospodarczego, energetycznego, ekologicznego, informacyjnego, infrastruktury krytycznej państwa, dostępu do zasobów naturalnych, naukowo-technicznego, społecznego, oznacza konieczność szerszego spojrzenia nie tylko na bezpieczeństwo wewnętrzne, ale i międzynarodowe. Ta swoista współzależność wymaga ze strony państw, a także organizacji międzynarodowych (powszechnych i regionalnych) podejmowania wielu wzajemnie ze sobą powiązanych przedsięwzięć, które powinny być ukierunkowane na minimalizowanie negatywnych zjawisk.

Informacja

Nieprzewidywalność i złożoność środowiska bezpieczeństwa międzynarodowego wymusza na państwach i organizacjach międzynarodowych gotowość do podejmowania działań pozwalających na eliminowanie/wykluczenie występujących zagrożeń dla bezpieczeństwa państw, regionów, a nawet świata. Tym samym państwa i organizacje międzynarodowe muszą wypracować, doskonalić i modyfikować mechanizmy, które pozwolą na skuteczne działanie w złożonych i zmieniających się warunkach. Realizacja celów przyjętych w sferze bezpieczeństwa przez państwo czy organizację międzynarodową wymaga dostępu do zasobów osobowych, rzeczowych, finansowych i informacyjnych.

Ponadto w dobie rozwoju społeczeństwa informacyjnego, uważanego niekiedy za cybernetyczne, którego nieodłącznym atrybutem są technologie infor-

[16] S. Dworecki, *Od konfliktu*..., s. 10.
[17] A. Żebrowski, *Wywiad i kontrwywiad*..., s. 34.

macyjne, państwa muszą je adaptować dla potrzeb bezpieczeństwa wewnętrznego i zewnętrznego. Technologie informacyjne obejmują telekomunikację, narzędzia i inne technologie związane z informacją, służące pozyskiwaniu, selekcjonowaniu, analizowaniu, przetwarzaniu, zarządzaniu i przekazywaniu informacji przy użyciu, w szczególności, sprzętu komputerowego i oprogramowania w dowolnym miejscu i w dowolnym czasie[18]. Należy mieć także na uwadze bezpieczeństwo informacyjne (w tym osobowe, przemysłowe) i bezpieczeństwo teleinformatyczne (w tym systemów i sieci teleinformatycznych).

Okazuje się, że rozwój technologii informacyjnych ma ścisły związek z bezpieczeństwem państwa, które z uwagi na tzw. usieciowienie podatne jest na atak i zakłócanie informacyjne ze strony przeciwnika. Bezpieczeństwo technologii informacyjno-komunikacyjnych i cyberprzestrzeni w coraz większym stopniu determinuje bezpieczeństwo państwa. W związku z tym zapewnienie bezpieczeństwa cyberprzestrzeni państwa powinno stanowić kluczowe zadanie. Zdobywanie informacji w osobowej i technicznej przestrzeni informacyjnej, odpowiednio zabezpieczone pod względem osobowym i technicznym, ma wpływ na proces decyzyjny i wykonawstwo zadań na wszystkich poziomach zarządzania bezpieczeństwem państwa.

Dla procesu decyzyjnego kluczowe znaczenie mają zasoby informacyjne. Takie podejście uzasadnia zmieniające się otoczenie wewnętrzne i zewnętrzne państwa, które nierozpoznane lub rozpoznane zbyt późno nie pozwala lub utrudnia dostosowanie się do nowych warunków. Natomiast otoczenie rozpoznane (np. z wyprzedzeniem, co jest niezmiernie trudne) powala na uwzględnienie występujących zmian.

Oznacza to, że skuteczne kierowanie bezpieczeństwem państwa zależy od posiadanych informacji[19], które pozwalają na poznanie zmian zachodzących w otoczeniu wewnętrznym i zewnętrznym (bliższym i dalszym) państwa. Ważne są również koncepcje, metody i motywacja, wiedza i wyobraźnia, a także czas na przemyślenia. Pozwala to odpowiednio wcześniej dostosować posiadany potencjał i przyszłe możliwości państwa. Dostęp do wiedzy i zasobów informacyjnych, umożliwiających wczesną weryfikację zagrożeń lub reakcję na już zaistniałe, jest dla systemu bezpieczeństwa państwa sprawą priorytetową[20]. Należy mieć na uwadze to, że bez znajomości otoczenia wewnętrznego i zewnętrznego państwa, a także zachodzących tam zmian, które są źródłem

[18] Technologie informacyjne (online), za: M.S. Witecka, *Zagrożenia asymetryczne*..., s. 37.

[19] Informacja jest elementem wiedzy, faktem, wiadomością, komunikatem lub wskazówką gromadzoną, komunikowaną lub przekazywaną komuś za pomocą jakiegoś kodu lub języka. Każda informacja, aby stanowiła wartość dla podmiotu kierującego, powinna być pełna i wyczerpująca. Poza treścią powinna zawierać w swoim składzie elementy pozwalające na jej identyfikację i ochronę, tzn.: czas nadania, czas odbioru, temat, nadawcę, odbiorcę, status (niesklasyfikowana, zastrzeżona, poufna, tajna, ściśle tajna), zob. A. Barczak, T. Sydoruk, *Bezpieczeństwo systemów informatycznych*, Akademia Podlaska, Siedlce 2002, s. 22.

[20] R. Kwećka, *Procesy informacyjne w ramach systemu reagowania kryzysowego Unii Europejskiej*, [w:] *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, red. J. Gryz, Wydawnictwo Adam Marszałek, Toruń 2009, s. 336.

szans i zagrożeń, trudno jest sporządzać scenariusze, redukować niepewność działania, podejmować właściwe decyzje, wskazywać możliwe koncepcje rozwoju, a przede wszystkim budować strategie, dla których rozpoznanie zagrożeń i szans w otoczeniu, a także słabych i mocnych stron państwa stanowią bazy danych. Dlatego posiadanie odpowiednich informacji jest dzisiaj dla każdego kierującego (dowodzącego) sprawą o kluczowym znaczeniu.

Przemiany cywilizacyjne, będące źródłem zarówno postępu, jak i zagrożeń, powodują, że współcześnie informacja decyduje o sposobie wykorzystania przez państwo (organizację międzynarodową) posiadanych zasobów i możliwości, zdolności dostosowania się do nowych warunków i programowania swojego rozwoju w procesie poprzedzającym wystąpienie np. sytuacji kryzysowej.

Każdy podmiot wykonujący zadania w sferze bezpieczeństwa i obronności państwa powinien znać swoje potrzeby informacyjne i wiedzieć, jakie informacje są potrzebne do tworzenia planów, gromadzenia zasobów i wykonywania podstawowych funkcji i działań. Powinien także określić, jakie potrzeby informacyjne są zaspokajane w niedostatecznym stopniu, a jakie nie są w ogóle zaspokajane, a także, w jakim stopniu przepływ informacji służy zarządzającym w procesie podejmowania decyzji i sprawnego kierowania[21].

Skala i dynamika zmian, jakie występują w otoczeniu wewnętrznym i zewnętrznym (bliższym i dalszym) państwa oraz towarzyszące im zagrożenia naturalne i celowe, wymagają dostępu do szerokiego spektrum informacji. Potrzeby informacyjne wynikają z istnienia luki informacyjnej, która jest zawsze odnoszona do konkretnego obserwatora. Ponadto jest ona wrażliwa na czynnik czasu, który w asymetrycznym środowisku międzynarodowym, skali i dynamice występujących zagrożeń, gdzie nieprzewidywalność i chaos dają o sobie znać, ma kluczowe znaczenie dla skutecznego kierowania bezpieczeństwem państwa. Na zakres i strukturę luki informacyjnej oddziałują czynniki obiektywne oraz subiektywne[22]. Pierwsze z nich mają ścisły związek z obiektywną wiedzą podmiotów zarządzających i dotyczą celowości prowadzonych obserwacji środowiska podatnego na zagrożenia oraz możliwością realizacji takiej obserwacji w ramach zarządzania kryzysowego. Dlatego przeprowadzenie obserwacji i stopień jej kompletności oraz osiągniętej przydatności jest najczęściej kompromisem między oczekiwaniami a możliwościami ich realizacji[23]. Z kolei czynniki subiektywne związane są z tym, że luka informacyjna jest zawsze czyjaś, a więc adresowana do konkretnego obserwatora[24], który powinien dążyć do jej zminimalizowania.

---

21 J. Penc, *Zarządzanie dla przyszłości. Twórcze kierowanie firmą*, Profesjonalna Szkoła Biznesu, Kraków 1998, s. 107.

22 W. Flakiewicz, *Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje*, Wydawnictwo C.H. Beck, Warszawa 2002, s. 31.

23 Tamże.

24 Tamże.

Należy mieć także na uwadze szczególny rodzaj zagrożenia dla informacji, którym jest człowiek i wspomniana technika teleinformacyjna i komunikacyjna, i występuje powszechne uzależnienie nie tylko pojedynczego człowieka, narodu czy państwa od technologii informacyjnych generujących jakościowo nowe zakłócenia dla prawidłowego przepływu informacji.

Pozyskiwanie informacji, sposoby ich zbierania, gromadzenia i przepływu powinny być zorganizowane na zasadzie systemu, który obejmowałby całe zbiory informacyjne (zasoby informacyjne) oraz te elementy, które umożliwiają zasilanie, nabywanie i dostarczanie użytkownikom tych zasobów[25].

