FOLIA 352

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 12(1) (2022)

ISSN 2657-8549

DOI 10.24917/26578549.12.1.1

ARTYKUŁY

Andrzej Żebrowski

Uniwersytet Pedagogiczny im. KEN w Krakowie

ORCID ID: 0000-0002-2779-9444

Zagrożenia dla bezpieczeństwa państw w XXI wieku (wybrane aspekty)

Threats to the security of states in the 21st century (selected aspects)

Abstrakt

Występujące zagrożenia dla bezpieczeństwa państwa (państw) naruszają funkcjonowanie ich instytucji i sfery ustawowej odpowiedzialności, co zagraża człowiekowi i jego środowisku. Zróżnicowany charakter ewoluujących źródeł zagrożeń skutkuje odmiennością oddziaływania i możliwości realizowania swoich zadań. Wiele zagrożeń o podłożu narodowościowym, etnicznym czy wyznaniowym nie zostało rozwiązanych w następstwie zakończenia I i II wojny światowej. W okresie bipolarnego podziału świata były kanalizowane, ale jego rozpad skutkował intensywnym rozwojem, co zakłóca bezpieczeństwo i porządek publiczny w wielu państwach. W połączeniu z nowymi zagrożeniami kształtują obecne środowisko bezpieczeństwa poszczególnych państw, gdzie podmioty sektora państwowego i prywatnego zmuszone są adaptować do zachodzących zmian. Szczególne zagrożenia stanowią techniki teleinformatyczne, komunikacyjne i cyberprzestrzeń, w której przeciwnik prowadzi penetrację osobowej i technicznej przestrzeni informacyjnej. Powszechność występowania i zależność wiążą się z możliwością ataku informacyjnego przez przeciwnika, który będzie dążył do zniszczenia znajdujących się w cyberprzestrzeni zasobów. Każdy uczestnik stosunków międzynarodowych wpisuje się w trwającą globalną wojnę informacyjną, która zdominowała środowisko człowieka i dominuje w naszym codziennym życiu. Oznacza to, że będzie ona źródłem wielu zagrożeń, a dominować będzie walka o umysły ludzi. Obrona przed tego rodzaju zagrożeniami jest praktycznie niemożliwa, tym bardziej, że przeciwnik będzie prowadził ofensywne działania zakłócające. Żyjemy w środowisku, gdzie zagrożenia są najczęściej akceptowane przez człowieka. Wymaga to zdecydowanych działań ochronnych, które nie zawsze są skuteczne.

Słowa kluczowe: bezpieczeństwo państwa; zagrożenia; klasyfikacja zagrożeń; trendy związane z zagrożeniami

Abstract

The existing threats to the security of the state(s) violate the functioning of their institutions and the sphere of statutory responsibility, posing a threat to people and their environment. The diversified nature of the evolving sources of threats result in varying impacts and

capabilities to perform the set tasks. Many national, ethnic and religious threats were not resolved following the end of World War I and II. They were channeled during the era of the bipolar division of the world, but its disintegration resulted in dynamic development, which disrupts the security and public order in many countries. Combined with new threats, they shape the current security environment of individual countries, where state and private sector entities are compelled to adapt to the changes taking place. ICT, communications and cyberspace techniques pose particular threats, with the adversaries penetrating the personal and technical information space. Ubiquity and dependence pose the risk of an information attack by the adversary, who will seek to destroy the resources located there. Each participant in international relations is part of the ongoing global information war that has dominated the human environment and our everyday life. This means that it will be a source of multiple threats, and the battle for the minds of people will predominate. Defense against this type of threat is practically impossible, especially that an adversary will conduct disruptive offensive actions. We live in an environment where threats are mostly accepted by humans. This requires strong protective measures that are not always effective.

Keywords: state security; threats; classification of threats; trends related to threats

Wprowadzenie

Zagrożenia zawsze towarzyszą ludzkiemu działaniu. Pod wpływem procesów cywilizacyjnych ulegają ewolucji co do skali i dynamiki występowania. Przemiany systemowe, jakie dokonały się na przełomie XX i XXI wieku, skutkują szerokim spektrum zagrożeń o zróżnicowanym podłożu. Na szczególną uwagę zasługują jednak zagrożenia celowe, których źródłem jest człowiek. Wykorzystując posiadaną wiedzę, umiejętności i dostęp do wielu cennych informacji, realizuje on swoje partykularne cele lub cele instytucji, obcego państwa. XXI wiek to początek globalnej wojny informacyjnej, która wspiera działania uczestników stosunków międzynarodowych w realizacji podstawowych funkcji. Szczególnymi uczestnikami są podmioty dysponujące potencjałem informatycznym i komunikacyjnym. Podatne na atak są przede wszystkim podmioty wysoko usieciowione. Mimo że współczesne środowisko człowieka zdominowała rewolucja naukowo-techniczna, to jednak nadal istnieje wiele zagrożeń, które nadają środowisku asymetryczny charakter. Zagrożenia dotykają niemal wszystkich sfer ludzkiej działalności, ich ewolucja wymusza na podmiotach konieczność monitorowania zachodzących procesów oraz identyfikowanie pojawiających się zagrożeń, z uwzględnieniem już istniejących. W materiale przedstawiono problemy dotyczące istniejących i pojawiających się nowych zagrożeń dla człowieka i jego środowiska, zarówno w otoczeniu wewnętrznym, jak i zewnętrznym państwa (państw).

Charakterystyka problemu

Środowisko bezpieczeństwa międzynarodowego ewoluujące pod wpływem wielu złożonych procesów, tak pozytywnych, jak i negatywnych, ma decydujący wpływ na

skalę i dynamikę zagrożeń, które są obecne w środowisku człowieka. To one kształtują nasze decyzje i działania zarówno w otoczeniu wewnętrznym, jak i zewnętrznym państwa (państw). Zmiany zachodzące we współczesnym świecie po rozpadzie bipolarnego podziału świata to początek jakościowo nowych procesów, które z perspektywy 30 lat przemian systemowych, w nowej rzeczywistości budzą wiele poważnych wątpliwości i problemów w skali globalnej. Okazało się, że na początku XXI wieku stosunki międzynarodowe (wielostronne i bilateralne) daleko wykraczają poza oddziaływanie wyłącznie polityczne, ideologiczne, kulturowe, gospodarcze czy militarne. Na początku nowego stulecia występujące relacje w coraz większym stopniu obejmują swym zasięgiem rozległe sfery: nauki, techniki, kultury, spraw socjalnych czy szeroko rozumianej świadomości społecznej (Dawidczyk, 2001, s. 5). Różnorodne rozwiązania natury technologicznej, wzorce kulturowe i konsumpcyjne, a także idee (nie zawsze o charakterze pokojowym) rozprzestrzeniają się w skali globalnej z nie mniejszą prędkością niż dotychczas wewnątrz poszczególnych państw (Anioł, 1989, s. 6).

Warto mieć na uwadze to, że zagrożenia w ogóle, w tym militarne, pozamilitarne, wewnętrzne i zewnętrzne, naturalne i celowe, mają charakter ponadczasowy, tzn. zawsze występowały w przeszłości, występują aktualnie i będą występowały w przyszłości, a ich skala i dynamika najczęściej nas zaskakuje. Czynniki występujące w otoczeniu wewnętrznym państwa (państw) i w przestrzeni bezpieczeństwa międzynarodowego generują zagrożenia, które wraz z przemianami cywilizacyjnymi będą ulegały ewolucji w czasie i przestrzeni.

Wyróżniające się negatywne procesy w globalnym środowisku bezpieczeństwa sprawiają, że zagrożenia znajdują się w zainteresowaniu wielu podmiotów sektora państwowego i prywatnego, zarówno ze względów politycznych czy gospodarczych, jak i w celu zwalczania zróżnicowanej przestępczości zorganizowanej.

Można postawić tezę, że „elegancja dawnego świata, wyrażająca się w jednoznacznym podziale na ich i nas, dobrych i złych, została zatracona, nastały czasy chaosu i skrajności, gdzie obok społeczeństw walczących o poszerzenie katalogu praw i wolności rosną w siłę fundamentalizm religijny, nacjonalizm, ksenofobia. Klasyczne, twarde zagrożenia bezpieczeństwa, choć nie znikają całkowicie, tracą na znaczeniu, ustępując miejsca innym zagrożeniom jakościowo nowym" (Witecka, 2011, s. 7).

Zagrożenie nie jest jednoznaczne, to sytuacja uświadomiona przez podmiot, który zostaje dotknięty danym zdarzeniem (Hołyst, 1997, s. 64–65). „W tej sytuacji z przedmiotem zdarzenia należy utożsamiać ludzi, ponieważ to oni w największym stopniu odczuwają skutki związane z zaistnieniem zagrożenia. Dlatego też można stwierdzić, iż zagrożenie powiązane jest z trudną sytuacją pojawiającą się podczas odczuwania przez człowieka obaw przed utratą życia oraz pozostałych cenionych wartości" (Kompała, 2014, s. 24).

Na uwagę zasługuje to, że pod pojęciem zagrożenia kryją się zdarzenia spowodowane przyczynami losowymi (naturalnymi) lub nielosowymi (celowymi), które wywierają negatywny wpływ na funkcjonowanie danego systemu lub powodują

niekorzystne (niebezpieczne) zmiany w jego otoczeniu wewnętrznym lub zewnętrznym (Ficoń, 2007, s. 76).

Warto mieć świadomość tego, że w każdym systemie bezpieczeństwa (narodowym i międzynarodowym) istnieją luki, najsłabszym zaś ogniwem jest zawsze człowiek. Jego słabości, a także dążenie do życia w dobrobycie, prowadzenia swobodnego stylu bycia, do swobód i określenia własnej tożsamości, są wykorzystywane przez osoby lub instytucje państw obcych (a niekiedy i własnego państwa). Osoba taka musi być atrakcyjna dla przeciwnika z uwagi na miejsce pracy, dostęp do informacji niejawnych i podatna na podjęcie współpracy.

