Anna Ibek
Krakowska Akademia im. Andrzeja Frycza Modrzewskiego

Niepewność w systemach bezpieczeństwa

Celem artykułu jest charakterystyka niepewności z perspektywy dylematów bezpieczeństwa, z jakimi borykają się osoby podejmujące decyzje w zakresie spraw związanych z bezpieczeństwem. Rozważania rozpocznie zdefiniowanie bezpieczeństwa z perspektywy podmiotów, którym może przysługiwać cecha „bycia bezpiecznym", ponieważ mówienie o bezpieczeństwie w oderwaniu od podmiotów jest pozbawione sensu. W grę wchodzą tylko podmioty posiadające jakąś aksjologię, gdyż z etycznego, a nawet ogólniej, z filozoficznego punktu widzenia, bezpieczeństwo jest związane z wartościami[1], a ściślej z wartościami ustrukturyzowanymi, czyli z aksjologią. Aksjologię może mieć tylko osoba[2]. Powstaje pytanie, o jaką osobę chodzi? Czy mowa jest tutaj, używając języka prawniczego, tylko o osobach fizycznych czy także o osobach prawnych, stowarzyszeniach i różnego rodzaju organizacjach? Wątpliwości nie pozostawiają osoby fizyczne, które tym się odróżniają od innych istot żywych, że potrafią głosić wartości, choćby takie jak: życie, zdrowie, przyjaźń, rodzina oraz odpowiednio się o nie troszczyć i zabiegać. Czy zatem „państwo" jako organizacja polityczna, terytorialna, nie ma świadomości wartości? Pytanie to, na które błyskawicznie nasuwa się twierdząca odpowiedź, jest dość trywialne. Równie oczywiste jest, jak w przypadku osób fizycznych, że państwo, a więc także inne osoby prawne, posiadają wartości i je w odpowiedni sposób artykułują zgodnie z przyjętą hierarchią. Dla podmiotu, któremu może przysługiwać cecha „bycia bezpiecznym", charakterystyczne jest, że zazwyczaj nie są to przypadki pojedynczych wartości, ale raczej konglomeratów wartości. Dodać należy także, że czasami można zaobserwować aksjologiczną niestabilność, polegającą na zmianie wyznawanych wartości i ich hierarchii, co może

[1] J. Szmyd, *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Kraków 2000, s. 45.

[2] J. Konieczny, *O pojęciu bezpieczeństwa*, Kraków 2012, s. 9.

być związane z modyfikacją priorytetów, często konieczną z powodu zmian sytuacji podmiotu bezpieczeństwa.

Drugim warunkiem możliwości bycia podmiotem bezpieczeństwa jest posiadanie jakiegoś zasobu dóbr, materialnych i/lub niematerialnych. Warunek ten wydaje się oczywisty, nie ma bowiem sensu mówienie o bezpieczeństwie kogoś/czegoś, kto nie posiada niczego. Spełnienie tego warunku też jednak nie wyczerpuje listy kryteriów przynależności do zbioru podmiotów, którym może przysługiwać cecha bycia bezpiecznym. Podmiot bezpieczeństwa musi ponadto mieć także zdolność suwerennego podejmowania decyzji dotyczących tego zasobu. Podsumowując, „podmiotem bezpieczeństwa może być obiekt posiadający jakiś zasób, będący w stanie podejmować decyzje dotyczące tego zasobu i uznający pewną aksjologię, tzn. mający zdolność do wyartykułowania swojej hierarchii wartości[3]".

Poziom bezpieczeństwa nie ma waloru stałości. Aby jednostka mogła przypisać sobie cechę „bycia bezpieczną" na określonym, pożądanym, optymalnym poziomie, musi podejmować adekwatne działania wpływające na ów poziom. Jednym ze sposobów osiągania optymalnego bezpieczeństwa jest stworzenie systemu bezpieczeństwa, zgodnie z przyjętą aksjologią i rodzajem dóbr, chronionych tym systemem.

Przed scharakteryzowaniem niepewności w kontekście systemów bezpieczeństwa, należy udzielić odpowiedzieć na pytanie, czym jest niepewność. W zależności od obszaru rozważań, w różnych – nieraz nawet bardzo słabo powiązanych ze sobą dziedzinach, takich jak psychologia, fizyka, statystyka, finanse, ekonomia, psychologia, inżynieria, teoria decyzji itd., termin „niepewność" jest stosowany w różnych znaczeniach. Jest to sytuacja naturalna.