System informacyjny stanowi uporządkowany układ nadawania i odbioru informacji, czyli formalne kanały komunikacji umożliwiające przepływ – przekaz – odbiór wiadomości, poleceń, rozkazów, zadań, obowiązków itd.[26] Trudno bowiem wyobrazić sobie sprawne i skuteczne kierowanie bezpieczeństwem państwa (w tym dowodzenia wojskiem) bez możliwości wymiany informacji między uprawnionymi podmiotami, w tym wykorzystania techniki teleinformatycznej. System informacji należy uznać za system nerwowy kierowania bezpieczeństwem państwa na wszystkich jego poziomach (dowodzenia wojskiem), za pośrednictwem którego utrzymuje się porządek we wzajemnych relacjach służbowych.

> System taki, zwany systemem informacji, powinien być rozumiany nowocześnie, tzn. jako komputerowa metoda zbierania, opracowywania, przechowywania, kodowania, dekodowania, aktualizowania, odtwarzania i przetwarzania danych oraz ich dostarczania w najprzydatniejszej formie kadrze kierowniczej do realizacji zadań i celów organizacji [państwa, organizacji międzynarodowej – przyp. autora][27].

Warunki, jakim powinien odpowiadać system informacji:

1. System powinien być dostosowany do potrzeb bezpieczeństwa państwa i obejmować wszystkie jego obszary, wszystkie poziomy kierowania i poziomy decyzyjne.
2. System powinien dostarczać informacji kompleksowych i aktualnych, aby państwo reagowało na zmianę warunków wewnętrznych i zewnętrznych.
3. System powinien dostarczać informacji tym, którzy ich rzeczywiście potrzebują, i to informacji w formie nadającej się bezpośrednio (bez przetwarzania) do użytku i najdogodniejszej dla podjęcia ostatecznych decyzji.
4. System powinien zapewnić efektywne wykorzystanie informacji, które jest uwarunkowane szybkością i częstotliwością ich obiegu – oznacza to, że dane powinny być aktualne, kompletne i odpowiednio posegregowane, gdyż to ułatwia ich obieg.
5. Droga przepływu informacji powinna być możliwie najkrótsza i zgodna ze strukturą organizacyjną państwa, województwa, powiatu i gminy, a po-

[25] J. Kisielnicki, *Informatyczna infrastruktura zarządzania*, Placet, Warszawa 1992, s. 15.

[26] L. Zbiegień-Maciąg, W. Pawnik, *Zarządzanie organizacją. Aspekt socjologiczny*, Wydawnictwo AGH, Kraków 1998, s. 15.

[27] J. Penc, *Zarządzanie dla przyszłości…*, s. 115–116.

szczególne podsystemy informacji powinny stanowić proste zbiory, które można sobie szybko przyswoić i wykorzystać w podejmowaniu praktycznych decyzji (sensowne, zwięzłe raporty).
6. Algorytmy opracowania informacji powinny zapewnić śledzenie przebiegu procesów kierowania (dowodzenia), konstruowanie ocen, prognozowanie przebiegu wydarzeń.
7. Koszty pozyskiwania i przetwarzania informacji nie powinny być wysokie, a metody ich zbierania, opracowywania, przechowywania i przepływu – uwzględniać możliwości komputeryzacji systemu informacyjnego, zaś forma ich prezentacji powinna być dostosowana do możliwości odczytywania przez zainteresowanych.
8. System powinien być zabezpieczony przed niepożądanym wpływem informacji nieformalnych i stale doskonalony, aby mógł zapewnić właściwy przepływ informacji[28].

> System informacyjny powinien być tak skonstruowany, aby wszystkim szczeblom decyzyjnym zapewniał dopływ informacji odpowiednich pod względem treści i w odpowiednim czasie. Powinien on zatem gwarantować ich przepływ przez wszystkie kanały informacyjne wiążące sobą zasoby i informacje o istniejących możliwościach i ograniczeniach[29].

System informacyjny w kierowaniu państwem czy dowodzeniu wojskami musi być spójny nie tylko wewnętrznie, ale również kompatybilny z analogicznymi systemami działającymi na poziomie Unii Europejskiej i Sojuszu Północnoatlantyckiego, a także umów bilateralnych.

System informacyjny powinien opierać się na rozbudowanej infrastrukturze informacyjnej uwzględniającej sieć wewnętrzną i zewnętrzną łączącą uprawnione podmioty uczestniczące w kierowaniu (dowodzeniu) bezpieczeństwem państwa. Sieć wewnętrzna powinna być zorganizowana na zasadzie tzw. mapy informacyjnej zmieniającej się z biegiem czasu pod wpływem zmian otoczenia państwa. Taka mapa musi zawierać węzły informacyjne (składające się z grup pracowników, dokumentów, wyszukiwania danych i komunikowania) oraz linie przepływu informacji między węzłami, ustalane zgodnie z wymaganiami tzw. odwróconej piramidy informacyjnej, która oznacza, że tam, gdzie koncentruje się władza, potrzebne są informacje mniej szczegółowe, a bardziej skondensowane, o szerokim przekroju, dające pogląd na całość działania organizacji i jej powiązania z otoczeniem, ułatwiające zintegrowane kierowanie (dowodzenie) bezpieczeństwem państwa[30]. Oznacza to, że system informacyjny powinien zawierać informacje uszeregowane według pewnej hierarchii, a mianowicie dla celów strategicznych, operacyjnych i taktycznych.

---

[28] Tamże, s. 116.

[29] Tamże, s. 118.

[30] J. Ingalls, *Human Energy*, Addison–Wesley Publishing Company, Menlo Park 1976, s. 113.

Przynależność Polski do NATO i Unii Europejskiej oznacza, że obok narodowych wyspecjalizowanych systemów informacyjnych korzystamy również z systemów znajdujących się w dyspozycji wskazanych organizacji.

> Dla zarządzania bezpieczeństwem i obronnością państwa (dowodzenia wojskami) istotnymi źródłami informacji są służby wywiadowcze i kontrwywiadowcze państw członkowskich Unii Europejskiej i Sojuszu Północnoatlantyckiego. Z uwagi na to, że na poziomie tych organizacji nie ma ponadnarodowych służb wywiadowczych i kontrwywiadowczych z uprawnieniami do prowadzenia pracy operacyjnej, dlatego tak ważna jest współpraca i koordynacja pracy narodowych służb tego charakteru państw członkowskich Unii i NATO. Na podstawie informacji otrzymywanych od służb wywiadowczych państw członkowskich opracowywane są informacje o charakterze niejawnym, które są przekazywane dla uprawnionych podmiotów Unii Europejskiej, Sojuszu Północnoatlantyckiego i poszczególnych państw członkowskich. W NATO obowiązuje centralna ocena informacji wywiadowczych i centralne określanie zadań, natomiast wykonanie tych zadań leży w kompetencji wywiadów poszczególnych państw[31].

Służby wywiadowcze państw członkowskich Unii i NATO posiadają również dostęp do informacji wywiadowczych zdobywanych za pośrednictwem wywiadu satelitarnego, który jest prowadzony przez nieliczne państwa członkowskie Sojuszu Północnoatlantyckiego, jak: Stany Zjednoczone, Kanada, Wielka Brytania, RFN, Hiszpania, Włochy, a także Centrum Satelitarne Unii Europejskiej.

Wiele systemów informacji wspierających działalność państw członkowskich Sojuszu Północnoatlantyckiego ma charakter niejawny z uwagi na realizowane zadania. Zabezpieczają one potrzeby instytucji sojuszu, a także państw członkowskich.

Charakter polityczny i finansowo-gospodarczy Unii Europejskiej uzasadnia posiadanie sektorowych systemów informacyjnych, które zasilają w informacje ogólne i wyspecjalizowane jednostki i komórki organizacyjne UE, a także uprawnione podmioty państw członkowskich. Tym samym istniejące systemy wspomagają procesy decyzyjne instytucji unijnych, państw członkowskich oraz jednostek organizacyjnych Sojuszu Północnoatlantyckiego. Przykładem jest informacyjne wsparcie o charakterze wywiadowczym i kontrwywiadowczym, a także w trakcie przygotowywania i prowadzenia misji humanitarnych z mandatu NATO czy UE. Systemy te wymagają regularnego zasilania w określone informacje i współpracy organów Unii i uprawnionych podmiotów państw członkowskich w zakresie wymiany informacji.

Systemy informacyjne Unii Europejskiej – systemy powiadamiania i alarmowania:

1. Globalny Monitoring dla Środowiska i Bezpieczeństwa (GMES).
2. Rozpoznanie geoprzestrzenne (GEOIN).

---

[31] A. Żebrowski, *Zarządzanie kryzysowe elementem bezpieczeństwa Rzeczypospolitej Polskiej*, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2012, s. 121.