Zjawiska, zdarzenia i procesy zachodzące w skali globalnej to pasmo przeobrażeń: politycznych, ideologicznych, społecznych, finansowych (elektroniczny pieniądz), ekonomiczno-gospodarczych, naukowych, technicznych, technologicznych, kulturowych i militarnych o trudnych do przewidzenia konsekwencjach. Wymusza to konieczność zmiany poglądów nie tylko na bezpieczeństwo państwa i bezpieczeństwo międzynarodowe, lecz także na zagrożenia, które stanowią jego nieodłączny element.

Szczególnie naganne są celowe działania człowieka polegające na bezwzględnej realizacji własnych celów kosztem interesów innych podmiotów międzynarodowych i wewnętrznych państwa, do użycia przemocy zbrojnej włącznie (w tym również w cyberprzestrzeni). Takie zachowania tworzą potencjalne zagrożenie dla stabilności wewnętrznej i bezpieczeństwa innych podmiotów międzynarodowych m.in. ze względu na możliwości zastosowania przemocy militarnej (Dworecki, 1996, s. 18). Takim przykładem jest konflikt Rosja–Ukraina, Białoruś–Polska, gdzie każdy z uczestników kieruje się partykularnymi interesami polityczno-gospodarczymi i militarnymi o zróżnicowanym podłożu.

Zagrożenie bezpieczeństwa państwa to splot zdarzeń wewnętrznych lub w stosunkach międzynarodowych, w przypadku których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju wewnętrznego bądź naruszenie lub utrata suwerenności państwa oraz jego partnerskiego traktowania w stosunkach międzynarodowych w wyniku zastosowania przemocy politycznej, psychologicznej, ekonomicznej, militarnej itp. (Dworecki, 1994, s. 61). Mogą one powstać na tle uwarunkowań wewnętrznych i/lub zewnętrznych, militarnych i/lub pozamilitarnych; w dowolnej konfiguracji i zróżnicowanym podłożu. Czynnikiem dominującym będą zawsze decyzje polityczne, które mają wpływ na wolę użycia posiadanego potencjału obronno-gospodarczego, podejmowane przez mocarstwa globalne i/lub pretendujące do takiej roli.

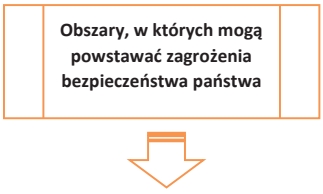
„Pojęcie zagrożenia dla bezpieczeństwa występuje często równolegle z innymi określeniami, takimi jak: patologia społeczna, przestępczość, nieprzystosowanie społeczne, demoralizacja, zachowania dewiacyjne. Zagrożenie dla bezpieczeństwa może przyjąć wszelkie postawy, które naruszają normy etyczne i wyrządzają mniej lub bardziej wymierne szkody społeczne" (Łepkowski, 2009, s. 218).

Tabela 1. Uwarunkowania powstania zagrożeń dla bezpieczeństwa państwa

UWARUNKOWANIA	
WEWNĘTRZNE	**ZEWNĘTRZNE**
MILITARNE (Dworecki, 1994, s. 25)	**POZAMILITARNE** (Łepkowski, 2009, s. 163)
Obejmują taki splot zdarzeń w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju państwa albo naruszenie bądź utrata jego suwerenności i integralności terytorialnej – w wyniku zastosowania wobec niego przemocy zbrojnej (militarnej).	Obejmują taki splot zdarzeń w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju państwa, ewentualnie naruszenie jego suwerenności w wyniku zastosowania wobec niego przemocy niezbrojnej, np. wywieranie nacisku i stosowanie sankcji politycznych lub ekonomicznych.

Źródło: Dostępna literatura przedmiotu.

Rysunek 1. Obszary konfliktotwórcze



polityczne		historyczne
ideologiczne		terytorialne
społeczne		kulturowe
psychologiczne		językowe
etniczne		ekologiczne
narodowościowe		wojskowe
wyznaniowe		naukowe
gospodarcze		informacyjne
finansowe		nacjonalizm, szowinizm, fundamentalizm
ograniczony dostęp do surowców energetycznych		ograniczony dostęp do bezpiecznej wody pitnej
ograniczony dostęp do technologii podwójnego zastosowania		ograniczony dostęp do żywności
globalna przestrzeń informacyjna		ograniczony dostęp do informacji lub jej brak
ekonomiczne		obce i własne służby specjalne
Postępująca anarchizacja życia społeczno-politycznego		
Masowe przemieszczanie się ludności		
Terroryzm międzynarodowy i zorganizowana przestępczość transnarodowa		
WYWIAD I KONTRWYWIAD		
GLOBALNA WOJNA INFORMACYJNA		

Źródło: Opracowano na podstawie (Dworecki, 1996, s. 19).

Podłoża występujących zagrożeń są zróżnicowane, ich występowanie – co do kontynentu, regionu czy państwa – a także ich skala, zakres i dynamika sprawiają, że mogą one powstać na tle napięć i sprzeczności interesów występujących w zasadzie we wszystkich sferach działania człowieka.

Każde zjawisko, wydarzenie czy proces ma indywidualne cechy charakterystyczne i właściwości, które pozwalają na identyfikację zagrożenia (zagrożeń). Obecne zagrożenia charakteryzują się globalizmem, nieprzewidywalnością, gwałtownością i asymetrycznością:

1. Globalizm zagrożeń dotyczy w głównej mierze skutków, jakie mogą generować zagrożenia, oraz sposobu wpływania na inne dziedziny funkcjonowania ludzi, państwa, czy też innych krajów (np. zagrożenia militarne czy też katastrofy naturalne mogą powodować perturbacje na całym świecie, ponieważ wiele państw jest ze sobą powiązanych poprzez różnego rodzaju sojusze oraz umowy międzynarodowe).
2. Nieprzewidywalność wiąże się z brakiem możliwości przewidzenia i określenia miejsca oraz czasu wystąpienia zagrożenia, tak aby istniała możliwość szybkiej oraz skutecznej reakcji. Wiąże się to nierozerwalnie z ograniczeniem skutków, jakie dane zagrożenie może spowodować, oraz z możliwością przygotowania ludzi na jego nadejście.
3. Gwałtowność, która opisuje siłę oraz skalę zachodzącego zjawiska. W bardzo wielu przypadkach gwałtowność zagrożeń jest tak duża, że podobnie jak w przypadku nieprzewidywalności występuje deficyt czasu na skuteczną reakcję.
4. Asymetryczność – można odnieść wrażenie, iż jest ona połączeniem wszystkich powyżej przedstawionych cech, aczkolwiek w asymetryczności należy dodatkowo uwzględnić zaburzenia równowagi w środowisku, a także w występujących na co dzień relacjach, powodujące znaczne trudności w zapanowaniu nad zaistniałym zjawiskiem (Kompała, 2014, s. 25).

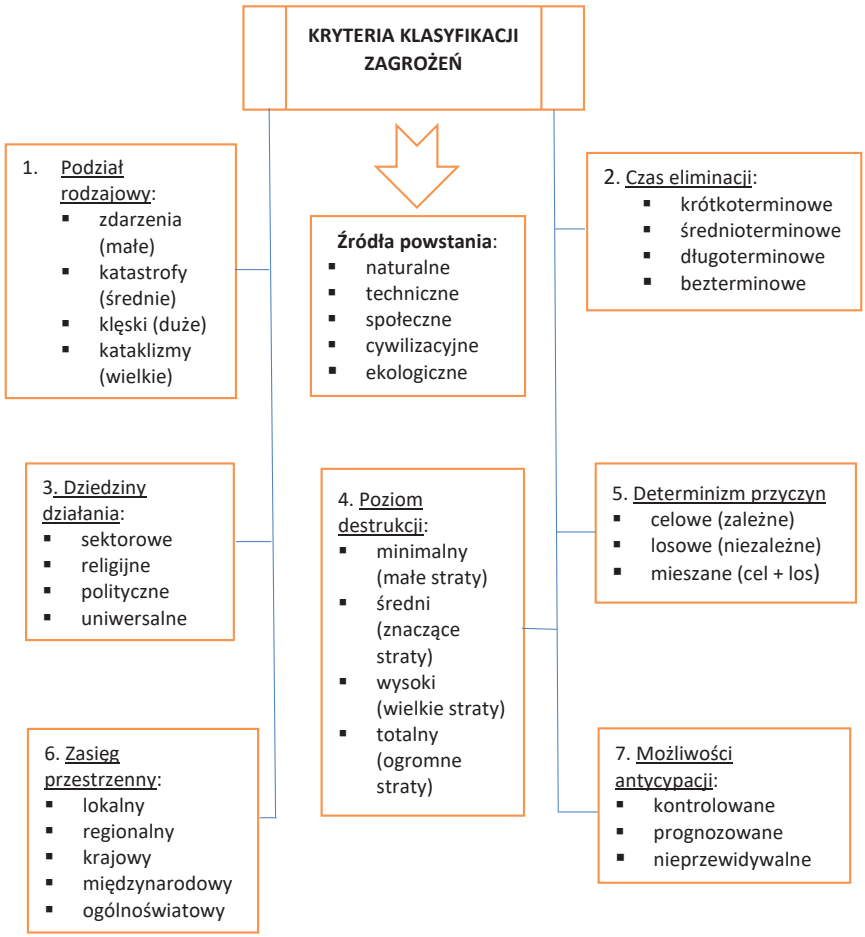
W klasyfikacji zagrożeń wyróżnić można następujące kryteria: źródła powstania, podział rodzajowy, czas eliminacji, dziedzinę działania, poziom destrukcji, determinizm przyczyn, zasięg przestrzenny, możliwość antycypacji (Kompała, 2014, s. 26).

Zagrożenia stanowią pochodną zarówno globalnych, regionalnych, jak i subregionalnych wyzwań bezpieczeństwa państwa w wymiarze narodowym oraz międzynarodowym (Malecki, 2011, s. 26).