Wydaje się, że w dziedzinie bezpieczeństwa pojęcie niepewności używane jest najczęściej do wyrażania stopnia przeświadczenia o wystąpieniu/niewystąpieniu w przyszłości pewnych zjawisk, do wskazywania braków w dostępnej dla badacza wiedzy, a także podczas charakteryzowania informacji, które ze swej natury często nie są jednoznaczne. Zawsze, gdy ma się do czynienia z ograniczonym w jakiś sposób zasobem wiedzy lub gdy możliwych jest kilka równoległych rozwiązań danej sytuacji, pojawia się problem niepewności.

Podstawowym pytaniem, dyktowanym przez zjawisko niepewności, nie jest wątpliwość, czy wiadomo wszystko, ale czy wiadomo wystarczają dużo lub tyle, ile wiedzieć się powinno w związku z założonym celem. Istotny jest również sposób wykorzystania dostępnej wiedzy, aby móc podejmować jak najlepsze, optymalne w danej sytuacji, decyzje. Najtrafniejszym podejściem

[3] *Ibidem*, s. 11.

do rozwiązania tego typu dylematów jest pragmatyzm, zorientowany głównie na użyteczność skutków wypracowywanych rozwiązań danej kwestii[4].

Istnieje cały szereg dobrze opracowanych i ogólnie uznanych narzędzi statystycznych, wykorzystywanych głównie w ekonomii, do obliczania i wyrażania niepewności. Ściślej rzecz ujmując, są one stosowane dla szacowania ryzyka, związanego z konkretnymi decyzjami. Pomiar ryzyka jest istotny zwłaszcza tam, gdzie warunkiem użyteczności podjętej decyzji jest wiarygodna informacja o stopniu prawdopodobieństwa jakiegoś stanu czy zdarzenia. Należy dodać, że mimo dość powszechnej praktyki utożsamiania pojęcia niepewności z pojęciem ryzyka, zagadnienia te są zupełnie inne.

Ujmowanie niepewności z perspektywy szacowania ryzyka ma charakter sformalizowany i ilościowy. Jest ono możliwe i celowe do stosowania w przypadku badania zbioru zjawisk o znanym rozkładzie częstości ich występowania, natomiast całkowicie zawodzi w przypadku badania zdarzeń jednostkowych, a z takimi ma się zwykle do czynienia w dziedzinie bezpieczeństwa. Tu zazwyczaj wystarczyć musi opisowe potraktowania zjawiska niepewności. Na poziomie opisowym niepewność wyrażana jest przez szereg różnych terminów określających subiektywny stopień prawdopodobieństwa, na przykład mało prawdopodobne, nieprawdopodobne, możliwe (istnieje taka szansa), prawdopodobne, wysoce prawdopodobne, prawie na pewno[5]. Poza tymi określeniami stosuje się także tzw. poziomy pewności (zaufania), które przypisywane są do konkretnych opinii, twierdzeń, sądów. Wyróżnia się trzy takie poziomy: pierwszy, dotyczący tzw. wysokiej pewności, przesądzający o tym, że twierdzenie bazuje na wysokiej jakości informacjach lub natura rozpatrywanego problemu czyni twierdzenie możliwie pewnym. Poziom drugi, tzw. umiarkowana pewność, mówiący o tym, że dostępna informacja jest podatna na wiele interpretacji lub że jest wiarygodna, ale wystarczająco nie potwierdzona. Ostatni, poziom trzeci, tzw. niska pewność, za pomocą którego opisuje się informację fragmentaryczną lub wątpliwą lub informację, która oparta jest na źródłach niegodnych zaufania[6].

Istotna dla analityka rozwiązującego konkretny problem, w którym pojawia się zjawisko niepewności, jest konieczność przestrzegania zasady transparentności. Chodzi o to, że przedstawiane wnioski, opinie, prognozy itd., powinny być wypracowane w sposób przejrzysty, a droga dojścia do nich nie budziła wątpliwości. Ponadto obowiązkiem analityka jest także udzielanie odpowiedzi na ewentualne pytania ze strony zleceniodawcy, a dotyczące np.

[4] www.senseaboutscience.org/data/files/resources/127/SAS012_MSU_ONLINE.pdf., s. 9.
[5] M.M. Lowenthal, *Intelligence. From Secrets to Policy*, Los Angeles 2012, s. 142.
[6] *Ibidem*, s. 143.

sposobu przyjęcia takiego a nie innego twierdzenia, założeń stworzonej opinii, oraz – przede wszystkim – źródeł rozpatrywanej niepewności[7].