3. Europejska Agencja Kosmiczna (ESA).
4. Instytut Unii Europejskiej Studiów nad Bezpieczeństwem (ISS).
5. System Wczesnego Ostrzegania i Alarmowania (EWRS).
6. System Wczesnego Powiadamiania i Wymiany Informacji o Zagrożeniach Radiologicznych bądź Nuklearnych (ECURIE).
7. System Ochrony Sieci Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej (CIWIN).
8. Bezpieczny Ogólny System Szybkiego Ostrzegania (ARGUS).
9. System Wczesnego Ostrzegania przed Biologiczno-Chemicznymi Atakami i Zagrożeniami (RAS – BICHAT).
10. System Informacyjny (EIS – EUROPOL-u).
11. System Ostrzegania przed Wadliwymi Produktami (RAPEX).
12. System Szybkiego Ostrzegania o Niebezpiecznych Produktach Żywnościowych (RASFF).
13. Zintegrowany i Skomputeryzowany System Weterynaryjny (TARCES).
14. Europejski System Wczesnego Powiadamiania i Wymiany Informacji o Zdrowiu Roślin (EUROPHYT).
15. System Zgłaszania Chorób Zwierząt (ADNS).
16. Centrum Monitoringu i Informacji (MIC).
17. Sieć osób zawodowo zajmujących się sprawami azylowymi (EURASIL).
18. Bezpieczna internetowa sieć informowania i koordynacji dla służb imigracyjnych państw członkowskich (ICONet).
19. Sieć Migracyjna (ESM).
20. Mechanizm wymiany informacji dotyczących środków państw członkowskich w obszarze azylu i migracji.
21. Europejska Sieć Umacniania Prawodawstwa (LEN).
22. System Informacyjny Schengen (SIS).
23. Wizowy System Informacyjny (VIS).
24. System Automatycznej Identyfikacji Odcisków Palców (Prüm AFIS).
25. Baza danych (Prüm DNA).
26. Europejska Sieć Informacji o Narkotykach i Narkomanii (REITOX).
27. System Informacji Celnej na poziomie Wspólnotowym (CIS).
28. Baza danych IRENE utworzona przez Urząd Zwalczania Nadużyć Finansowych (OLAF).
29. Wspólnotowy System Ochrony Własności Intelektualnej (COPIS)[32].

Przedstawione systemy informacyjne oznaczają, że Unia Europejska monitoruje obszary istotne dla bezpieczeństwa wewnętrznego Unii i państw członkowskich.

Kierowanie bezpieczeństwem państwa (dowodzenie wojskami) wymaga monitorowania miejsc o podwyższonym ryzyku przez uprawnione podmioty, w tym służby specjalne. Monitorowanie oznacza systematyczną kontrolę

[32] *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, red. J. Gryz, Toruń 2009.

otoczenia bliższego i dalszego, ujawnianie pojawiających się zmian mających wpływ na funkcjonowanie państwa (organizacji międzynarodowych, sojuszników) oraz przekazywanie informacji o nich uprawnionym podmiotom zarządzającym w celu wykorzystania ich w planowaniu średnio- i długookresowym. Zadaniem tego monitoringu, zwanego często strategicznym, jest dostarczanie podmiotom uczestniczącym w kierowaniu (dowodzeniu) bezpieczeństwem państwa informacji umożliwiających realizację trzech rodzajów celów: defensywnych, pasywnych i ofensywnych[33].

> System monitoringu nieustannie śledzi i rozpoznaje sytuacje w aspekcie zagrożeń mogących prowadzić do zakłócania aktualnego stanu bezpieczeństwa państwa. Procedurę tę realizuje się w czasie rzeczywistym, pod kątem natychmiastowego uruchomienia czynności przeciwdziałania kryzysowego[34].

Warto mieć świadomość tego, że jeżeli w procesie prowadzonego monitoringu nie nastąpi wskazanie i rozpoznanie zagrożenia, to np. system zarządzania kryzysowego nie zostanie uruchomiony. Również w sytuacji, gdy zagrożenie nie zostanie rozpoznane w odpowiednim czasie, system alarmowy także nie zostanie uruchomiony, a w konsekwencji nie zostaną wprowadzone siły i środki niezbędne dla bezpieczeństwa państw.

Proces identyfikacji i diagnozowania zagrożeń przez system monitoringu można wyrazić za pomocą następującego ciągu czynności:

1. Cykliczne przeszukiwanie zadanej przestrzeni stanów systemowych na przykład za pomocą inteligentnych sensorów, w celu rozpoznania ewentualnego zagrożenia. Im krótszy jest okres między poszczególnymi cyklami identyfikacji, tym wyższa jest sprawność danego systemu monitoringu.
2. W przypadku zidentyfikowania i zaklasyfikowania danego zdarzenia jako potencjalne zagrożenie uruchamiany jest program jego szczegółowej oceny, celem postawienia hipotetycznej diagnozy co do stopnia i skali powstałego niebezpieczeństwa.
3. Stopień generowania niebezpieczeństwa jest dodatkowo weryfikowany w odniesieniu do aktualnej sytuacji i rzeczywistych uwarunkowań. Każde zagrożenie musi być odniesione do szerokiego spektrum warunków sytuacyjnych, ograniczeń czasoprzestrzennych i realnych możliwości skutecznego reagowania.
4. Wszystkie nadchodzące i diagnozowane zagrożenia muszą być relatywizowane względem innych, aktualnie zaistniałych i badanych, zdarzeń krytycznych. Chodzi o to, aby jednoznacznie zidentyfikować największe w danej chwili zagrożenia i nadać im najwyższy priorytet obsługi (reagowania). Jednym z lepszych kryteriów diagnozowania zagrożeń jest zapew-

[33] J. Penc, *Zarządzanie dla przyszłości*…, s. 131–132.

[34] K. Ficoń, *Inżynieria zarządzania kryzysowego. Podejście systemowe*, PWN, Warszawa 2007, s. 251.

ne kryterium oparte na szacowaniu stopnia ryzyka związanego z zaistniałym zagrożeniem.

5. Rezultatem działania systemu monitoringu jest przygotowanie danych źródłowych do podjęcia decyzji o uruchomieniu kolejnych procedur reagowania (zarządzania) kryzysowego. Hierarchicznie uporządkowany zbiór dopuszczalnych decyzji dotyczących aktualnej sytuacji kryzysowej powinien być podstawą podjęcia ostatecznej decyzji, optymalnej na przykład ze względu na poziom ryzyka lub możliwości wykonawcze systemu zarządzania kryzysowego.
6. Identyfikacja pojawiających się zagrożeń jest procesem ciągłym i dlatego system monitoringu musi działać bardzo sprawnie, szybko i jednoznacznie. Identyfikacja musi zakończyć się precyzyjną diagnozą stopnia niebezpieczeństwa albo poziomu stworzonego ryzyka jako następstwo realizacji danego zagrożenia[35].

System monitoringu jest systemem wczesnego ostrzegania i alarmowania przed zagrożeniami. Pozwala on na obserwowanie ważnych dla państwa (sojuszników) dziedzin życia w celu poznania pojawiających się symptomów zagrożeń oraz dostrzeganie zjawisk, dzięki którym możliwe będzie wykorzystanie posiadanych zasobów, jak również reakcja na zagrożenia. System wczesnego ostrzegania dostarcza podmiotom uczestniczącym w kierowaniu (dowodzeniu) bezpieczeństwem państwa różnych użytecznych informacji o zjawiskach i procesach oraz prawdopodobieństwie ich wystąpienia i rozwoju. Dzięki temu umożliwia im w miarę szybkie, elastyczne reagowanie na nadciągające zmiany oraz podejmowanie działań modyfikujących ich przebieg, a w konsekwencji przystosowanie do nowych wymagań otoczenia[36].

> System monitoringu należy traktować jako system alarmowania, który służy do przekazywania dla określonego zespołu ludzi bądź pojedynczych osób [...] sygnału (znaku umownego) do wykonania ustalonego wcześniej polecenia, zarządzenia, rozkazu nakazującego natychmiastowe przejście do określonego działania, zwykle w wypadku grożącego niebezpieczeństwa napadu (powietrznego, jądrowego, chemicznego) ze strony nieprzyjaciela[37].

System ten obejmuje również państwa członkowskie Unii Europejskiej, Sojuszu Północnoatlantyckiego i państwa trzecie.

Skala, dynamika i skutki zagrożeń naturalnych i celowych, a także ich umiędzynarodowienie powodują, że pojedyncze państwa nie są w stanie im zapobiegać. Wymaga to zaangażowania całej społeczności międzynarodowej, w tym także organizacji międzynarodowych zarówno powszechnych, jak i regionalnych.

Oznacza to konieczność zbudowania jakościowo nowych narzędzi, które pozwolą na skuteczne zarządzanie, w tym także koordynowanie działań

---

35 Tamże, s. 252.

36 J. Penc, *Zarządzanie dla przyszłości*..., s. 135.

37 *Leksykon wiedzy wojskowej*, t. 1, red. M. Laprus, MON, Warszawa 1973, s. 13.

np. w sytuacjach kryzysowych o charakterze wielosektorowym. Wymaga to stworzenia systemu monitorowania miejsc o podwyższonym ryzyku, co powinno przekładać się na system powiadamiania i alarmowania na poziomie Unii Europejskiej oraz Sojuszu Północnoatlantyckiego i państw członkowskich. Przyjęcie właściwego systemu monitorowania i wizualizacji w czasie rzeczywistym sytuacji kryzysowych w państwach członkowskich Unii Europejskiej oraz NATO, a także w ich bliższym i dalszym otoczeniu niewątpliwie przyczyni się do zbudowania skutecznego systemu szybkiego reagowania przy uwzględnieniu posiadanych sił i środków.

Unia Europejska i NATO, uwzględniając zaangażowanie polityczne, ekonomiczne i wojskowe w środowisku międzynarodowym, wzrastające zagrożenia (naturalne i celowe), konieczność zapewnienia bezpieczeństwa państwom członkowskim Unii oraz NATO i jej obywatelom, zbudowały złożony system monitorowania, powiadamiania i alarmowania obejmujący zróżnicowane obszary swojej działalności. Jest to proces, w ramach którego trwa doskonalenie już istniejących systemów, a także trwają prace nad uruchomieniem nowych, co wynika m.in. ze skali i dynamiki zagrożeń asymetrycznych.