Człowiek funkcjonujący w globalnym środowisku bezpieczeństwa i otoczeniu wewnętrznym państwa (państw) styka się z bliżej nieokreśloną liczbą niebezpieczeństw – tych, które zagrażały mu zawsze, i nowych, pojawiających się wraz z przemianami cywilizacyjnymi. Każdy poziom bezpieczeństwa determinowany jest przez istniejące (przyszłe) zagrożenia w danym układzie, a także miejscu i czasie. Również nadmierna eksploatacja i zanieczyszczanie środowiska naturalnego coraz częściej prowadzą do poważnych zagrożeń dla zdrowia i życia człowieka (np. smog). Odmienny charakter mają źródła zagrożeń bezpodmiotowych oraz zagrożeń intencjonalnych, sprawczych (czyli spowodowanych działaniem określonego podmiotu

w określony sposób) (Żuber, 2006, s. 7). Do zagrożeń sprawczych zalicza się zagrożenia umyślne oraz nieumyślne. Ponadto zgodnie ze stanem przygotowania podmiotu (jednostki, grupy społecznej, narodu, państwa, organizacji, firmy) do sytuacji zagrożenia można zaliczyć zagrożenia nieprzewidywalne (nieuświadomione) i przewidywalne (uświadomione) (Wrzosek, 2010, s. 21).

Rysunek 2. Kryteria klasyfikacji zagrożeń



Źródło: Opracowano na podstawie (Ficoń, 2007, s. 78).

„Zagrożenia mogą być zarówno niespodziewane, jako produkt uboczny działań podjętych w celu osiągnięcia konkretnych pozytywnych korzyści, jak i zamierzone, jako wytwór podmiotu dla wykorzystania ich jako instrumentów do umyślnego oddziaływania na inny podmiot, celem osiągnięcia konkretnych negatywnych dla

niego zjawisk. Zagrożenia mogą mieć także charakter ciągły, np. zjawiska przyrodnicze lub elementy programu pewnej grupy społecznej przekazywanego z pokolenia na pokolenie. W takiej sytuacji społeczeństwo często akceptuje zagrożenia jako zjawiska niepożądane, ale realnie istniejące, niemożliwe do wyeliminowania" (Wrzosek, 2010, s. 22).

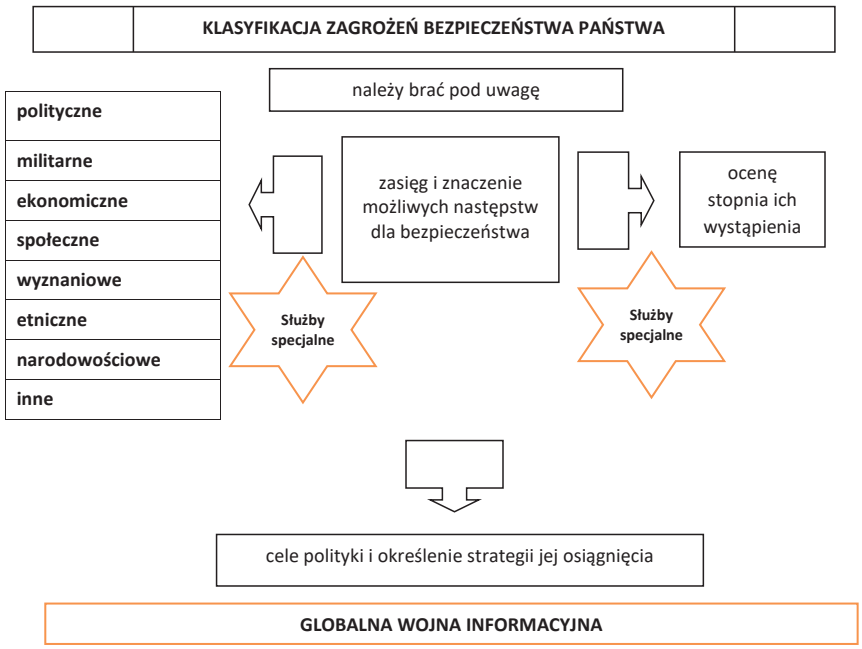
Dzięki takim wyznacznikom jak czas, przestrzeń czy skala oddziaływania można opisać zjawisko zagrożenia w zależności od jego charakteru (militarne i/lub pozamilitarne) oraz wskazać z dużym prawdopodobieństwem poziom mogących wystąpić szkód. Oznacza to konieczność prowadzenia monitoringu miejsc będących źródłem zagrożeń, analizy symptomów wystąpienia negatywnego zjawiska (zdarzenia), jego oceny, podjęcia decyzji oraz uruchomienia posiadanych sił i środków. Nie może to być jednorazowe przedsięwzięcie, a proces, co pozwoli na kontrolowanie zagrożonego środowiska człowieka.

„Procesy, które zachodzą w otoczeniu państwa (państw), stanowią źródła wielu złożonych zagrożeń, zarówno pod względem ilościowym, jak i jakościowym. W wielu przypadkach zagrożeniami są m.in.: środowisko naturalne, występujące anomalie związane z trwającym konfliktem cywilizacyjnym, psychoza wybuchu globalnej wojny, negatywna kooperacja między państwami, trwające konflikty w cyberprzestrzeni, postęp naukowo-techniczny, pandemie i epidemie, działalność służb specjalnych, globalna wojna informacyjna. Stanowią one wysokie ryzyko wystąpienia działań o charakterze destrukcyjnym w państwach (regionach), dotykających następujących obszarów: politycznego, społecznego, ekonomicznego, militarnego, ekologicznego, transportowego, edukacyjnego, prawnego, ochrony zdrowia, ochrony infrastruktury krytycznej, religijnego, kulturowego, informacyjnego, a także tych nowych, które są aktualnie słabymi sygnałami. Dlatego współczesne zagrożenia militarne i niemilitarne, przyrodnicze i cywilizacyjne wymagają wskazania kryteriów ich podziału" (Żebrowski, 2018, s. 34).

Warto mieć na uwadze, że „zagrożenia są nieuniknione, a w niektórych przypadkach stale obecne w otaczającej nas rzeczywistości. Ich przyczyna tkwi w naturze ludzkiej i wówczas mówimy o zagrożeniach celowych związanych z negatywną aktywnością człowieka naruszającego prawo krajowe i/lub międzynarodowe. Należy podkreślić, że zagrożenia celowe (ekologiczne, techniczne, cywilizacyjne, militarne, informacyjne, informatyczne, terroryzm, przestępczość zorganizowana, służb specjalnych) to świadome działania człowieka, których skutki są niekiedy trudne do przewidzenia. Stanowią one największe wyzwanie dla każdego niemal państwa. Ich destrukcyjne skutki mają najczęściej charakter niejawny, co oznacza, że wpisują się w nasze codzienne życie i czynią największe szkody dla jednostki, grupy społecznej, narodu, państwa. Głęboko zakonspirowana działalność naraża obiekt ataku na długofalowe negatywne oddziaływanie. Przy umiejętnym prowadzeniu tego rodzaju działalności fakt ich prowadzenia, a także sprawcy mogą nigdy nie zostać wykryci. Dlatego tak ważna jest znajomość typologii zagrożeń, ich symptomów i przesłanek,

a także konieczność monitorowania otoczenia wewnętrznego i zewnętrznego państwa pod kątem zachodzących tam procesów" (Żebrowski, 2018, s. 35).

Rysunek 3. Klasyfikacja zagrożeń bezpieczeństwa państwa

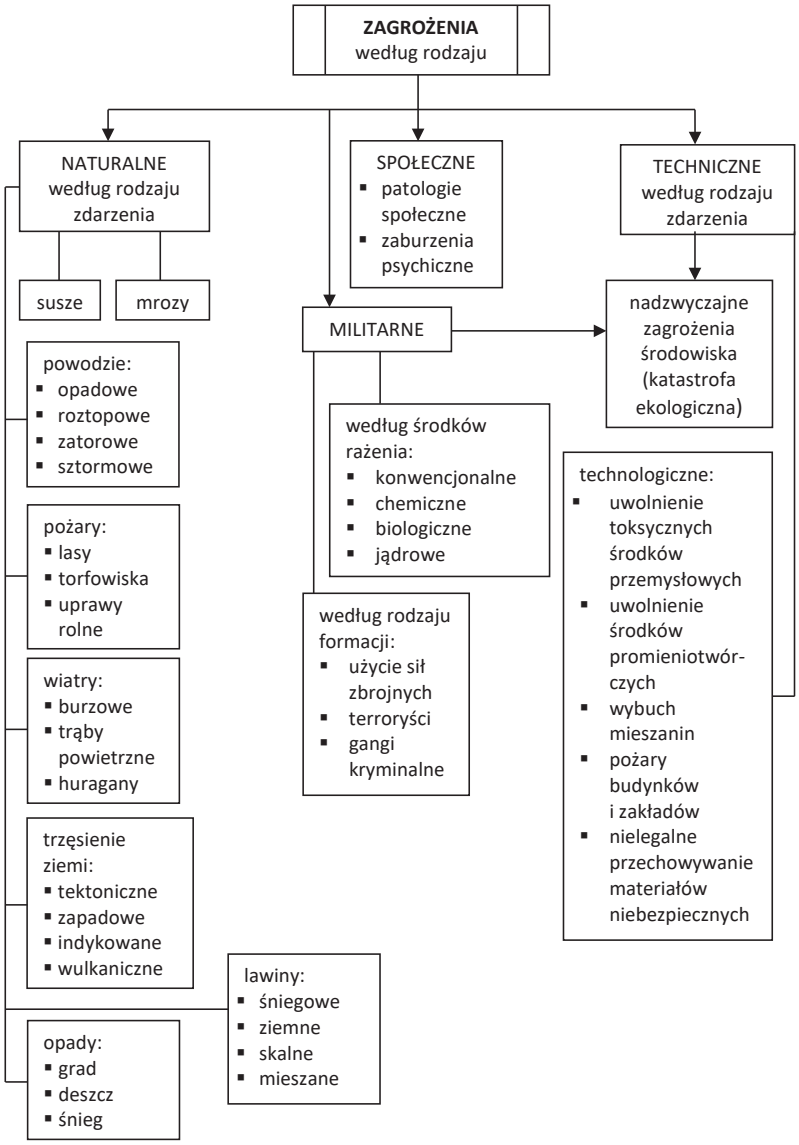


Źródło: Opracowanie własne (Żebrowski, 2018, s. 38).