W każdym systemie bezpieczeństwa pewne jest jedno, mianowicie niepewność. Jest ona egzystencjalnym zjawiskiem występującym we wszystkich relacjach międzyludzkich, zwłaszcza w obszarze szeroko pojętego bezpieczeństwa. Fakt jej istnienia rodzi tzw. dylematy bezpieczeństwa (*security dilemma*), które są bardziej fundamentalne i typowe dla studiów o bezpieczeństwie, aniżeli wojna, konflikt czy strategia itp., ponieważ warunkowane są poprzez wszechobecną niepewność[8]. Ta ostatnia nie jest chwilowym i nietrwałym zjawiskiem. Przeciwnie, ostatecznie jest nieunikniona, codziennie, w różnym zakresie i odczuciu, towarzysząc każdemu podmiotowi bezpieczeństwa. Niepewności nie należy utożsamiać z niebezpieczeństwem (*insecurity*), gdyż ta pierwsza, mówiąc obrazowo i metaforycznie może być wyobrażona jako „dom", który składa się z kilku pokoi. Każde z pomieszczeń może mieć różny poziom bezpieczeństwa. Może zdarzyć się i tak, że poprzez rozbudowane zaufanie wśród darzących się nim członków społeczeństwa, stopień bezpieczeństwa został osiągnięty, choć te jednostki dalej mieszkają w jednym z „bezpiecznych pokoi domu niepewności". W kontekście międzynarodowych relacji niepewność skutkuje tym, że rządzący nigdy nie posiądą stuprocentowej pewności co do intencji, motywów i zamiarów swoich przeciwników. Innymi słowy, nigdy nie zdobędą wiedzy pewnej co do aktualnych lub przyszłych zachowań swoich konkurentów. Taka sytuacja określana jest mianem nierozwiązywalnego problemu niepewności (*unresolvable uncertainty*), będącego rdzeniem konsekwencji istnienia dylematów bezpieczeństwa. Czynniki warunkujące ten problem są wielorakie, przy czym mogą zostać sprowadzone do dwóch zjawisk psychologicznych. Chodzi mianowicie o dwuznaczną symbolikę broni oraz o tzw. problem innych umysłów (*other minds problem*)[9]. Dwuznaczna symbolika broni dotyczy trudności związanych z odróżnieniem broni ofensywnej od defensywnej, bo jak głosi stare powiedzenie: „to, czy twoja broń jest ofensywna czy defensywna, zależy tylko od tego, czy naciśniesz spust czy nie". W zależności od realiów konkretnej sytuacji, broń raz będzie służyła do ataku, a innym razem posłuży do obrony. Nigdy natomiast nie wiadomo, kiedy do takiego zdarzenia dojdzie. Natomiast tzw. problem innych umysłów referowany jest jako niezdolność do całkowitego poznania intencji, motywów, przekonań, emocji, uczuć przeciwnika. Mówiąc dosłownie, nie istnieje

[7] J.B. Steinberg, *The Policymaker's Perspective: Transparency and Partnership*, [w:] *Analyzing Intelligence. Origins, Obstacles, and Innovations*, red. R.Z. George, J.B. Bruce, Washington 2008.

[8] K. Booth, N. Wheeler, *Uncertainty*, [w:] *Security Studies. An Introduction*, red. D. Williams, London 2008, s. 133–134.

[9] *Ibidem*, s. 134.

możliwość „wejścia w umysł" innego podmiotu. Wydaje się celowe, mówiąc o problemie innych umysłów, mówienie o zasadzie ograniczonego zaufania, hołdowanie której może przyczynić się do redukcji poziomu niepewności. Brak takiej reguły może przyczynić się do powstania na poziomie państwowym, ale nie tylko, bardzo dotkliwych skutków, będących reperkusjami kosztów popełnionego błędu, które nigdy nie są trywialne. Historia zna wiele przypadków, w których objawił się problem innych umysłów, począwszy od drobnych, dyplomatycznych nieporozumień, poprzez mylną interpretację informacji wywiadowczych, a skończywszy na niemożności przewidzenia nieuchronnych działań wojennych. Trudności te potęgują różnice kulturowe między narodami oraz ścisła ochrona informacji państwowych. Paradoksalnie rzecz ujmując, dwuznaczna symbolika i problem innych umysłów są zjawiskami reprezentującymi „pewność niepewności" (*the certainty of uncertainty*)[10]. Te same zjawiska dotyczą, na gruncie bezpieczeństwa biznesu, organizacji gospodarczych, których dylematy mogą dotyczyć rozpoznawania sytuacji kryminologicznej okolicy, w której działają (a przeciwnikiem jest przestępca kryminalny). Przed takimi samymi dylematami może także stanąć, i zazwyczaj staje, osoba indywidualna, rozpatrując swoje osobiste bezpieczeństwo.