Proces zdobywania, gromadzenia, przetwarzania i dystrybucji danych powinien być realizowany i doskonalony w czasie poprzedzającym wystąpienie określonego zagrożenia.

Skuteczna reakcja na zagrożenia dla bezpieczeństwa państwa lub Sojuszu wymaga uwzględnienia następujących elementów:

1) określenia przez uprawnione podmioty cywilne i wojskowe potrzeb informacyjnych;
2) wskazania i postawienia zadań podmiotom cywilnym i wojskowym uprawnionym do zdobywania informacji;
3) zrozumienia zjawisk i zdarzeń występujących w otoczeniu zewnętrznym i wewnętrznym państwa;
4) wypracowania decyzji;
5) reakcji na występujące zjawiska i zdarzenia.

Państwo dysponuje wyspecjalizowanymi podmiotami, które zabezpieczają jego potrzeby informacyjne zarówno z otoczenia wewnętrznego, jak i zewnętrznego (bliższego i dalszego).

Służby specjalne

Skuteczne kierowanie bezpieczeństwem państwa (dowodzenie wojskami) wymaga dostępu do informacji o zjawiskach i zdarzeniach występujących zarówno w jego otoczeniu wewnętrznym, jak i zewnętrznym. Specyfika systemu decyzyjnego związana z kierowaniem (dowodzeniem) na poziomie państwa obejmuje wiele elementów, wśród których na uwagę zasługują[38]:

[38] G. Rydlewski, *Rządowy system decyzyjny w Polsce*, Elipsa, Warszawa 2002, s. 32–33.

1) złożony charakter, jaki można przypisać procesowi decyzyjnemu, który obejmuje etapy inicjatyw, ich analizy i selekcji, przekształcenia w projekty, wyjaśnianie i rozstrzyganie sporów, ocenę prawną, rozstrzygnięcia podmiotów decyzyjnych na wszystkich poziomach zarządzania kryzysowego w państwie;
2) usytuowanie decydenta w systemie politycznym i prawnym;
3) relacje z otoczeniem, kiedy decyzje są podejmowane w warunkach niepewności.

Obok służby dyplomatycznej informacje dostarczają: rozpoznanie sił zbrojnych i rodzajów wojsk, służby wywiadu i kontrwywiadu wojskowego i cywilnego, służby antykorupcyjne, służby ochrony granic i celne, służby wywiadu finansowego, policja, żandarmeria wojskowa, wywiad elektroniczny i radiokontrwywiad, służby do walki z narkotykami, służby do walki z przestępczością zorganizowaną. Podmioty te z uwagi na realizowane zadania, każdy w zakresie swojej właściwości, posiadają możliwości prowadzenia czynności operacyjno-rozpoznawczych.

Dla swobodnego poruszania się w międzynarodowej przestrzeni bezpieczeństwa każdego państwa szczególne znaczenie mają informacje niejawne, chronione przez podmioty państwowe, jak i pozapaństwowe. Dominującą pozycję w systemie ich zdobywania zajmują wyspecjalizowane podmioty, jakimi są służby specjalne, które z uwagi na posiadany potencjał osobowy i pozaosobowy są w stanie wejść w posiadanie informacji tego charakteru.

> Instytucja służb specjalnych, ukształtowana w poszczególnych państwach w warunkach odrębności, będąca cząstką ich historii i swoistym, tajnym dziedzictwem, zawsze była i pozostanie odmienna w każdym państwie. W związku z tym nie ma uniwersalnego modelu strukturalno-funkcjonalnego służb specjalnych, który nadawałby się do udanej adaptacji w różnych państwach. Dynamika zagrożeń dla państwa i związana z nią elastyczność reagowania służb specjalnych (poprzez odpowiednie rozłożenia punktów ciężkości pracy operacyjnej) powoduje konieczność dostosowania, a niekiedy zmian struktur organizacyjnych tych służb w celu zwiększenia skuteczności ich działania. W bardzo rzadkich przypadkach powoływane są nowe służby państwowe uprawnione do prowadzenia pracy operacyjnej w celu zwalczania ograniczonej, ale uznanej za nadzwyczaj groźną dla funkcjonowania państwa, grupy zagrożeń – przestępstw (np. korupcji w życiu publicznym)[39].

Służby specjalne są tajnymi, cywilnymi i wojskowymi agendami państwowymi, uprawnionymi do realizacji zadań związanych z wewnętrzną i zewnętrzną ochroną interesów państwa.

Szczególną rolę cywilnych i wojskowych służb specjalnych w rozpoznawaniu i neutralizowaniu zagrożeń globalnych należy traktować jako ogólną prawidłowość, dotyczącą zdecydowanej większości współczesnych służb spe-

[39] B. Libera, *Podstawy wiedzy o służbach specjalnych*, [w:] *Urzędnik i biznesmen w środowisku międzynarodowym. Wybrane aspekty pragmatyki zawodowej*, red. J. Barcz, B. Libera, Wydawnictwo ABC–Wolters Kluwer, Warszawa 2007, s. 181.

cjalnych, natomiast koncentrację działań służb na tych samych rodzajach zagrożeń – nie jako zajmowanie się tym samym, lecz jako ich odmienną działalność o charakterze komplementarnym[40].

Należy zaznaczyć, że służby specjalne w ramach ustawowych uprawnień – na ich granicy, jak również poza nią – stosują tajne środki i metody działania jako podstawowe narzędzia pracy, określanej w języku tych służb jako praca operacyjna (czynności operacyjno-rozpoznawcze)[41]. Praca operacyjna wskazuje na odmienność tych służb od innych podmiotów państwowych – pod względem zakresu działalności, która jest objęta ustawową ochroną i traktowana jako informacje niejawne oznaczone klauzulą niejawności typu: „tajne" i „ściśle tajne".

W systemie kierowania bezpieczeństwem państwa (dowodzenia wojskami) służby specjalne (kontrwywiad cywilny i wojskowy[42] oraz wywiad cywilny i wojskowy[43]) realizują funkcję informacyjną, która jest uwzględniona w ustawowym katalogu wykonywanych zadań związanych z rozpoznawaniem i przeciwdziałaniem zagrożeniom dla bezpieczeństwa wewnętrznego i zewnętrznego państwa. Posiadanie systemu informacji, które przekładają się na wiedzę podmiotów funkcjonujących w systemie bezpieczeństwa wewnętrznego i zewnętrznego państwa, a dotyczących zagrożeń dla jego funkcjonowania, wymaga zdobywania i gromadzenia tych informacji, ich przetwarzania, dystrybucji i ochrony.

Służby wywiadowcze dostarczają informacji o sytuacji międzynarodowej, postępującej globalizacji, a tym samym o wyzwaniach i zagrożeniach, jakie występują w otoczeniu zewnętrznym bliższym i dalszym państwa oraz ich wpływie na bezpieczeństwo zewnętrzne i wewnętrzne państwa/sojuszników.

Międzynarodowe zagrożenia dla bezpieczeństwa państwa:
1) terroryzm,
2) nacjonalizm,
3) totalitaryzm i autorytaryzm,
4) mafie oraz przemyt broni i ludzi,

---

40 B. Libera, *Rodzaje zagrożeń w środowisku międzynarodowym*, [w:] *Urzędnik i biznesmen*…, s. 167.

41 B. Libera, *Podstawy wiedzy o służbach specjalnych*…, s. 175.

42 Służby kontrwywiadowcze wybranych państw: Federalne Biuro Śledcze (FBI) – USA, Federalny Urząd Konstytucji (BfV) – RFN, Urząd Bezpieczeństwa Bundeswehry (MAD) – RFN, Federalna Służba Bezpieczeństwa (FSB) – Rosja, MI 5 – Wielka Brytania, Szin Bet – Izrael, AMAN – Izrael, Agencja Bezpieczeństwa Wewnętrznego (ABW) – Polska, Służba Kontrwywiadu Wojskowego (SKW) – Polska, Dyrekcja Generalna Bezpieczeństwa Wewnętrznego (DGSI) – Francja, Dyrekcja Ochrony Bezpieczeństwa Sił Zbrojnych (DPSD) – Francja.

43 Służby wywiadowcze wybranych państw: Federalna Służba Wywiadowcza (BND) – RFN, Centralna Agencja Wywiadowcza (CIA) – USA, Agencja Wywiadu Obronnego (DIA) – USA, Służba Wywiadu Zagranicznego (SWZ) – Rosja, Główny Zarząd Wywiadowczy (GRU) – Rosja, MI 6 – Wielka Brytania, Sztab Wywiadu Obronnego (DIS) – Wielka Brytania, Mossad – Izrael, Agencja Wywiadu (AW) – Polska, Służba Wywiadu Wojskowego (SWW) – Polska, Dyrekcja Generalna Bezpieczeństwa Zewnętrznego (DGSE) – Francja, Dyrekcja Wywiadu Wojskowego (DRM) – Francja.

5) narkobiznes i korupcja,
6) pandemie i epidemie,
7) proliferacja broni masowego rażenia i handel bronią,
8) ludobójstwo,
9) nielegalny handel bronią,
10) spory religijne i ruchy separatystyczne,
11) państwa w stanie rozpadu,
12) podmioty pozapaństwowe,
13) kataklizmy (klęski żywiołowe) i katastrofy techniczne,
14) ubóstwo i przeludnienie,
15) konflikty etniczne i terytorialne,
16) masowe migracje (uchodźcy),
17) fundamentalizm religijny,
18) kryzysy energetyczne i żywnościowe,
19) kryzysy ekonomiczne,
20) degradacja środowiska naturalnego,
21) agresja o charakterze terrorystycznym,
22) konflikty przygraniczne, incydenty zbrojne,
23) agresja przeciwko państwu,
24) ataki asymetryczne i inne,
25) inne[44].