Początek XXI wieku zdominowany jest przez trwającą globalną wojnę informacyjną, obecną we wszystkich sferach ludzkiej działalności. Stanowi ona zagrożenie dla jednostki, grupy społecznej, narodu, państwa. Swoimi mackami wnika w każdy zakątek świata, gdzie nie tylko zdobywa informacje, ale przede wszystkim zakłóca percepcję czynnych i biernych jej uczestników. Jej negatywne skutki są dostrzegane w okresie trwania COVID-19, zaangażowane podmioty dostosowują się bowiem do zmian zachodzących w skali globalnej i w poszczególnych państwach, a uczestnicy wojny informacyjnej wykorzystują wszelkie dostępne instrumenty pozwalające na prowadzenie walki o ludzi, o ich dusze. Kształtowanie naszej świadomości to cel strategiczny w walce o dominację w środowisku bezpieczeństwa międzynarodowego i w otoczeniu wewnętrznym każdego państwa. Temu złożonemu procesowi towarzyszy wiele złożonych zagrożeń, a informacja jest jednocześnie zasobem, bazą danych i bronią. „Istnieje ścisły związek między postępem cywilizacyjnym a informacją, o którą trzeba walczyć. Konieczność walki o informację prowadzi do

kształtowania się nowych form konfliktów i sposobów ich rozgrywania, tj. walki w obszarze informacji" (S.P., 1997, s. 34–35).

Rysunek 4. Typologia zagrożeń ludności, mienia i środowiska



Źródło: Opracowanie na podstawie (Jakubczak, 2003, załącznik 33).

Systematyczny dopływ informacji m.in. o zagrożeniach, bez względu na ich podłoże, pozwala na budowanie wiedzy, określanie ich skali, dynamiki i charakteru,

a także skutków. Zagrożenia te mogą wystąpić w czasie pokoju, w stanie kryzysu i konfliktu zbrojnego. W procesie identyfikowania, rozpoznawania, a także prognozowania zagrożeń należy mieć na uwadze to, że zderzenie celowej (o charakterze negatywnym) aktywności jednostki, instytucji i sił natury nie tylko prowadzi do trudno przewidywalnych zniszczeń, lecz także stanowi źródło innych zagrożeń, np.: wybuchu epidemii, głodu, pożarów, powodzi, osuwisk ziemi, masowego przemieszczania się ludności, katastrof komunikacyjnych, katastrof technicznych, uwolnienia przemysłowych substancji toksycznych, rozszczelnienia reaktorów jądrowych w elektrowniach, zainfekowania infrastruktury informacyjnej i teleinformatycznej zaliczanej do infrastruktury krytycznej państwa.

Tabela 2. Zagrożenia ludności, mienia i środowiska

Lp.	Zagrożenia	
1	pierwotne (awarie, katastrofy, kataklizmy)	• naturalne (woda, powietrze, ogień, ziemia, kosmos). Spowodowane fizyczno-chemicznymi zjawiskami natury, przyrody, kosmosu, do niedawna jeszcze bez udziału człowieka, • techniczne (komunikacyjne, technologiczne, budowlane, komunalne, nielegalne przechowywanie materiałów niebezpiecznych). Związane z racjonalną (głównie gospodarczą) działalnością człowieka, rozwojem cywilizacyjnym i postępem naukowo-technicznym, • militarne (bezpośrednie użycie sił zbrojnych, akty terroru), • nadzwyczajne zagrożenia środowiska (także niektóre zdarzenia z zakresu zagrożeń technicznych i militarnych o charakterze antropomorficznym)
2	wtórne (klęski żywiołowe)	• zagrożenia egzystencji człowieka (masowe zgony, głód, epidemie i pandemie), społeczne (patologie społeczne: przestępczość, narkomania, prostytucja, masowe bezrobocie, zaburzenia zdrowia psychicznego). Generowane w sposób mniej lub bardziej celowy przez człowieka, postęp kulturalno-cywilizacyjny, a także różne teorie naukowe i poglądy społeczne jednostek, grup i organizacji społecznych, • naruszenie równowagi biologicznej (nadmierny przyrost fauny i flory, epizootie, epifitozy), • masowe straty (zniszczenie lub długotrwałe skażenie środowiska naturalnego, klęska ekologiczna, pomór zwierząt, zniszczenie dóbr niezbędnych do przeżycia)
3	inne (Lidwa, 2010, s. 7)	• zastosowanie broni chemicznej i biologicznej, przede wszystkim w państwach o nieustabilizowanej sytuacji politycznej, • niekontrolowany przepływ broni masowego rażenia i komponentów do jej wytwarzania, w tym substancji radioaktywnych, • międzynarodowy terroryzm, sabotaż, kidnaping, narkomania, zorganizowana przestępczość itp., • duża liczba konfliktów lokalnych o zróżnicowanym podłożu (fundamentalizm, nacjonalizm, wojny religijne), • niekontrolowane i nielegalne migracje, • starzejący się arsenał broni jądrowej i zawodne systemy ostrzegania.
Przyczyny zagrożeń obejmują różne kompilacje powyższych źródeł o zróżnicowanym stopniu ich udziału oraz nowo zaistniałe, nieznane dotychczas kategorie zagrożeń.		

Źródło: Opracowanie na podstawie (Jakubczak, 2003, załącznik 33).

Przemiany cywilizacyjno-kulturowe, trwająca rewolucja naukowo-techniczna, ze szczególnym wskazaniem na techniki teleinformatyczne i komunikacyjne, w połączeniu z celową (negatywną) działalnością człowieka stanowią – obok wielu pozytywnych zjawisk – największe zagrożenie dla ludzkiej egzystencji i środowiska. W związku z tym można wskazać następujące trendy związane z zagrożeniami dla globalnego środowiska bezpieczeństwa i poszczególnych państw:

1. kształtowanie się w świecie nowego ładu politycznego, gospodarczego i militarnego:
   - próby tworzenia stref wpływów lub regionalnej dominacji
   - zastraszanie państw w celu wpływania na ich wolną wolę w kwestii wstępowania do organizacji bezpieczeństwa lub pozostawania poza nimi
   - nastawienie konfrontacyjne w stosunkach międzynarodowych jako wynik mentalności zimnowojennej
   - tworzenie nowych linii podziału w miejsce starych
   - brak wzajemnego zaufania i współpracy w sytuacjach kryzysowych
   - naruszenie zobowiązań wynikających z Karty Narodów Zjednoczonych
   - brak kultury politycznej, nieumiejętność pokojowego rozwiązywania napięć i konfliktów
   - słabość rządów prawa w nowo powstałych państwach, a także w państwach, które wyzwoliły się spod wpływów obcej dominacji
   - terroryzm religijny (w szczególności islamski) jako instrument praktyki politycznej
   - terroryzm ekonomiczny państwa wobec własnych obywateli
   - rozwój przestępczości zorganizowanej w skali globalnej, regionalnej, subregionalnej i lokalnej
   - rozruchy i niepokoje społeczne ludności na tle polityki migracyjnej państw, organizacji międzynarodowych
   - rozruchy i niepokoje społeczne ludności na tle polityki wewnętrznej, sprzeciw wobec naruszania zasad demokracji i państwa prawa
   - akty piractwa morskiego (Dawidczyk, 2001, s. 39–40);
2. nabierająca tempa dynamika państwowo-narodowej struktury świata:
   - spory wewnętrzne i zewnętrzne powstałe na tle etnicznym, terytorialnym oraz dążeń narodowych do uzyskania suwerenności w państwach europejskich
   - agresywne ruchy secesjonistyczne
   - terroryzm sterowany przez państwa i organizacje niepaństwowe
   - próby tworzenia stref wpływów lub regionalnej dominacji przez mocarstwa regionalne
   - migracje na tle ekonomicznym i politycznym, ludobójstwa (Dawidczyk, 2001, s. 41);
3. gwałtowny postęp naukowo-techniczny:
   - terroryzm jako wynik zmian w zakresie dostępu do nowych technik negatywnego oddziaływania i niszczenia. Nowe formy terroryzmu: cyberterroryzm, terroryzm ekologiczny, superterroryzm

- zwiększona podatność państw, organizacji niepaństwowych, banków, instytucji międzynarodowych na możliwość destruktywnego informatycznego, elektronicznego, cybernetycznego oddziaływania
- narodziny nowej klasy społecznej, tzw. klasy kognitatorów, ludzi nieuznających tradycyjnych wartości związanych z instytucją państwa narodowego, poszukujący swojej szansy w świecie wirtualnym ze szkodą dla państwa – oraz negatywne oddziaływanie tej klasy na tradycyjne struktury państwowe
- niepokoje i rozruchy społeczne na tle bezrobocia jako efektu postępu technicznego
- pogłębiające się frustracje społeczne na tle rosnącego zapóźnienia technologicznego państw w stosunku do Zachodu (Dawidczyk, 2001, s. 42);