Niepewność warunkuje też tzw. dylematy bezpieczeństwa, które dotyczą interakcji między podmiotami bezpieczeństwa. Chodzi mianowicie o dylemat interpretacji (*dilemma of interpretation*) oraz dylemat reakcji (*dilemma of response*), z którymi borykają się osoby podejmujące decyzje z zakresu bezpieczeństwa. Ten pierwszy powstaje, gdy decydent boryka się z problemem oceny zachowań przeciwnika. Może stać przed kwestią odpowiedzi na m.in. takie pytania, jak czy „siły wojskowe" konkurenta w konkretnym okresie, mają charakter ofensywny czy raczej defensywny, czy zakup nowych czołgów ma na celu zwiększenie systemu obronnego państwa „x", czy raczej państwo „x" zamierza wejść w zbrojny konflikt, czy parta polityczna, która głosi powszechną dostępność broni dla każdego pełnoletniego obywatela, zamierza bardziej dosadnie „wypowiadać" się w tym zakresie, czy niepubliczna szkoła wyższa „y", ogłaszająca nabór na prawo, zapowiadając przy tym studia bez obowiązku zapłaty czesnego, może stanowić zagrożenie dla niepublicznej szkoły wyższej w której pracuje decydent. Generalnie, dylemat bezpieczeństwa sprowadza się do konieczności udzielenia odpowiedzi na pytanie, jak interpretować dane zachowanie, motyw, intencje.

Dylemat reakcji rodzi się, gdy w tym samym konkretnym przypadku zaistnieje dylemat interpretacji. Najpierw należy zaobserwować zjawisko, zanalizować problem, aby móc w jakiś sposób się do niego ustosunkować. Na tym

[10] *Ibidem*, s. 136.

etapie decydenci muszą odpowiedzieć na pytanie: jak zareagować, co zrobić. Należy zauważyć, że nie zawsze rozwiązanie dylematu reakcji będzie wymagało podjęcia aktywności ze strony podmiotu bezpieczeństwa. Celowa czasem jest/będzie bezczynność. W przypadku obu dylematów kluczem do sukcesu jest zawsze dostęp do informacji. Żeby móc interpretować, należy posiadać wiedzę o tym, co ma być analizowane, a aby reagować, trzeba być dobrze poinformowanym na temat sposobów odpowiedzi i ich możliwych konsekwencji. Istotne wydaje się pytanie, co się może stać, jeśli podmiot bezpieczeństwa zareaguje na błahy, niesłuszny, sprowokowany sygnał. Jeśli dylemat reakcji oparty był na błędnych przeświadczeniach co do intencji i motywów przeciwnika, może dojść do spotęgowania stopnia wzajemnej wrogości, w sytuacji która tego nie wymagała. Podmiot, w stosunku do którego zareagowano nie mając przy tym uzasadnionych podstaw, będzie musiał się bronić, aby móc zachować poczucie bezpieczeństwa. Dojdzie do „spiętrzenia" wzajemnej niechęci, mimo że sytuacja faktyczna tego w żaden sposób nie wymagała. Zjawisko takie określane jest jako tzw. paradoks bezpieczeństwa (*security paradox*)[11]. Jednostka, która sprowokowała tę sytuację w celu polepszenia własnego poziomu bezpieczeństwa, spowodowała, że ostatecznie, zarówno ona, jak i przeciwnik stracili na tym, obniżając swoje poziomy bezpieczeństwa. W związku z tym należy podkreślić, że rozwiązywanie dylematów bezpieczeństwa powinno być pozostawione osobom kompetentnym, posiadającym potrzebną do tego typu rozważań wiedzę, choć często działają one w sytuacji deficytu informacyjnego i pod presją czasu. Wydaje się dość oczywiste, że u podłoża dylematów bezpieczeństwa leży strach przed tym, co jest oraz przed tym, co będzie. Podmioty bezpieczeństwa operujące zasobami dóbr, nie chcą stracić elementów tych zasobów, co powoduje, że interpretują i reagują na bodźce wysyłane ze strony innych jednostek.