Z kolei służby kontrwywiadowcze dostarczają informacji o zagrożeniach mających wpływ na bezpieczeństwo wewnętrzne państwa/sojuszników.

Tabela 1. Zagrożenia dla bezpieczeństwa wewnętrznego państwa

Lp.	Zagrożenia		
	Zagrożenia dla bytu ludności	Zagrożenia bezpieczeństwa i porządku publicznego	Zagrożenia dóbr publicznych
1.	degradacja środowiska naturalnego i antropogenicznego	terror polityczny i kryminalny	katastrofy techniczne
2.	kataklizmy i katastrofy	demonstracje i protesty	kataklizmy (klęski żywiołowe)
3.	pandemie i epidemie	zamachy i zabójstwa	skażenia chemiczne i promieniotwórcze
4.	skażenie chemiczne i promieniotwórcze	uprowadzenia	skażenia środkami toksycznymi,
5.	skażenie środkami toksycznymi	branie zakładników	degradacja środowiska naturalnego, antropogenicznego i infrastruktury państwa
6.	terror polityczny i kryminalny	korupcja	grabieże majątku i zasobów

[44] Z. Lach, S.A. Łaszczuk, *Geografia bezpieczeństwa*, Akademia Obrony Narodowej, Warszawa 2004, s. 15.

7.	bezrobocie i korupcja	grabieże	przestępczość zorganizowana
8.	degradacja miast	mafie i gangi	upadek gospodarki
9.	ubóstwo	przemyt i handel bronią	nielegalne operacje finansowe
10.	narkomania	oszustwa i fałszerstwa	inne
11.	inne	przestępczość zorganizowana	
12.		inne	

Źródło: Z. Lach, S.A. Łaszczuk, *Geografia bezpieczeństwa*..., s. 15

Służby specjalne zasilają strategiczny system informacyjny władzy wykonawczej, który jest sprzężony ze strukturą organizacyjną państwa na wszystkich poziomach zarządzania jego bezpieczeństwem. Jego podstawową cechą jest to, że stanowi uporządkowaną sieć powiązań informacyjnych między służbami specjalnymi, służbami o charakterze policyjnym, służbami rozpoznania sił zbrojnych (rodzajów sił zbrojnych), uprawnionymi organami administracji rządowej i zarządzania kryzysowego. Służby specjalne pełnią także funkcję systemu wczesnego ostrzegania, a w ściśle określonych warunkach nawet alarmowania. Należy podkreślić, że funkcja informacyjna służb specjalnych powinna być doskonalona już w czasie pokoju. Dostęp do informacji zróżnicowanych, które są obiektem zainteresowania uprawnionego podmiotu, zwiększa możliwość dokonania wyboru, co ma istotny wpływ na minimalizację ryzyka podejmowania niewłaściwych decyzji. Informacje te warunkują m.in. skuteczność działania państwa/sojuszników. Podmioty decyzyjne uczestniczące w kierowaniu bezpieczeństwem państwa muszą rozwiązywać coraz trudniejsze i coraz bardziej złożone problemy, a także w sposób właściwy reagować na zmieniające się warunki.

> Na szczególną uwagę zasługują służby wywiadowcze, które z uwagi na usytuowanie w zglobalizowanym świecie nabierają coraz większego znaczenia. W świecie, który staje się coraz bardziej wielobiegunowy, coraz bardziej złożony i którego nie można już dalej postrzegać przez pryzmat współzawodnictwa ze Związkiem Radzieckim, zachodzi potrzeba wykorzystania wywiadu w coraz większym, a nie mniejszym zakresie[45].

Na przykład w komunikacie rządu Wielkiej Brytanii, dotyczącym powstania nowej Komisji Parlamentarnej do spraw Bezpieczeństwa i Wywiadu, znaleźć można stwierdzenie o „potrzebie wykorzystania w tym niespokojnym i nieprzewidywalnym świecie służb wywiadowczych i odniesienie się do kluczowej roli tego rodzaju instytucji w zwalczaniu zagrożeń dla bezpieczeństwa naszych obywateli i interesów naszego państwa na całym świecie”[46].

[45] D.L. Boren, *The Intelligence Community*: *How Crucial*?, „Foreign Affaris” 1992, Vol. 71, No. 3.

[46] Lord Mac Kay, Izba Lordów, 9 grudnia 1993, Zbiór oficjalnych sprawozdań z posiedzeń parlamentu angielskiego Hansard, col. 1024, 1026.

Zakres działania wywiadu ustala się w długiej perspektywie czasowej z uwzględnieniem przeszłości, teraźniejszości i przyszłości. Rządy zawsze powinny dbać o ścisłe związki z wywiadem przy uwzględnieniu bezpieczeństwa wewnętrznego i obronności państwa.

> Chodzi przede wszystkim o uniknięcie poważnych porażek i niebezpieczeństw, ataku z zaskoczenia, wpływu innego kraju na sytuację wewnętrzną w państwie, rozpadu państwa i nagłych zmian politycznych. Znaczenie wywiadu zależy od zagrożeń, słabych punktów w systemie bezpieczeństwa państwa i narodowego sposobu postrzegania działalności wywiadu. Państwa, w których występują największe zagrożenia bezpieczeństwa (wewnętrzne i zewnętrzne), mają najwięcej powodów, aby traktować działania wywiadu bardzo poważnie. […] Również słabość państwa jest istotnym powodem do inwestowania w wywiad[47].

Bezpieczeństwo państwa to również obrona jego posiadłości zamorskich (np. Falklandy – Wielka Brytania), ochrona obywateli i ich własności poza granicami państwa, a także reakcja na zagrożenia ze strony innych państw, w tym stosunek do konfliktów regionalnych. Ponadto zaangażowanie państw w realizację polityki zagranicznej jest zróżnicowane. Oznacza to, że aktywna polityka zagraniczna to większa rola wywiadu, natomiast mniejsze zaangażowanie to ograniczony udział tej służby w realizacji funkcji zewnętrznej państwa.

Pozycja wywiadu w państwie zależy od wielu wzajemnie powiązanych ze sobą czynników, do których należy zaliczyć: miejsce państwa w środowisku międzynarodowym, charakter i kierunek prowadzonej polityki zagranicznej, jego potencjał gospodarczy i wojskowy, potencjał naukowo-techniczny, sojusze polityczno-wojskowe i gospodarcze, siły zbrojne (wyszkolenie, wyposażenie i uzbrojenie), posiadanie broni masowego rażenia, nakłady przeznaczane na bezpieczeństwo i obronność, zagrożenia wewnętrzne i zewnętrzne, słabe strony, postrzeganie przez władze państwowe.

Kolejna niezmiernie ważna kwestia to relacje wywiadu z siłami zbrojnymi. Występują one przede wszystkim na linii wywiad cywilny – siły zbrojne. W państwach, gdzie dominującą pozycję na tle innych służb specjalnych zajmuje wywiad cywilny (np. CIA w Stanach Zjednoczonych, BND w RFN, Mossad w Izraelu, SWZ w Federacji Rosyjskiej, MI6 W. Brytania), jego pozycja w procesie realizacji funkcji informacyjnej jest znacząca. Bardzo często ma miejsce rywalizacja o prymat nad innymi służbami specjalnymi. Wywiad cywilny nabiera jeszcze większego znaczenia, kiedy rządy, realizując swoją politykę zagraniczną, wyznaczają siłom zbrojnym zadania poza granicami państwa, np. z mandatu ONZ czy NATO. Rola wywiadu cywilnego sprowadza się ogólnie do zabezpieczenia miejsca wykonywania zadań przez narodowe siły zbrojne pod kątem operacyjnym, a podstawowym celem sił zbrojnych jest zaspokojenie potrzeb informacyjnych (np. działania w Iraku czy Afganistanie). Oczywiście,

[47] M. Herman, *Potęga wywiadu*, Bellona, Warszawa 2002, s. 337.

może się to odbywać w ramach współpracy i współdziałania ze służbami wywiadowczymi innych państw.

W odniesieniu do komponentów sił zbrojnych, żandarmerii wojskowej czy policji nie można zapominać o wywiadzie wojskowym, którego podstawowym zadaniem jest zabezpieczenie potrzeb informacyjnych sił zbrojnych do wykonywania zadań w czasie pokoju, kryzysu i wojny. Oznacza to, że siły zbrojne muszą być zdolne do zachowania swojego potencjału i efektywności w czasie pokoju oraz skutecznie działać w czasie wojny. Znaczenie wywiadu wojskowego jeszcze bardziej wzrasta, gdy władze państwowe traktują siły zbrojne i wymienione pozostałe komponenty do użycia w praktyce. Udział jednostek narodowych w Sojuszu Północnoatlantyckim czy w operacjach humanitarnych ONZ uzasadnia konieczność podjęcia wyprzedzających działań (osobowych i pozaosobowych) przez wywiad wojskowy prowadzonych na poziomie strategicznym, operacyjnym i taktycznym. Istnieje konieczność rozpoznania rejonu geograficznego pod kątem wyznaczenia/wyznaczania i wskazania celów. Działalność wywiadu wojskowego to również wsparcie procesu planowania oraz szeroko rozumiane zabezpieczenie realizacji konkretnych działań bojowych, w tym zapewnienia bezpieczeństwa jednostkom sił narodowych (sojuszniczych) biorących udział w działaniach bojowych[48].