4. postępująca dyfuzja cywilizacyjno-kulturowa:
   - rozrost sekt religijnych i ich negatywny wpływ na system społeczny poszczególnych państw
   - ruchy polityczne odwołujące się do agresywnego nacjonalizmu, rasizmu, ksenofobii, antysemityzmu i innych form nietolerancji
   - dehumanizacja stosunków społecznych
   - erozja autorytetu władzy
   - rozwój terroryzmu spowodowany falą fundamentalizmu, poczuciem etnicznej odrębności, nieuznawaniem odmiennych wartości
   - alienacja społeczeństwa, rozwój przestępczości, bezrobocie i inne patologie społeczne (Dawidczyk, 2001, s. 44);
5. osiąganie przez cywilizację granic biosfery:
   - zanieczyszczenie i skażenie przez odpady nuklearne i chemiczne terenów objętych klęską ekologiczną
   - kurczące się zasoby surowców naturalnych, w szczególności paliw kopalnych decydujących o przetrwaniu państw
   - podnoszenie się poziomu oceanu światowego na skutek topnienia śniegu w obszarach podbiegunowych; zalewanie nisko położonych obszarów
   - spadek poziomu dostępnych zasobów wody pitnej i przewidywane konflikty na tym tle
   - erozja i zanieczyszczenia gleby poprzez zbyt intensywną produkcję rolniczą; problemy z wyżywieniem rosnącej populacji świata
   - masowe migracje ludności z terenów objętych klęskami żywiołowymi i głodem (Dawidczyk, 2001, s. 44–45);
6. przechodzenie od mechanistycznej do systemowej wizji świata:
   - mechanistyczne postrzeganie współczesnego świata; wynikający z tego brak zdolności zarówno organizacyjnych, jak i funkcjonalnych do aktywnego dostosowania organizacji państwowych do wczesnego reagowania na pojawiające się zagrożenia oraz podejmowania działań uprzedzających, kreatywnych

- zjawisko globalnej wioski jako czynnik dezintegrujący tradycyjne struktury społeczne, powodujący erozję autorytetu władzy, pozbawiający obywateli tradycyjnej ochrony, którą roztaczało państwo
- utrwalający się podział kulturowy między cywilizacjami owocujący falą fundamentalizmu religijnego
- narastanie znaczenia aktorów ponadpaństwowych i niepaństwowych – konsekwencją tego będzie coraz częstsza praktyka przechodzenia szeregu kompetencji państwa na rzecz innych aktorów sceny światowej, co stanowi zagrożenie dla realizacji długofalowej polityki gospodarczej prowadzonej przez władze; prowadzić to może do narastania negatywnych nastrojów społecznych, konfliktów wewnątrz państw
- uniezależnienie się podmiotów niepaństwowych i korporacji od decyzji politycznych i gospodarczych państw, na terytoriach których się znajdują; skutkiem tego narastanie sprzeczności prowadzących do konfliktów, a nawet nowego typu wojen (np. informatycznych, w cyberprzestrzeni)
- marginalizacja, peryferyzacja i kolonizacja przez inne państwa/struktury ponadnarodowe
- turbulencyjność i nieprzewidywalność (Dawidczyk, 2001, s. 45–47);

7. zbieżność lub integracja techniczna:
   - konflikty o prawa dostępu do informacji, przetwarzania informacji, dystrybucji informacji
   - cyberprzestrzeń jako obszar konfliktu
   - rozszerzająca się luka technologiczna między powstającymi ośrodkami potęgi w świecie: Europą, Stanami Zjednoczonymi, Chinami, Japonią, państwami Bliskiego Wschodu
   - informacja jako czynnik rozwarstwienia w gospodarce światowej
   - zjawisko globalnej wioski jako czynnik dezintegrujący tradycyjne struktury społeczne, powodujący erozję autorytetu władzy, pozbawiający obywateli tradycyjnej ochrony, którą roztaczało państwo
   - narastanie wewnętrznych napięć w poszczególnych państwach, związane z polaryzacją społeczeństw: pracownicy nauki i eksperci wchodzą do elit władzy, dominująca zaś część populacji pozostaje w sferze zunifikowanej w skali światowej subkultury masowej
   - zróżnicowanie potencjału technicznego staje się trudnym do wyrównania czynnikiem utrwalającym nierówność informacyjną w skali światowej
   - stale narastający rozwój zorganizowanej przestępczości, szczególnie przestępczości wykorzystującej cyberprzestrzeń i korzystającej z osiągnięć technologii umożliwiającej konstruowanie i użycie broni masowego rażenia
   - rosnąca liczba przestępstw bankowych, skarbowych, kryminalnych, których środowiskiem będzie przestrzeń cybernetyczna
   - informatyzacja i militaryzacja przestrzeni kosmicznej (Dawidczyk, 2001, s. 48).

Zagrożenia zewnętrzne i wewnętrzne państwa

Otoczenie wewnętrzne i zewnętrzne każdego państwa generuje wiele złożonych zagrożeń o zróżnicowanym charakterze i podłożu. Procesy związane z globalizacją sprawiają, że granice między bezpieczeństwem wewnętrznym i zewnętrznym się zacierają, a zachodzące tam procesy wzajemnie się przenikają, co czyni je złożonymi i trudnymi do rozpoznania oraz przeciwdziałania im. Ich wzajemne nakładanie się sprawia, że ich źródła są niekiedy trudne do wskazania i zidentyfikowania. Przeciwnik stosuje zróżnicowane formy maskowania, wykorzystywane są propaganda, dezinformacja, manipulacja, kłamstwo, przy czym maskowanie to nieodzowne elementy globalnego środowiska bezpieczeństwa międzynarodowego. Stanowi to poważne zagrożenie w zasadzie dla każdego podmiotu, w przypadku którego dominują operacje informacyjne ukierunkowane na zakłócanie percepcji przeciwnika.

Globalizacja i aktywność informacyjna uczestników stosunków międzynarodowych w złożonym i asymetrycznym środowisku generują zagrożenia, które wraz z przemianami cywilizacyjnymi występują zarówno w otoczeniu wewnętrznym, jak i zewnętrznym państwa (państw).

Tabela 3. Uwarunkowania wewnętrzne i zewnętrzne zagrożeń bezpieczeństwa państwa

UWARUNKOWANIA	
WEWNĘTRZNE (Łepkowski, 2009, s. 164)	**ZEWNĘTRZNE** (Łepkowski, 2009, s. 164)
To stan w państwie, który uniemożliwia organom władzy utrzymanie ładu i porządku publicznego oraz zachowania życia i mienia ludności, a także korzystanie z praw i swobód obywatelskich zagwarantowanych konstytucją i innymi przepisami prawa.	Zagrożenie, w wyniku którego zwiększone jest prawdopodobieństwo utraty lub ograniczenia suwerenności czy też integralności terytorialnej państwa, źródłem tego zagrożenia jest inne państwo (najczęściej ościenne).

Źródło: Dostępna literatura przedmiotu.

Zgodnie z postanowieniami Aktu Końcowego KBWE za zagrożenie zewnętrzne bezpieczeństwa uznaje się naruszenie przez państwo, w stosunku do innego państwa, jednej z następujących zasad:

1. suwerennej równości, poszanowania praw nieodłącznych od suwerenności;
2. powstrzymywania się od groźby użycia siły lub samego jej użycia;
3. nienaruszalności granic;
4. integralności państwa;
5. pokojowego załatwiania sporów;
6. nieingerencji w sprawy wewnętrzne;
7. poszanowania praw człowieka i podstawowych rodzajów wolności, łącznie z wolnością myśli, sumienia, wyznania lub przekonań;
8. równouprawnienia i praw narodów do samostanowienia;
9. partnerskiej współpracy między państwami;
10. wypełniania w dobrej wierze zobowiązań wynikających z prawa międzynarodowego (Dworecki, 1996, s. 23).

Przyjmuje się, że bezpieczeństwo państwa może być zagrożone, jeżeli występują systemowe sprzeczności pod względem:

1. uznawanych wartości, tzn. celów, potrzeb, interesów, aspiracji, dążeń;
2. determinant stabilności wewnętrznej i interpretacji suwerenności państwa;
3. oceny zachowań i intencji podejmowanych działań;
4. postrzegania i oceniania rzeczywistości, traktowane jako zjawiska konfliktotwórcze proste lub złożone (kombinacja prostych), powstające na zidentyfikowanym podłożu (Dworecki, 1996, s. 19).

Wskazane sprzeczności są obecne w procesie realizacji nie tylko polityki zagranicznej, ale także wewnętrznej, która znajduje się pod wpływem procesów występujących w środowisku bezpieczeństwa międzynarodowego. Ich wzajemne przenikanie się generuje zagrożenia, których destrukcyjny charakter dotyka nie tylko jednostki czy grupy społeczne, ale narody, państwa, subregiony, regiony, kontynenty. Jest to szczególnie widoczne w trwającej wojnie dyplomatycznej (2020/2021 i 2022), w której dominujące podmioty w globalnym środowisku bezpieczeństwa: Stany Zjednoczone i Federacja Rosyjska prowadzą ofensywne operacje informacyjne, kierując się własnymi celami politycznymi i ekonomiczno-gospodarczymi. Strategie bezpieczeństwa narodowego, doktryny wojenne i posiadane potencjały militarne, wspierane przez agresywne cele polityczne i państwa zależne, stanowią zagrożenie dla środowiska bezpieczeństwa międzynarodowego.

„Za zagrożenia zewnętrzne uznaje się te czynniki destrukcyjne, których skutki lub straty są odczuwalne poza podmiot je generujący. Występują one w jego otoczeniu i środowisku. Są nimi zagrożenia wobec innego podmiotu bezpieczeństwa, wynikające z aktywności zewnętrznej podmiotu, takie jak: użycie siły i przemocy, agresja, podbój terytorium, działania militarne i niemilitarne, polityczne, ekologiczne, ekonomiczne, ideologiczne, technologiczne i naukowe czy kulturowe. Efektem występowania zagrożeń zewnętrznych jest utrata stabilności i bezpieczeństwa podmiotu bezpieczeństwa wyższej rangi, jak organizacji międzynarodowych (Unia Europejska) lub sojuszy militarnych (Sojusz Północnoatlantycki)" (Sójka, 2017, s. 183).