Podmioty bezpieczeństwa, oprócz samej świadomości istnienia omawianych dylematów, powinny być wrażliwe na powszechność ich występowania (*security dilemma sensibility*)[12]. Wskazane byłoby, aby decydenci mieli zdolność przewidywania „ruchów" przeciwnika, jego zamierzeń, przed ich faktycznym urealnieniem. Dzięki odpowiedniemu prognozowaniu zdarzeń, środki potencjalnie potrzebne do utrzymania optymalnego poziomu bezpieczeństwa mogłyby zostać zgromadzone, a przynajmniej zabezpieczone, zgodnie z zasadą *Si vis paceum, para bellum.*

W tym miejscu nasuwają się pytania dotyczące rozumowań używanych podczas procesu interpretowania danych oraz przewidywania możliwego

[11] *Ibidem*, s. 135.
[12] *Ibidem*, s. 141.

rozwoju wydarzeń na podstawie wnioskowania abdukcyjnego. Paradoksalnie w tego rodzaju inferencjach, których prawidłowa realizacja w konkretnym przypadku powinna redukować niepewność decyzyjną, na każdym kroku rozumowań pojawia się zjawisko niepewności. Wniosek taki związany jest z charakterem tych inferencji, który ma cechy niemonotoniczności. Większości przypadków rozumowań są to tzw. rozumowania podważalne (*defeasible inference*). W tym typie wnioskowaniach nowe informacje mogą przyczynić się do wskazania wątpliwości w prawidłowości twierdzeń, które wcześniej zostały uznane za prawdziwe[13]. Logika podważalna, która jest bazą dla tego typu rozważań, pozwala na rozumowanie w sytuacji niepewności i niekompletności wiedzy, sytuacji, która jest typową dla szeroko rozumianego zapewniania bezpieczeństwa. Podczas tego procesu na jego początku, ale także w trakcie nigdy nie jest tak, że decydentom udaje się ujawnić wszystkie relewantne informacje i zabezpieczyć wszystkie odpowiednie dane. Brak wiedzy może być „tymczasowo" uzupełniony poprzez generalizacje, które nadadzą spójność możliwym interpretacjom i reakcjom na zdarzenia. Niemniej, po uzyskaniu nowej wiedzy, będą one musiały być zweryfikowane, dzięki czemu zostanie rozstrzygnięty status ich uzasadnienia tzn. uznanie, czy są one adekwatne w danych okolicznościach czy też nie.

Zgodnie z tzw. zasadą wrażliwości dylematów bezpieczeństwa, głównym celem podmiotów bezpieczeństwa jest prognozowanie możliwości interpretacyjnych i reakcyjnych dotyczących potencjalnych zdarzeń, mogących wystąpić w bliższej lub dalszej perspektywie czasowej. Określenie tych rozwiązań jako prognostycznych, jest jak najbardziej uzasadnionym zabiegiem, ponieważ ich stworzenie jest tylko próbą myślowego „odtworzenia" jakiegoś fragmentu bliżej nieokreślonej przyszłości, gdzie jej prawdziwość/pewność w chwili planowania, nie wymaga i nie może wymagać potwierdzenia, co zgodne jest ze zjawiskiem powszechności oraz nierozwiązywalność niepewności. U podłoża rozwiązywania dylematów bezpieczeństwa w zakresie logicznych struktur inferencyjnych, leży – wspomniany wcześniej – abdukcjonizm.

Poszukiwanie wyjaśnień jest jedną z najbardziej typowych form aktywności poznawczych. Pytania: „dlaczego stało się tak-a-tak?", „po co?", „jako do tego doszło?", „jak można interpretować zgromadzone informacje?", „jak zareagować na dane zdarzenie?" – są podstawowymi zagadnieniami, uzyskanie na nie odpowiedzi jest jednym z głównych celów podmiotów bezpieczeństwa. W kontekście procesu funkcjonowania systemu bezpieczeństwa to właśnie ujawnione w sprawie informacje muszą zostać w racjonalny sposób zinter-

[13] F. Bex, *Evidence for a Good Story: A Hybrid Theory of Arguments, Stories and Criminal Evidence*, Groningen 2009, s. 25.

pretowane i wyjaśnione, a na ich podstawie będzie można uzyskać konkretne wnioski o charakterze zagrożenia.