Dla bezpieczeństwa państw członkowskich Unii Europejskiej i Sojuszu Północnoatlantyckiego ważnym źródłem informacji są narodowe służby wywiadowcze i kontrwywiadowcze tych organizacji. Należy mieć na uwadze również służby specjalne państw trzecich, które z uwagi na swój potencjał osobowy i informacyjny mogą w określonych sytuacjach wspierać nie tylko pojedyncze państwa (np. Stany Zjednoczone), ale i organizacje międzynarodowe (np. ONZ, NATO, Unię Europejską, WNP). Z uwagi na to, że na poziomie Unii Europejskiej i NATO nie ma ponadnarodowych służb wywiadowczych i kontrwywiadowczych z uprawnieniami do wykonywania czynności operacyjno-rozpoznawczych, dlatego tak ważna jest współpraca i koordynacja pracy narodowych służb tego typu państw członkowskich wskazanych organizacji. Na podstawie informacji otrzymywanych od służb wywiadowczych/kontrwywiadowczych państw członkowskich opracowuje się informacje o charakterze niejawnym, które są przekazywane uprawnionym podmiotom Unii Europejskiej, Sojuszu Północnoatlantyckiego i poszczególnych państw członkowskich, niekiedy również państwom trzecim (np. w ramach walki z międzynarodowym terroryzmem). W NATO obowiązuje centralna ocena informacji wywiadowczych/kontrwywiadowczych i centralne określanie zadań, natomiast wykonanie tych zadań leży w kompetencji wywiadów/kontrwywiadów poszczególnych państw.

Na tym etapie ważna jest również współpraca międzynarodowa w zakresie wymiany informacji o charakterze wywiadowczym, szczególnie pochodzących z rozpoznania kosmicznego (należy przy tym pamiętać, że nie wszystkie narodowe służby wywiadowcze uprawiają rozpoznanie satelitarne).

[48] Tamże, s. 338.

Współczesne przygotowanie i prowadzenie operacji humanitarnych (z mandatu ONZ, NATO, Unii Europejskiej), zwalczanie klęsk żywiołowych, użycie sił specjalnych, policji, żandarmerii wojskowej czy sił zbrojnych na polu walki nie jest możliwe bez posiadania dostępu do danych pochodzących z rozpoznania satelitarnego. Satelita to umieszczony na orbicie statek kosmiczny zaopatrzony w aparaturę do przesyłania zdjęć i sygnałów radiowych na Ziemię. Satelity dzieli się na: rozpoznawcze[49], komunikacyjne, naukowo-badawcze, geofizyczne, astronomiczne, meteorologiczne. Służby wywiadowcze/kontrwywiadowcze państw członkowskich Unii i NATO posiadają również dostęp do informacji wywiadowczych zdobywanych za pośrednictwem wywiadu satelitarnego, który jest uprawiany przez nieliczne państwa członkowskie (Stany Zjednoczone, Wielką Brytanię, Francję, RFN, Hiszpanię i Włochy).

W zależności od szczebla dowodzenia wyróżnia się następujące poziomy rozpoznania[50]:

1) strategiczne – to najwyższy poziom rozpoznania, gdzie wykorzystywane są wszystkie zdobyte dane niezbędne do opracowania strategii oraz planów wojskowych odnoszących się do państwa i środowiska międzynarodowego; dotyczą one sfer: politycznej, ekonomicznej, dyplomatycznej i wojskowej;
2) operacyjne – jego celem jest zdobycie danych niezbędnych do przygotowania i prowadzenia operacji (kampanii) zarówno militarnych, jak i innych (specjalnych, pokojowych) na teatrze działań; dane te dotyczą zazwyczaj określonego rejonu geograficznego;
3) taktyczne – jego celem jest dostarczanie dowódcom niezbędnych danych wymaganych do przygotowania i prowadzenia działań taktycznych; dotyczą one rejonu będącego w zainteresowaniu danego związku taktycznego lub oddziału.

Rozpoznanie satelitarne ma przewagę nad innymi działaniami rozpoznawczymi z uwagi na to, że jest prowadzone zarówno w czasie pokoju, kryzysu, jak i wojny (we wszystkich warunkach atmosferycznych). Dostarcza dane w czasie niemal rzeczywistym na poziomie strategicznym, operacyjnym i taktycznym. Przyjmuje się, że prowadzenie jakichkolwiek działań nie jest możliwe bez udziału rozpoznania satelitarnego. Wraz z postępem naukowo-technicznym poprawie ulega wyposażenie satelitów rozpoznawczych, ponadto ma miejsce wszechobecna specjalizacja. Rozpoznanie satelitarne ma tę przewagę nad klasycznym, że nie narusza suwerenności państwowej w świetle prawa międzynarodowego.

Podział satelitów rozpoznawczych ze względu na przeznaczenie i zamontowane urządzenia:

---

[49] Satelity rozpoznawcze posiadają m.in. Stany Zjednoczone, Federacja Rosyjska, Chiny, Wielka Brytania, Francja, RFN, Hiszpania i Włochy.

[50] G. Nowacki, *Rozpoznanie satelitarne USA i Federacji Rosyjskiej*, Akademia Obrony Narodowej, Warszawa 2002, s. 59–60.

1. Satelity rozpoznania obrazowego (IMINT), w tym fotograficzne (PHOTINT), umożliwiają wykonywanie zdjęć dużych obszarów Ziemi z dużą dokładnością i w stosunkowo krótkim czasie. Ten typ rozpoznania, oprócz typowych funkcji wywiadowczych, jest również instrumentem weryfikacji przestrzegania przez państwa ograniczeń w rozbudowie potencjału strategicznego. Satelity te pełnią funkcję kontrolną w zakresie przestrzegania porozumień dotyczących narodowych środków technicznych.
2. Satelity rozpoznania sygnałów elektromagnetycznych (SIGNINT), które polega na rejestracji sygnałów emitowanych przez urządzenia promieniujące energię elektromagnetyczną, m.in. radarowe systemy obrony powietrznej, środki rakietowe potencjalnego przeciwnika, urządzenia pracujące w systemie dowodzenia i łączności. Satelity te mają także możliwość prowadzenia walki elektronicznej.
3. Satelity rozpoznania pomiarowego i sygnaturowego (MASINT), które polega na analizie danych technicznych przekazywanych przez satelity w celu identyfikowania źródeł, nadajników i urządzeń promieniujących różnego rodzaju energie. W jego skład wchodzi rozpoznanie radiolokacyjne, podczerwieni, chemiczne i biologiczne oraz broni wiązkowej.
4. Satelity rozpoznania oceanicznego przekazują m.in. dane dotyczące obserwacji mórz i oceanów. Są one w stanie określać położenie jednego z najniebezpieczniejszych (trudnych do zlokalizowania) komponentów strategicznej triady nuklearnej przeciwnika, tzn. atomowych okrętów podwodnych, nosicieli broni jądrowej.
5. Satelity wczesnego wykrywania i ostrzegania prowadzą rozpoznanie rakiet międzykontynentalnych lub bombowców strategicznych tuż po starcie. Kolejnym zadaniem tych satelitów jest rozpoznanie prób nuklearnych – identyfikacja i lokalizacja miejsc, w których są prowadzone próby jądrowe oraz ocena stopnia skażenia radioaktywnego[51].

Ważną rolę w procesie zdobywania informacji odgrywa wywiad geoprzestrzenny (GEOIT). Jego zadaniem jest zbieranie, analiza i dystrybucja informacji geoprzestrzennych. W procesie studyjnym prowadzona jest analiza obrazów oraz informacji geoprzestrzennych w celu opisania, oceny i wizualizacji cech fizycznych i geograficznych, jakie zachodzą na Ziemi. Wywiad geoprzestrzenny oferuje następujące kategorie produktów i serwisów: lotnictwo, nautyka, topografia i ląd, pozycjonowanie i cele, nazwy geograficzne, analiza. Na przykład w Stanach Zjednoczonych wywiadem geoprzestrzennym zajmuje się Narodowa Agencja Wywiadu Satelitarnego, która znajduje się w strukturze Departamentu Obrony USA.

Dla zabezpieczenia informacyjnego państw członkowskich Unii Europejskiej/NATO obok rozpoznania satelitarnego ważny jest również udział samolotów wczesnego wykrywania i powiadamiania systemu AWACS. Samoloty

[51] Tamże, s. 61 i 64.

tego systemu pełnią rolę powietrznych centrów dowodzenia i kierowania działaniami, zabezpieczają kontrolę i wsparcie informacyjne na szerokim obszarze zainteresowania. Wykonują one wymienione zadania na korzyść państw członkowskich Unii Europejskiej i Sojuszu Północnoatlantyckiego.

Unia Europejska stworzyła i nadal rozbudowuje systemy powiadamiania i alarmowania, których obszary zainteresowania są zróżnicowane.

Systemy powiadamiania i alarmowania UE:

1. Europejska Agencja Kosmiczna (ESA).
2. Globalny Monitoring dla Środowiska i Bezpieczeństwa (GMES).
3. Centrum Satelitarne Unii Europejskiej (EUSC).
4. Instytut Unii Europejskiej Studiów nad Bezpieczeństwem (ISS).
5. System Wczesnego Ostrzegania i Alarmowania (EWRS).
6. System Wczesnego Powiadamiania i Wymiany Informacji o Zagrożeniach Radiologicznych bądź Nuklearnych (ECURIE).
7. System Ochrony Sieci Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej (CIWIN).
8. Bezpieczny Ogólny System Szybkiego Ostrzegania (ARGUS).
9. System Wczesnego Ostrzegania Przed Biologiczno-Chemicznymi Atakami i Zagrożeniami (RAS – BICHAT).
10. System Powiadamiania Europolu.
11. Centrum Monitoringu i Informacji (MIC).