Z kolei za zagrożenia wewnętrzne bezpieczeństwa państwa uważa się zespół przyczyn, których źródłem są elementy struktury państwa prowadzące do destabilizacji sytuacji lub naruszenia podstawowych wartości, takich jak:

1. wola przetrwania (państwa, narodu);
2. terytorialna integralność;
3. niezależność polityczna, suwerenność wyboru ustroju społeczno-politycznego oraz swoboda w podejmowaniu decyzji dotyczących polityki wewnętrznej i zewnętrznej;
4. jakość i warunki życia (zachowanie odpowiedniego standardu życiowego społeczeństwa i perspektyw wszechstronnego rozwoju) (Dworecki, 1996, s. 24).

W innym ujęciu zagrożenia dla bezpieczeństwa są rozumiane jako:

1. zaburzenie wzorców i mechanizmów stosunków międzyludzkich;
2. procesy, przez które stosunki w grupach zostają rozbite;

3. niedostosowanie społeczne będące następstwem podziału kulturowego (Hołyst, 2014, s. 281).

Poczucie zagrożenia co do zaspokojenia potrzeb egzystencjalnych może się wyrażać w nastrojach, emocjach i opiniach człowieka, grupy zawodowej lub środowiskowych grup społecznych. Stanowią one bardzo czuły wskaźnik stosunku wskazanych podmiotów do władzy, partii politycznych, organizacji społecznych, a także wydarzeń międzynarodowych i zachodzących w otoczeniu wewnętrznym państwa. Zagrożenia uzewnętrzniają się najczęściej w negatywnym charakterze zachowań, poczynając od niezadowolenia, a na agresji kończąc. „Te negatywne zachowania mają bezpośredni wpływ na stabilność wewnętrzną państwa. Im szerszy krąg wyraża swoją dezaprobatę dla zachodzących w ich otoczeniu procesów, tym większe ich zagrożenie" (Dworecki, 1996, s. 30). Zjawiska destabilizujące sytuację wewnętrzną powstają w następujących procesach:

1. tworzenia warunków socjalno-bytowych;
2. gwarantowania bezpieczeństwa i swobód obywatelskich;
3. prywatyzacji i reprywatyzacji;
4. kreowania polityki przemysłowej, rolnej i usług;
5. rozwoju nauki, techniki i technologii, ochrony środowiska naturalnego;
6. tworzenia prawa i jego przestrzegania (Dworecki, 1996, s. 30).

Wskazane procesy niewątpliwie zawierają wspólne elementy przyczynowo-skutkowe, ponadto zależą również od innych warunków, jakie występują w otoczeniu wewnętrznym i zewnętrznym państwa (bliższym i dalszym).

Do zjawisk destabilizujących sytuację wewnętrzną państwa można zaliczyć: arogancję władzy; korupcję urzędników; recesję gospodarczą i wzrastające zadłużenie państwa; złe gospodarowanie mieniem państwowym i spółdzielczym; zjawiska nacjonalizmu, szowinizmu, fundamentalizmu religijnego; ubożenie społeczeństwa i utrzymujące się bezrobocie; utratę praw nabytych; ograniczanie praw i swobód obywatelskich; brak stabilnych unormowań prawnych i sprawnego wymiaru sprawiedliwości; ograniczanie dostępu do surowców naturalnych i nowoczesnych technologii; trudności w wymianie handlowej, naukowej i kulturalnej mające często charakter restrykcyjny; nasilające się dążenia rewindykacyjne; próby ograniczania tożsamości narodowej i wyznaniowej; masowe migracje i tzw. pseudoturystykę; ekspansję obcych kultur i inne (Dworecki, 1996, s. 31–33).

Na podkreślenie zasługuje jednak demagogiczna retoryka polityków i spadek ich wiarygodności (czarę goryczy przelewają pustosłowie i koniunkturalna polityka elit politycznych widoczna w kolejnych kampaniach wyborczych. Okazuje się, że łatwiej zdobyć władzę, niż ją sprawować z korzyścią dla dobra społeczeństwa. Przyczyna tego stanu rzeczy tkwi w kolizji ideologii i sposobu sprawowania władzy z indywidualnymi ambicjami politycznymi członków elit władzy) (Dworecki, 1996, s. 33).

Procesy zachodzące w otoczeniu zewnętrznym państw silnie oddziaływają na ich otoczenie wewnętrzne. Okazuje się, że zagrożenia bezpieczeństwa państw z uwagi na sprzeczności interesów grup społecznych, narodowościowych, etnicznych

i wyznaniowych mają tendencje wzrostowe. Dzieje się to za sprawą mniejszości narodowych i wyznaniowych, a także masowej migracji, co w połączeniu z sytuacją społeczno-polityczną i gospodarczą państwa oraz odczuwalnym brakiem poprawnych warunków socjalno-bytowych może prowadzić do destabilizacji życia wewnętrznego. Brak rozsądnych zachowań elit politycznych, reakcji administracji państwowej, a także podejmowanych decyzji i działań najczęściej prowadzi do eskalacji niezadowolenia społecznego. Sprzyja to m.in. rozwojowi przestępczości zorganizowanej o charakterze międzynarodowym, a nawet terroryzmu, tym bardziej że mniejszości narodowe (wyznaniowe) stanowią bazę werbunkową dla jednostek, instytucji przeciwnika. Ponadto mniejszości narodowe, etniczne czy religijne stanowią narzędzie oddziaływania ideologicznego, politycznego, kulturowego, gospodarczego, a nawet mogą stać się przyczyną interwencji militarnej państw graniczących, występujących w obronie swoich obywateli.

W przypadku państwa zagrożenie to odnosi się do respektowania prawa, porządku i ładu powszechnego, ochrony życia, mienia i zdrowia oraz istnienia sprawnej instytucji politycznej reprezentującej społeczeństwo zorganizowane w naród i władzę (Sójka, 2017, s. 183).

Współczesnym, a zarazem globalnym, dominującym i wszechobecnym zagrożeniem dla bezpieczeństwa właściwie każdego podmiotu są zagrożenia informacyjne. Komputeryzacja, informatyzacja i powstanie globalnej sieci informacyjnej (Internetu) stwarzają jakościowo nowe możliwości zdobywania, przetwarzania i przesyłania informacji w zróżnicowanej formie. „Nowoczesne techniki i technologie wykorzystywane w procesie przekazywania informacji o różnorodnym przeznaczeniu i stopniu ważności są praktycznie dostępne bez żadnych ograniczeń. Ta rewolucja techniczna stwarza warunki do stworzenia koncepcji osiągnięcia zwycięstwa przez wykorzystanie instrumentów walki informacyjnej. Według poglądów specjalistów z wielu krajów technika informacyjna jest podstawową bronią XXI wieku, a pod względem skuteczności oddziaływania jest porównywalna z bronią masowego rażenia" (Żebrowski, 2002, s. 333–334).

Osobowe i techniczne przestrzenie informacyjne funkcjonujące w przestrzeni walki informacyjnej narażone są na penetrację. Znajdują się one w zainteresowaniu wielu podmiotów, w tym najczęściej do tego nieuprawnionych. „Stykamy się z zagrożeniami związanymi m.in. ze szpiegostwem, sabotażem, terroryzmem (klasycznym i informatycznym), czy też sfrustrowanymi członkami organizacji zróżnicowanymi co do charakteru prowadzonej działalności. Zagrożenie dla systemów informacyjnych i informatycznych stanowi każdy, kto posiada wiedzę i umiejętności praktyczne pozwalające na wykonanie ataku na wytypowany system. Można spotkać się z następującymi typami ataku informacyjnego:

1. zerwanie procedur związanych z wymianą informacji;
2. manipulowanie informacją (dezinformacja, zatajenie, zniekształcenie);
3. korzystanie z automatycznego dostępu do zasobów informacyjnych, a także nielegalne pozyskiwanie i wykorzystywanie informacji;

4. nielegalne kopiowanie danych zawartych w systemach informacyjnych, w tym bazach i bankach danych;
5. masowe niszczenie oprogramowania specjalnego" (Żebrowski, 2002, s. 336).

Aktualnie można wskazać następujące formy wojny informacyjnej, którymi są: postęp, atak informacyjny, zakłócanie informacyjne, działania psychologiczne, niszczenie fizyczne, walka elektroniczna i ochrona informacji niejawnych.

„Korzyści, jakie wynikają z funkcjonujących systemów informacyjnych, są oczywiste i wszyscy taką wiedzę na ten temat posiadają. Wiążą się z tym określone zagrożenia, które poprzez kompleksowe przedsięwzięcia prawno-organizacyjne i techniczne mogą być minimalizowane, a nawet wyeliminowane" (Żebrowski, 2002, s. 337). Można zatem wskazać następujące obszary zagrożeń dla systemów komputerowych:

1. wiarygodność personelu i jego kwalifikacje;
2. centra administracyjne systemu i sieci;
3. infrastruktura telekomunikacyjna;
4. produkcja sprzętu i oprogramowania;
5. nośniki danych;
6. procedury korzystania z systemów i sieci komputerowych (Rączkiewicz, 1995, s. 3).

Powszechny dostęp do technologii komunikacyjnych i informacyjnych zdominował wszystkie sfery działalności naszego codziennego życia. Informatyzacja życia, w związku z rozwojem wszechobecnego Internetu, przynosi wszystkim znaczące korzyści, jednak wiąże się z nią także szereg niebezpieczeństw. Tej formie działalności towarzyszą bowiem całkowicie nowe zagrożenia dla jednostki, instytucji, a nawet dla całych społeczeństw (Białas, 2002, s. 11). Jest to pasmo zagrożeń zarówno celowych, jak i przypadkowych.