Hipotezy tworzone podczas inferencji abdukcyjnych, są propozycjami rozwiązań dylematów bezpieczeństwa, zarówno interpretacyjnego, jak i reakcji, ale także znajdują swoje zastosowanie w wypełnianiu zasady wrażliwości dylematów. Dobra praktyka zapewniania bezpieczeństwa przez realizację odpowiedniego systemu, zależy w dużej mierze od poprawnego podejmowania decyzji (jak zinterpretować uzyskaną informację, co oznacza dana informacja, jak na nią zareagować, czy posiadane środki są wystarczające do utrzymania pożądanego poziomu bezpieczeństwa, czy należy je zwiększyć, jakie konsekwencje może przynieść zaistniałe zdarzenie itp.) na podstawie wielokrotnie przetwarzanych, dostępnych w sprawie informacji. Każda decyzja w obszarze bezpieczeństwa wymaga uwzględnienia dostępnego materiału informacyjnego, jego wiarygodności i siły, przyszłego wykorzystania w celu wskazania możliwych kierunków rozwoju interesującej dla decydenta sprawy. Tymczasem proces podejmowania decyzji przez podmioty bezpieczeństwa napotyka na swojej drodze wiele przeszkód. Oczywiste jest, że materiał, na którym można byłoby oprzeć pojedyncze rozstrzygnięcie, może być zwyczajnie niedostępny w sprawie, bo na przykład nie udało się go ujawnić lub został zniszczony przez konkurentów, przeciwnicy mogą zapewniać efektywną kontrolę nad transmisją przekazywanych informacji[14]. Nie oznacza to jednak, że z powodu tego rodzaju ograniczeń niemożliwe jest sprawne i właściwe podejmowanie decyzji. Wymaga to jednak uświadomienia sobie istnienia tego rodzaju przeszkód, zagrożeń z tym związanych i dokonywania, za sprawą takiego myślenia, ustawicznego polepszania procesu śledczego i minimalizowania ryzyka oraz niepewności, przez doskonalenie przebiegu podejmowania decyzji i nabywaniu wiedzy o ludzkim zachowaniu[15]. Zaznaczyć należy, że generowanie dużej liczby hipotez akcji wymaga od decydentów jednoczesnego przetwarzania różnorakich informacji i danych, z uwzględnieniem ich potencjalnego znaczenia dla konkretnego przypadku, a przecież możliwości poznawcze i myślowe ludzkiego umysłu są ograniczone. Najczęstszym źródłem błędów w tworzeniu i ocenie hipotez są poznawcze ograniczenia i uprzedzenia (*cognitive biases*). Pojawiają się one podczas procesu podejmowania decyzji jako odpowiednie schematy myślenia, często uproszczone i błędne. Jednym z dobrze znanych zagrożeń, immamentnie związanych z zapewnianiem bezpieczeństwa, jest tzw. efekt tunelowy (*tunnel vision*). Pojawia się, gdy najbar-

[14] P. Stelfox, *Criminal Investigation. An Introduction to principles and practice*, Portland 2009, s. 174.

[15] *Ibidem*, s. 174.

dziej prawdopodobna interpretacja zdarzenia/informacji, jaką udało się do pewnego momentu skonstruować, jest uznawana jako hipoteza kierunkowa, warunkująca reakcję, przez co pozostałe, alternatywne możliwości, są niewystarczająco analizowane[16]. Rezultatem efektu tunelowego jest interesowanie się tylko tymi informacjami, które są relewantne dla początkowej hipotezy, podczas gdy istotne dane mogą zostać utracone, zwłaszcza w tych sprawach, w których analizowany splot wydarzeń okazał się niepoprawny[17]. Wiąże się to z kolejnym źródłem zagrożenia występującym w procesie rozstrzygania dylematów bezpieczeństwa podczas rozumowania na podstawie zgromadzonych informacji, a mianowicie tzw. błąd konfirmacji (*confirmation biases*). Polega on na tym, że poszukuje się przede wszystkim takich faktów, które weryfikują i potwierdzają hipotezy i wcześniej poczynione założenia, a jednocześnie ignoruje to, co mogłoby temu zaprzeczać albo dyskredytować informacje w oparciu o które sformułowano hipotezy. Występuje na etapie, gdy zostały już stworzone wielorakie hipotezy, a decydenci pomijają oszacowanie „diagnostyki" posiadanych informacji, za sprawą której można znacząco wpłynąć na oceny względnego stopnia prawdopodobieństwa różnych hipotez[18]. Niebezpieczeństwem związanym z błędem konfirmacji jest także to, że często objawia się on jako nieświadoma tendencja afirmacji pierwszych teorii, opinii, gdzie możliwość rozpoznania tego zjawiska jest znacznie trudniejsza niż wtedy, gdy posiada się świadomie wiedzę o takim potencjalnym ryzyku[19].