Przykładami sytemu powiadamiania i alarmowania w Unii Europejskiej są:

– Globalny Monitoring Środowiska i Bezpieczeństwa (GMES)[52] przeznaczony jest do kontrolowania stanu środowiska z pułapu satelitarnego, lotniczego i naziemnego. Zgromadzone za pomocą satelitów oraz pomiarów naziemnych dane są przetwarzane w celu świadczenia usług informacyjnych pozwalających na skuteczniejsze zarządzanie środowiskiem oraz poprawę bezpieczeństwa obywateli Unii Europejskiej. Dzięki temu zapewnia się sprawniejsze reagowanie w przypadku katastrof naturalnych, efektywniejsze korzystanie z zasobów naturalnych, lepszy monitoring jakości i czystości wód, powietrza itd. Program GMES obejmuje:
  a) komponent usługowy zapewniający dostęp do informacji obejmujących następujące obszary tematyczne: monitoring obszarów lądowych, zarządzanie kryzysowe, bezpieczeństwo, monitoring środowiska morskiego, monitoring atmosfery, dostosowywanie się do zmian klimatu i łagodzenie ich skutków;
  b) komponent kosmiczny zapewniający trwałe obserwacje z instalacji kosmicznych na potrzeby obszarów tematycznych, o których mowa w lit. a);

[52] Program GMES opiera się na badaniach zrealizowanych na mocy decyzji Nr 1982/2006/WE oraz w ramach programu Europejskiej Agencji Kosmicznej dotyczącego komponentu kosmicznego GMES – Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 911/2010 z dnia 22.09.2010 r. w sprawie europejskiego programu monitorowania Ziemi (GMES) i początkowej fazy jego realizacji (lata 2011–2013) – Dz.U. L. 276 z 20.10.2010 r.

c) komponent *in situ* zapewniający obserwacje z instalacji powietrznych, morskich oraz naziemnych na potrzeby obszarów tematycznych, o których mowa w lit. a).

– Centrum Satelitarne Unii Europejskiej (EUSC) jest odpowiedzialne za przetwarzanie i dostarczanie informacji pochodzących m.in. z analizy obrazów satelitarnych. Zadaniem Centrum jest wspieranie procesów decyzyjnych w dziedzinie Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB) Unii Europejskiej. Obszary zainteresowania w działalności EUSC wynikają z kierunków określonych w Strategii Bezpieczeństwa Unii Europejskiej. Należą do nich zadania związane z monitorowaniem: konfliktów regionalnych państw upadłych, grup przestępczości zorganizowanej, ugrupowań terrorystycznych, procesów związanych z proliferacją broni masowego rażenia. Centrum Satelitarne pełni również funkcję systemu wczesnego ostrzegania Unii Europejskiej, umożliwiając typizację, a tym samym daje Wspólnocie możliwość zapobiegania możliwym konfliktom zbrojnym i kryzysom humanitarnym.

Przy realizacji powyższych zadań EUSC wspiera działania Unii m.in. w obszarach: bezpieczeństwa ogólnego (nadzór nad obszarami zainteresowania), realizacji zadań petersberskich, wykonywania zadań ratowniczych i humanitarnych, zadań realizowanych z udziałem sił zbrojnych w zarządzaniu kryzysowym. Ponadto wsparcie realizowane przez EUSC dotyczy obszarów: planowania wyprzedzającego, kontroli proliferacji uzbrojenia i broni masowego rażenia, wsparcia ćwiczeń, oraz innych działań realizowanych przez państwa członkowskie Unii Europejskiej. Działania operacyjne EUSC realizowane są głównie w formie współpracy z Radą DG VIII, Sztabem Wojskowym UE, Wspólnym Centrum Sytuacyjnym[53].

W działalności Centrum można dopatrzyć się początków przyszłego wywiadu satelitarnego Unii Europejskiej.

– Instytut Unii Europejskiej Studiów nad Bezpieczeństwem (ISS), prowadzi badania naukowe nad problematyką bezpieczeństwa i obrony w Unii Europejskiej, a jego podstawowym zadaniem jest przyczynianie się do rozwoju Wspólnej Polityki Zagranicznej i Bezpieczeństwa (WPZiB).

– System Wczesnego Powiadamiania i Wymiany Informacji o Zagrożeniach Radiologicznych bądź Nuklearnych (ECURIE)[54] został utworzony w celu powiadamiania uprawnionych podmiotów państw członkowskich Unii Europejskiej i Szwajcarii o incydentach w obiektach nuklearnych. System pozwala na wszczęcie działań pozwalających na ochronę ludności. Państwa członkowskie UE i stowarzyszone zobowiązane są do przekazywania informacji o pomiarach promieniowania prowadzonych na własnym terytorium. Europejska

[53] *System reagowania kryzysowego*…, s. 347.

[54] Podstawę prawną funkcjonowania systemu ECURIE stanowią: decyzja Komisji UE Nr 87/600/ Euratom w sprawie utworzenia systemu ECURIE; decyzja Komisji UE Nr 89/618/ Euratom w sprawie ustalenia narzędzi wykonawczych, członków UE i państw uczestniczących w systemie ECURIE; umowa między Europejską Wspólnotą Energii Atomowej a państwami nienależącymi do Unii w sprawie udziału tych ostatnich we wspólnotowych ustaleniach dotyczących wczesnej wymiany informacji w przypadku pogotowia radiologicznego Nr 2003/C 102.02.

Wspólnota Energii Atomowej (EURATOM) pełni rolę organu nadzorczego nad systemem ECURIE. System ten uruchamia się w przypadku zagrożeń radiologicznych, które występują w rejonach obiektów wykorzystujących energię atomową lub w miejscach jej produkcji.

– System Ochrony Sieci Ostrzegania o Zagrożeniach dla Infrastruktury Krytycznej (CIWIN)[55] stanowi podstawę wymiany informacji między organami państw członkowskich oraz umożliwienia im korzystania z systemu wczesnego ostrzegania w zakresie ochrony infrastruktury krytycznej.
– System Wczesnego Ostrzegania przed Biologiczno-Chemicznymi Atakami i Zagrożeniami (RAS – BICHAT) jest przeznaczony do informowania o wymienionych atakach i zagrożeniach. W systemie obowiązuje zasada wzajemnego kontaktowania się i wymiany informacji pomiędzy punktami kontaktowymi państw członkowskich Unii Europejskiej i państw stowarzyszonych. W sytuacji wystąpienia podwyższonego ryzyka lub próby ataku terrorystycznego państwa uczestniczące w systemie wczesnego ostrzegania przed biologiczno-chemicznymi atakami i zagrożeniami powiadamiają Centrum Komunikacji i Dowodzenia za pośrednictwem Krajowego Punktu Kontaktowego usytuowanego w Ministerstwie Spraw Wewnętrznych. W następstwie tego uruchamiany jest Zespół Zarządzania Kryzysowego, którego zadaniem jest weryfikacja otrzymywanych informacji i przydział odpowiednich instrumentów w zależności od rodzaju zagrożenia. Po zatwierdzeniu środków zaradczych przez Komisję Unii Europejskiej i wyborze systemu

[55] Podstawy prawne systemu CIWIN stanowią: Komunikat Komisji UE z dnia 12.12.2006 r. w spawie Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPCIP) (COM 2006/786), Wniosek Komisji UE z dnia 12.12.2006 r. w sprawie rozpoznania i wyznaczenia europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie zwiększenia jej ochrony (COM 2006/787), Decyzja Rady UE z dnia 8.11.2007 r. w sprawie ustanowienia wspólnotowych mechanizmów ochrony ludności (2007/779/WE, Euratom), Decyzja Rady UE z dnia 14.12.1987 r. w sprawie wspólnotowych warunków wczesnej wymiany informacji w przypadku zdarzenia radiacyjnego, ustanawiająca wspólnotowy system wczesnego powiadamiania i wymiany informacji w sytuacjach zagrożenia radiacyjnego (87/600/Euratom), Dyrektywa Rady Nr 82/894/EWG z dnia 21.12.1982 r. w sprawie zgłaszania chorób zwierząt we Wspólnocie, Dyrektywa Rady z dnia 8.05.2000 r. w sprawie środków ochronnych przed wprowadzeniem do Wspólnoty organizmów szkodliwych dla roślin (2000/29/WE), Decyzja Parlamentu Europejskiego i Rady z dnia 24.09.1998 r. ustanawiająca sieć nadzoru i kontroli epidemiologicznej chorób zakaźnych we Wspólnocie (2119/98/WE), Dyrektywa Parlamentu Europejskiego i Rady z dnia 3.12.2001 r. w sprawie ogólnego bezpieczeństwa produktów (2001/95/WE), Rozporządzenie Parlamentu Europejskiego i Rady z dnia 28.01.2002 r. ustanawiające ogólne zasady i wymagania prawa żywnościowego, powołujące Europejski Urząd ds. Bezpieczeństwa Żywności oraz ustanawiające procedury w zakresie bezpieczeństwa żywności (178/2002), Decyzja Komisji UE z dnia 19.08.2003 r. dotycząca opracowania zintegrowanego skomputeryzowanego systemu weterynaryjnego pod nazwą TRACES (2003/623/WE), Decyzja Komisji z dnia 23.12.2005 r. zmieniająca regulamin wewnętrzny Komisji (2006/25/WE, Euratom), Zielona księga w sprawie rozszerzenia Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPCIP) przyjęta w dniu 17.11.2005 r. w sprawie konsultacji z państwami członkowskimi Unii Europejskiej oraz przedstawicielami sektora prywatnego.

neutralizującego następuje jego aktywacja oraz kontrola działania[56]. Należy podkreślić, że w przypadku zagrożenia bezpieczeństwa państwo członkowskie Unii Europejskiej powiadamia Centrum Komunikacji i Dowodzenia, Biuro Ochrony w Brukseli lub Dyrekcję ds. Zdrowia i Konsumentów celem powiadomienia Komisji UE. W przypadku poważnego kryzysu uruchamiany jest dodatkowo Sztab Reagowania Kryzysowego, który w sytuacji wybuchu kryzysu o skali globalnej przekazuje informacje do Światowej Inicjatywy Bezpieczeństwa (GHSI), dysponującej siłami i środkami do walki z terroryzmem stosującym broń biologiczną i/lub broń chemiczną.