Tabela 4. Podział zagrożeń według kryteriów źródła pochodzenia oraz motywacji

	CELOWE	PRZYPADKOWE
wewnętrzne	**Działania legalnych wewnętrznych użytkowników**: • akt zemsty na pracodawcy, • uzyskanie korzyści majątkowych, • szpiegostwo, • sabotaż, • szantaż pracownika, • akt cyberterroryzmu	**Niezamierzone działania legalnych użytkowników:** • błędy operatorów w użytkowaniu programów, • wady oprogramowania, • wady sprzętu, • zalania w sieci wod.-kan. lub c.o., • awarie infrastruktury (klimatyzacja, uszkodzenia sieci teledacyjnych, przepięcia lub przeciążenia sieci zasilającej)
zewnętrzne	**Cyberprzestępczość:** • cyberterroryzm, • szpiegostwo, • wojna w cyberprzestrzeni, • działania tzw. haktywistów przeciwko systemom informatycznym, • działania zmierzające do nieuprawnionego pozyskiwania informacji lub dostępu, np. przez przedstawicieli mediów informacyjnych	**Powódź, trzęsienie ziemi, huragan, wyładowania atmosferyczne, inne klęski żywiołowe:** • pożar, zalanie spowodowane opadami deszczu, • zawilgocenie, zapylenie, opary chemiczne, • długotrwałe braki w dostawie prądu, • przerwy i zakłócenia w dostępie do sieci teleinformatycznej

Źródło: Opracowanie na podstawie (Barczak, Sidoruk, 2003, s. 77).

Komercjalizacja i powszechność Internetu stanowią zaproszenie dla oszustów, złodziei, handlarzy pornografią dziecięcą, dilerów narkotykowych oraz wszelkiego typu osobników (np. terrorystów, zorganizowanych grup przestępczych, służb specjalnych, najemników), którzy stanowią zagrożenie dla bezpieczeństwa państwa (Shinder, 2004, s. 15). Zjawiska te stwarzają ponadto możliwość propagowania wrogich idei, poglądów, szerzenia nienawiści o zróżnicowanym podłożu, a także tworzą miejsce na dyskusję o wojnie między cywilizacjami (zachodnią i islamską), wojnie religijnej prowadzonej w XXI wieku. Co więcej, dają możliwość totalnej inwigilacji oraz mogą być miejscem przyszłej bitwy. Nie bez znaczenia jest również związana z nimi kwestia widma elektromagnetycznego – oznacza bowiem, że przyszłe pole walki będzie roić się od impulsów elektromagnetycznych, spośród których jedne służyć będą komunikacji, inne nawigacji, a jeszcze inne mogą wyrządzić ludziom krzywdę (Latiff, 2018, s. 35).

Tabela 5. Obszary zagrożeń dla systemów komputerowych

Lp.	OBSZAR ZAGROŻEŃ	CZYNNIKI ZWIĄZANE ZE ŚWIADOMĄ DZIAŁALNOŚCIĄ CZŁOWIEKA (ZAGROŻENIA AKTYWNE)	CZYNNIKI NIEZALEŻNE OD CZŁOWIEKA LUB ZWIĄZANE Z JEGO NIEŚWIADOMOŚCIĄ (ZAGROŻENIA PASYWNE)
1	centra administrowania systemami i siecią	• sabotaż, • podpalenia, • strajki okupacyjne	• klęski żywiołowe, • awarie instalacji: zasilania, klimatyzacji, gaśniczej
2	infrastruktura telekomunikacyjna	• podsłuch linii	• błędy związane z przesyłaniem, adresowaniem danych
3	produkcja sprzętu i oprogramowania	• kopiowanie oprogramowania, • wprowadzanie wirusów do programów, • nieuczciwość firm oferujących oprogramowanie z nieprofesjonalnymi rozwiązaniami zabezpieczającymi	• wykorzystywanie nieaktualnych wersji programów lub plików
4	procedury korzystania z systemów i sieci informatycznych	• świadome wprowadzanie błędnych danych, • kopiowanie, podmiana, niszczenie plików	• błędy w trakcie wprowadzania danych, • zniszczenie plików przez nieuwagę
5	nośniki danych	• kradzież lub podmiana nośników, • kopiowanie nośników w celu analizy danych	• błędy przy manipulacji nośnikami powodujące utratę danych, • zniszczenie danych polem magnetycznym lub elektrycznością statyczną

Źródło: Opracowanie na podstawie (Rączkiewicz, 1995, s. 3).

Wspomniany rozwój technik teleinformatycznych i komunikacyjnych, ich wszechobecność oraz zależność sprawiają, że są one podatne na atak przeciwnika, przede wszystkim w cyberprzestrzeni. W istniejących systemach informatycznych

wzrasta penetracja rozległych i lokalnych sieci teleinformatycznych, które obsługują zautomatyzowane systemy zarządzania, dowodzenia, rozpoznania, oraz zautomatyzowane systemy kierowania uzbrojeniem. Stanowią one bogate źródło informacji dla uczestników kooperacji negatywnej. Bogate i niezmiernie wartościowe informacje czerpie się także z promieniowania samych komputerów oraz ich urządzeń wejścia i wyjścia. „Narażone są na penetrację i dostęp do ich baz danych, a zgromadzone w nich zasoby i strumienie danych stają się obiektami rozpoznania, modyfikacji lub zniszczenia. Włączenie się do nich nieupoważnionych użytkowników jest stosunkowo łatwe. Mogą oni śledzić, podsłuchiwać i przechwytywać dane, a także prowadzić dezinformację bądź niszczenie" (Janczak, 2001, s. 134). Warto mieć na uwadze to, że ten rodzaj „zakłócania dotyczy wszystkich poziomów działań na informacjach, pozyskiwania, przetwarzania, przesyłania i przechowywania. Zakłócanie obejmuje penetrację bierną stanowiącą zagrożenie dla zachowania tajemnicy oraz penetrację aktywną, zagrażającą autentyczności danych" (Janczak, 2001, s. 136).

Aktywność informacyjna, której celem jest zakłócanie informacyjne, ma za zadanie neutralizowanie wszelkiej działalności uczestników kooperacji negatywnej w osobowej i technicznej przestrzeni informacyjnej. Rozwój technik teleinformatycznych i komunikacyjnych sprawia, że główne zainteresowanie obejmuje przede wszystkim penetrację technicznej przestrzeni informacyjnej. „Jednak jego skuteczność wymaga również prowadzenia zakłócania informacyjnego w osobowej przestrzeni informacyjnej, gdzie obiektem ataku jest człowiek, przy czym może to być jednostka, grupa społeczna, naród lub społeczność międzynarodowa. Zakłócanie w tej przestrzeni jest realizowane przez wyspecjalizowane agendy rządowe (najczęściej aparat dyplomatyczny, wywiad i kontrwywiad). Tego rodzaju działania są również podejmowane przez podmioty biznesowe, zorganizowane grupy przestępcze, organizacje terrorystyczne i najemników XXI wieku" (Żebrowski, 2018, s. 390).

W procesie zakłócania informacyjnego szczególną rolę przypisuje się informacji niszczącej, która jako instrumentarium walki informacyjnej spełnia dwie zasadnicze funkcje:

- Po pierwsze, służy szeroko rozumianemu pozorowaniu, mającemu na celu wprowadzanie przeciwnika w błąd. Jego celem jest udostępnienie przeciwnikowi takich postaci danych, które po przetworzeniu będą przedstawiać sytuację nierealną, a zarazem maksymalnie stwarzającą pozory działań rzeczywistych.
- Po drugie, powoduje dezorganizację pracy systemów zarządzania bezpieczeństwem państwa, dowodzenia wojskami, łączności, rozpoznania, kierowania uzbrojeniem przeciwnika oraz dąży do fizycznej destrukcji nośników danych (Janczak, 2001, s. 15).

Niszczenie w ramach zakłócania informacyjnego najczęściej przyjmuje postać ataku informacyjnego, który jest realizowany w następujących formach:

1. ataku informatycznego (w sferze przetwarzania danych cyfrowych);
2. ataku elektronicznego;
3. ataku ogniowego;

4. działań psychologicznych;
5. dezinformacji (mylenia) (Szpyra, 2003, s. 109).

Na szczególną uwagę zasługuje jednak atak ogniowy, który skutkuje fizycznym zniszczeniem wszystkich elementów infrastruktury krytycznej państwa (infrastruktur sektorowych), w tym infrastruktury informacyjnej i informatycznej, a także personelu. Ten rodzaj ataku należy postrzegać w kategorii przemocy militarnej, która jest wynikiem zewnętrznej aktywności politycznej państwa, ukierunkowanej na realizację określonych celów (w tym politycznych, gospodarczych, wojskowych), gdzie obiektem ataku są systemy informacyjnego komunikowania i zasoby informacyjne przeciwnika.

*

Współczesny świat zdominowany przez trwający postęp naukowo-techniczny, szczególnie widoczny w technikach teleinformatycznych i komunikacyjnych, stanowi poważne wyzwanie dla społeczności międzynarodowej. Wyzwanie to oznacza zarówno szanse, jak i zagrożenia dla technicznej i osobowej przestrzeni informacyjnej. Ogólnoświatowe środowisko bezpieczeństwa zdominowane jest przez inwigilację w globalnej przestrzeni informacyjnej.

Niejawne i systematyczne zbieranie informacji o przeciwnikach politycznych, państwach sąsiedzkich czy sojuszniczych było realizowane od początku istnienia państwowości (Chrzczonowicz, Kwiatkowska-Darul, Skowroński, 2003, s. 11). Na przełomie XX i XXI wieku zapoczątkowano prowadzenie intensywnej kontroli społeczeństwa, której skala i skuteczność są wspierane przez postęp w nauce i technice (Bauman, 2013, s. 5).

Kontrola społeczeństwa jest związana z inwigilacją, która w kryminalistyce oznacza „działalność legalną, a nawet konieczną w każdym współczesnym państwie. Jest ona jednym z gwarantów przestrzegania prawa i realizowania ideału praworządności. Działania w zakresie inwigilacji *sensu largo* są również nieuniknione. Problemem jest natomiast wyznaczenie optymalnej granicy pomiędzy prawem do prywatności a możliwością legalnej ingerencji w tę sferę życia jednostki. Państwo prawa powinno realizować postulat inwigilacji ograniczonej, legalnej i kontrolowanej, którą można nazwać inwigilacją inwigilowaną" (Chrzczonowicz, Kwiatkowska-Darul, Skowroński, 2003, s. 11).

Warto mieć na uwadze to, że „inwigilacja jest kluczowym wymiarem nowoczesnego świata i w większości krajów ludzie doskonale zdają sobie sprawę, jak duży wpływ wywiera ona na ich życie. Kamery wideo umieszczone w miejscach publicznych są naturalnym widokiem nie tylko w Londynie i Nowym Jorku, ale także w Delhi, Szanghaju, Moskwie czy Rio de Janeiro. Podróżni na lotniskach całego świata wiedzą, że oprócz kontroli paszportowej czekają na nich jeszcze nowe atrakcje w postaci skanerów prześwietlających ubrania oraz czytników biometrycznych, które zaczęły się pojawiać masowo po 11 września 2001 roku. Te zastosowane środki kontroli

można tłumaczyć względami bezpieczeństwa, lecz coraz bardziej wszechobecne stają się także inne formy inwigilacji, związane z dokonywaniem najprostszych, codziennych zakupów lub dostępem do serwisów społecznościowych. Musimy okazywać dowód tożsamości, wprowadzić hasło albo posłużyć się kodem liczbowym w najrozmaitszych sytuacjach, np. robiąc zakupy albo wchodząc do budynku. Każdego dnia wyszukiwarki Google zapamiętują nasze wpisy, pomagając w opracowaniu strategii marketingowych dostosowanych do naszych indywidualnych potrzeb" (Bauman, 2013, s. 9–10).

Dostępne źródła informacji wpływają na prywatność na dwa sposoby:

- pierwszy – osoby zbierające dane mogą w ogólnie dostępnych źródłach trafić na poufne informacje o ludziach, którymi się interesują;
- drugi – można znaleźć dane o różnych osobach, przeszukując niektóre ogólnie dostępne źródła, zwłaszcza w Internecie (Denning, 2002, s. 93).

Nauka, technika i nowoczesne to Echelon – globalna sieć wywiadu elektronicznego. System powstał przy udziale Stanów Zjednoczonych, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii w ramach porozumienia AUSCANNZUKUS i jest zarządzany przez amerykańską służbę wywiadu NSA. Kolejny element ogólnoświatowej inwigilacji to PEGASUS, oprogramowanie szpiegujące przeznaczone do instalacji na systemach iOS i Android opracowane i dystrybuowane przez izraelską firmę NSO Group.

Wielu badaczy zauważa, że inwigilacja, niegdyś solidna i niewzruszona, stała się obecnie znacznie bardziej mobilna i elastyczna, przenikając do wielu sfer życia, w których dawniej odgrywała marginalną rolę (Bauman, 2013, s. 9–10).

Podsumowanie

Zmieniające się środowisko człowieka ma znaczący wpływ na poziom jego bezpieczeństwa. Ewoluujące zjawiska i procesy generują wiele złożonych zagrożeń, które zakłócają funkcjonowanie państwa (państw) w wymiarze wewnętrznym i zewnętrznym. Ich źródeł upatruje się w siłach natury, które stanowią coraz większe zagrożenie i są zróżnicowane co do rejonu geograficznego. Dla środowiska bezpieczeństwa międzynarodowego największe zagrożenie stanowią celowe działania człowieka, który usytuowany w różnych obiektach posiada naturalne możliwości prowadzenia destrukcyjnej działalności. Obok znanych zagrożeń niebezpieczeństwo stanowią nowe, gdyż postęp cywilizacyjny oprócz aspektów pozytywnych generuje wiele złożonych zjawisk zakłócających funkcjonowanie państwa (państw). W trwającej rewolucji naukowej i technicznej dominującą pozycję zajmują techniki teleinformatyczna i komunikacyjna. Wspierają one działania człowieka, ale jednocześnie pozwalają nieuprawnionym podmiotom na atakowanie interesujących ich obiektów. Należy mieć na uwadze to, że trwający rozwój będzie wspierał człowieka w jego ofensywnych działaniach, a jednocześnie będzie miał negatywny wpływ na podejmowane decyzje.

Bibliografia

Anioł, W. (1989). *Geneza i rozwój procesu globalizacji*. Centralny Ośrodek Metodyczny Studiów Nauk Politycznych.

Barczak, A., Sidoruk, T. (2003). *Bezpieczeństwo systemów informatycznych zarządzania*. Bellona.

Bauman, L. (2013). *Płynna inwigilacja rozmowy*. Wydawnictwo Literackie.

Białas, A. (Red.) (2002). *Podstawy bezpieczeństwa systemów teleinformatycznych*. Wydawnictwo Pracownia Komputerowa Jacka Skalmierskiego.

Chrzczonowicz, P., Kwiatkowska-Darul, V., Skowroński, K. (Red.) (2003). *Społeczeństwo inwigilowane w państwie prawa*. Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.

Dawidczyk, A. (2001). *Nowe wyzwania, zagrożenia i szanse dla bezpieczeństwa Polski u progu XXI wieku*. AON.

Denning, E.D. (2002). *Wojna informacyjna i bezpieczeństwo informacji*. Wydawnictwo Naukowo-Techniczne.

Dworecki, S. (1994). *Zagrożenia bezpieczeństwa państwa*. AON.

Dworecki, S. (1996). *Od konfliktu do wojny*. Wydawnictwo BUWIK.

Ficoń, K. (2007). *Inżynieria zarządzania kryzysowego. Podejście systemowe*. BEL Studio.

Hołyst, B. (1997). *Wiktymologia*. PWN.

Hołyst, B. (2014). *Bezpieczeństwo. Ogólne problemy badawcze*. PWN.

Jakubczak, R. (2003). *Obrona narodowa w tworzeniu bezpieczeństwa RP*. Bellona.

Janczak, J. (2001). *Zakłócanie informacyjne*. AON.

Kompała, D. (2014). Istota zagrożeń. *Zeszyty Naukowe. Obronność*, 3(11), 23–34.

Latiff, R.H. (2018). *Wojna przyszłości w obliczu nowego globalnego pola bitwy*. PWN.

Lidwa, W. (2010). Zagrożenia niemilitarne mogące wywołać sytuacje kryzysowe. W W. Lidwa, W. Krzeszowski, W. Więcek (Red.), *Zarządzanie w sytuacjach kryzysowych* (s. 7). AON.

Łepkowski, W. (2009). *Słownik terminów z zakresu bezpieczeństwa narodowego*. AON.

Malecki, G. (2011). Polityczne zagrożenia bezpieczeństwa publicznego. W S. Kowalkowski (Red.), *Niemilitarne zagrożenia bezpieczeństwa publicznego* (s. 26). AON.

Pawłowski, J. (Red.) (2017). *Podstawy bezpieczeństwa narodowego (państwa)*. Wydawnictwo Akademia Sztuki Wojennej.

Rączkiewicz, M. (1995). *Bezpieczeństwo sieci komputerowych*. Fundacja Postępu Telekomunikacji.

Shinder, D.L. (2004). *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*. Helion.

S.P. (1997). Informacja jako decydujący czynnik sukcesu w przyszłych konfliktach zbrojnych. *Wojskowy Przegląd Zagraniczny*, 1, 33–41.

Sójka, W. (2017). Zagrożenia bezpieczeństwa narodowego Polski. W J. Pawłowski (Red.), *Podstawy bezpieczeństwa narodowego (państwa)* (s. 183). Akademia Sztuki Wojennej.

Szpyra, R. (2003). *Militarne operacje informacyjne*. AON.

Witecka, M.S. (2011). Zagrożenia asymetryczne a technologie informacyjne*. Towarzystwa Wiedzy Obronnej. Zeszyt Problemowy*, 4.

Wrzosek, M. (2010). *Identyfikacja zagrożeń organizacji zhierarchizowanej.* AON.

Żebrowski, A. (2002). Bezpieczeństwo infrastruktury informacyjnej. W R. Borowiecki, M. Kwieciński (Red.), *Informacja w zarządzaniu przedsiębiorstwem – pozyskanie, wykorzystanie i ochrona (wybrane problemy teorii i praktyki)* (s. 333–337). Wydawnictwo Zakamycze.

Żebrowski, A. (2018). *Globalna przestrzeń zagrożeń. Wybrane aspekty*. Wydawnictwo Sztafeta.

Żuber, M. (2006). *Katastrofy naturalne i cywilizacyjne. Zagrożenia i reagowanie kryzysowe*. WSOWL.

Biogram autora

Andrzej Żebrowski – prof. zw. dr hab. inż., profesor nauk społecznych w zakresie nauk o polityce, kierownik Katedry Bezpieczeństwa Wewnętrznego Instytutu Nauk o Bezpieczeństwie Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie. Kierunki badawcze: bezpieczeństwo wewnętrzne i zewnętrzne państwa, służby specjalne, walka informacyjna. Autor publikacji: *Kontrola cywilna nad Siłami Zbrojnymi Rzeczypospolitej Polskiej* (1997), *Przywileje i immunitety dyplomatyczne i konsularne podczas konfliktu zbrojnego* (1999), *Czynności operacyjno-rozpoznawcze (regulacje prawne)* (2000), *Kontrola cywilna nad służbami specjalnymi III Rzeczypospolitej (1989–1999). Zagadnienia politologiczno-prawne* (2001), *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej (wywiad i kontrwywiad w latach 1989–2003)* (2005), *Wywiad i kontrwywiad XXI wieku* (2010), *Zwalczanie przestępczości zorganizowanej w Unii Europejskiej. Zagadnienia politologiczno-prawne* (2011), *Zarządzanie kryzysowe elementem bezpieczeństwa Rzeczypospolitej Polskiej* (2012), *Walka informacyjna w asymetrycznym środowisku bezpieczeństwa międzynarodowego* (2016), *Informacja jednym z elementów bezpieczeństwa państwa. Wybrane aspekty* (2017), *Globalna przestrzeń zagrożeń. Wybrane aspekty* (2018). Autor licznych artykułów związanych ze wskazanymi obszarami badawczymi.