– System Powiadamiania Europol, który bezzwłocznie powiadamia jednostki narodowe (oraz ich oficerów łącznikowych, jeśli jednostki narodowe tego zażądają), o wszelkich informacjach dotyczących ich państwa i o ujawnionych powiązaniach między przestępstwami objętymi kompetencją Europolu. Przekazywane mogą też być informacje i dane wywiadowcze dotyczące innych poważnych przestępstw, o których Europol dowiedział się w trakcie wykonywania swych obowiązków.
– Centrum Monitoringu i Informacji (MIC)[57] jest strukturą Komisji Europejskiej funkcjonującą w ramach Wspólnotowego Mechanizmu Ochrony Ludności, który może być aktywowany w sytuacjach zagrożeń naturalnych lub spowodowanych przez człowieka. Głównymi zadaniami MIC są: monitorowanie sytuacji kryzysowych; utrzymywanie stałej łączności z punktami kontaktowymi w państwach uczestniczących; koordynacja operacji ratowniczych i humanitarnych prowadzonych w ramach Wspólnotowego Mechanizmu Ochrony Ludności.

System informacyjny w kierowaniu bezpieczeństwem państwa powinien zapewniać dopływ informacji dla uprawnionych użytkowników w państwie/sojuszników z taką częstotliwością i w takim czasie, aby mogły być one wykorzystywane w procesie decyzyjnym.

Społeczność międzynarodowa mimo istnienia poważnych zagrożeń, szczególnie o charakterze niemilitarnym, dla bezpieczeństwa państw czy regionów, nie jest skłonna do utworzenia ponadnarodowych służb specjalnych z szerokimi uprawnieniami do wykonywania czynności operacyjno-rozpoznawczych. Postawa taka wynika m.in. z obawy przed częściową utratą suwerenności w tak delikatnej materii, jaką są służby specjalne. Ponadto państwa nie chcą dzielić się swoimi tajemnicami, a przede wszystkim udostępniać swoich aktywów osobowych.

[56] *System reagowania kryzysowego*..., s. 369.

[57] Podstawę prawną działania MIC stanowi Decyzja Rady z dnia 8 listopada 2007 r. ustanawiająca wspólnotowy mechanizm ochrony ludności (2007/779/WE, Euratom).

Podsumowanie

Narodowe służby specjalne realizują zadania w trudnym i nieprzewidywalnym środowisku bezpieczeństwa międzynarodowego. W ich działalności niebagatelną rolę odgrywa czas, który jest wyznacznikiem sukcesu, ale i porażki. Współcześnie świat wymaga służb, które będą zdobywały informacje w skali globalnej. Wymaga to jednak międzynarodowej współpracy zarówno służb wywiadowczych, jak i kontrwywiadowczych. Państwa członkowskie Sojuszu Północnoatlantyckiego i Unii Europejskiej na poziomie tych organizacji prowadzą taką współpracę, ale to na narodowych służbach specjalnych spoczywa ciężar prowadzenia aktywnych działań operacyjno-rozpoznawczych.

Bibliografia

Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych*, Akademia Podlaska, Siedlce 2002

Boren D.L., *The Intelligence Community: How Crucial?* „Foreign Affaris" 1992, Vol. 71, No. 3

Dworecki S., *Od konfliktu do wojny*, Buwik, Warszawa 1996

Encyklopedia terroryzmu, Bellona, Warszawa 2004

Ficoń K., *Inżynieria zarządzania kryzysowego. Podejście systemowe*, PWN, Warszawa 2007

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

Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, Akademia Obrony Naukowej, Warszawa 2003

Herman M., *Potęga wywiadu*, Bellona, Warszawa 2002

Ingalls J., *Human Energy*, Addison–Wesley Publishing Company, Menlo Park 1976

Jemioło T., *Globalizacja – szanse i zagrożenia*, Akademia Obrony Narodowej, Warszawa 2000

Kisielnicki J., *Informatyczna infrastruktura zarządzania*, Placet, Warszawa 1992

Koziej S., *Współczesne problemy bezpieczeństwa międzynarodowego i narodowego (studium analityczne*), PWSBiA, Warszawa 2003

Kozub M., *Strategiczne środowisko bezpieczeństwa w pierwszych latach XXI wieku*, Akademia Obrony Narodowej, Warszawa 2009

Kwećka R., *Procesy informacyjne w ramach systemu reagowania kryzysowego Unii Europejskiej*, [w:] *System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary*, red. J. Gryz, Wydawnictwo Adam Marszałek, Toruń 2009

Lach Z., Łaszczuk S.A., *Geografia bezpieczeństwa*, Akademia Obrony Narodowej, Warszawa 2004

Leksykon wiedzy wojskowej, red. M. Laprus, t. 1, MON, Warszawa 1973

Lord Mac Kay, Izba Lordów, 9 grudnia 1993, Zbiór oficjalnych sprawozdań z posiedzeń parlamentu angielskiego Hansard col. 1024, 1026

Nowacki G., *Rozpoznanie satelitarne USA i Federacji Rosyjskiej*, Akademia Obrony Narodowej, Warszawa 2002

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

Piskozub A., *Przemiany kulturowe i cywilizacyjne w perspektywie społeczeństwa postindustrialnego i aspekty globalizacji kulturowej – uwarunkowania i wnioski*, [w:] *Polska na drodze do nowoczesnej cywilizacji*, red. J. Dąbrowski, t. 2, PAN, Warszawa 1990

Rydlewski G., *Rządowy system decyzyjny w Polsce*, Elipsa, Warszawa 2002

System reagowania kryzysowego Unii Europejskiej. Struktura – charakter – obszary, red. J. Gryz, Wydawnictwo Adam Marszałek, Toruń 2009

Urzędnik i biznesmen w środowisku międzynarodowym. Wybrane aspekty pragmatyki zawodowej, red. J. Barcz, B. Libera, Wydawnictwo ABC–Wolters Kluwer, Warszawa 2007

Witecka M.S., *Zagrożenia asymetryczne a technologie informacyjne*, „Zeszyt Problemowy TWO" 2011, nr 4

Zbiegień-Maciąg L., Pawnik W., *Zarządzanie organizacją. Aspekt socjologiczny*, Wydawnictwo AGH, Kraków 1998

Żebrowski A., *Wywiad i kontrwywiad XXI wieku*, Wyższa Szkoła Ekonomii i Innowacji w Lublinie, Lublin 2010

Streszczenie

Służby specjalne zawsze zabezpieczały potrzeby informacyjne uprawnionych podmiotów politycznych i wojskowych państwa. Wykonują swoje ustawowe zadania zarówno w czasie pokoju, kryzysu i wojny. Przemiany systemowe na świecie będące następstwem rozpadu bipolarnego podziału świata, wszechobecna globalizacja, a także postęp naukowo-techniczny to wydarzenia, które zmieniły środowisko bezpieczeństwa międzynarodowego. Pojawiło się wiele nowych zagrożeń, a także uaktywniły się te, które dotychczas były tłumione. Stanowią one wyzwanie dla służb wywiadu i kontrwywiadu praktycznie każdego państwa. Ponadto postępująca współzależność państw, jak i nieprzewidywalne środowisko międzynarodowe sprawiają, że skuteczne wykonywanie zadań przez służby specjalne w sferze wewnętrznego i zewnętrznego bezpieczeństwa państw wymaga ich współpracy zarówno w procesie wymiany informacji, jak i wykonywania czynności operacyjno-rozpoznawczych. Istotne jest również ich przystosowanie pod względem prawnym, organizacyjnym i wyposażenia do zmieniających się warunków w środowisku działania.

Słowa kluczowe: środowisko bezpieczeństwa, szanse, wyzwania, zagrożenia bezpieczeństwa, bezpieczeństwo narodowe, bezpieczeństwo wewnętrzne, bezpieczeństwo międzynarodowe, służby specjalne, globalizacja

Secret Service in the Changing Environment of International Security in the Twenty First Century

Abstract

Secret service has always secured the information needs of eligible political and military state bodies. Its statutory tasks are carried out both in times of peace, crisis and war. Systemic changes in the world resulting from the collapse of the bipolar division of the world, pervasive globalization as well as scientific and technical progress have changed the international security environment. Many new threats have arisen, while those that were so far suppressed have been activated. All that comes as a challenge for the intelligence and counterintelligence services of virtually every country. In addition, a progressive interdependence of the countries as well as the unpredictable international environment cause

that the effective implementation of the tasks carried out by special services in the field of internal and external security requires their cooperation both in the process of exchange of information as well as in performing reconnaissance operations. It is also important to adapt them in legal and organizational terms to the changing conditions of the operational environment.

Keywords: security environment, opportunities, challenges, security threats, national security, homeland security, international security, special services, globalization