Kolejnym problemem, który może przyczynić się do obniżania poziomu bezpieczeństwa, jest tzw. myślenie grupowe (*groupthink*) określane też jako „gromadomyślenie". Oczywiste jest, że owo zjawisko występuje tam, gdzie ma się do czynienia z jakimś skupiskiem ludzi, mniejszym lub większym, a więc także w obszarze systemów bezpieczeństwa, gdzie angażowani są różnego rodzaju specjaliści. Myślenie grupowe prowadzi do podejmowania błędnych decyzji i kryzysów, gdyż umożliwia grupie widzenie i słyszenie tylko tego, co chce, zgodnie z aforyzmem „widzimy to, co chcemy widzieć". Kluczową rolę odgrywa tutaj przywódca, decydent, który swoim autorytetem i doświadczeniem zawodowym może wywierać presję do podejmowania rozwiązań, które będą zgodne z jego kierunkiem myślenia. Wydawać by się mogło, że każdy z członków grupy wnosi do niej twórczy intelektualny wkład, czego skutkiem powinna być rzeczowa i wielostronna ocena sytuacji oraz podjęcie właściwej decyzji. To dlatego powszechnie się uważa, że myślenie zespołowe

[16] F. Bex, *op. cit.*, s. 4.

[17] S. van den Braak, *Sensemaking Software for Crime Analysis*, Utrecht 2010, s. 20.

[18] *Ibidem*, s. 20.

[19] B.E. Turvey, *Criminal Profiling. An Introduction to Behavioral Evidence Analysis*, Amsterdam 2008, s. 144–145.

zapewnia lepsze wyniki, niż samodzielne. Okazuje się jednak – i to bardzo często – że inteligencja grupy wcale nie przewyższa poziomu inteligencji jej poszczególnych członków, że decyzje rozmaitych społeczności są wyjątkowo nietrafne i że byłoby lepiej, gdyby były one podejmowane przez pojedyncze osoby. Zespół bowiem ulega złudzeniu co do swojej nieomylności i wyższości intelektualnej, przy czym złudzenie to jest tym silniejsze, im wyższy jest status społeczny każdego z uczestników, im wyższym dyplomem może się on legitymować i im większy jest poziom wewnętrznej spójności grupy[20].

Daje się zauważyć, że zjawisko to dotyczy też sposobu analizowania informacji dostępnych w sprawie. Może wówczas wystąpić specyficzne „filtrowanie informacji", tzn. członkowie grupy starają się nie dopuścić informacji sprzecznych ze zdaniem grupy, informacje niepomyślne są lekceważone, rozumowanie o dowodach jest ograniczane do analizy zaledwie paru działań bez weryfikacji całej gamy innych rozwiązań, gardzi się określonymi hipotezami, które początkowo zostały uznane za niezadowalające przez większość członków grupy, grupa korzysta w małym stopniu z możliwości uzyskania informacji od ekspertów, którzy mogliby oszacować zyski i straty, wykazuje też selektywną tendencyjności w sposobie reagowania na informacje, zależnie od tego, czy są one w zgodzie z wcześniej podjętymi decyzjami czy nie[21].

Jak się okazuje, nie można całkowicie wyeliminować zjawiska myślenia grupowego, ale można dążyć do jego minimalizacji. Począwszy od przybrania odpowiedniej postawy przez lidera danej grupy, który powinien każdemu z członków przypisać konkretną, odpowiedzialną rolę, umożliwić im wypowiadanie własnych, sądów, przekonań i proponowanie uzasadnionych rozwiązań, rozpatrywanie szerokiego zakresu rozwiązań. Zdaniem I. Janisa, twórcy tego pojęcia, przynajmniej jeden z członków danej grupy powinien odgrywać rolę „adwokata diabła", którego zadaniem jest „szukanie dziury w całym", czyli wyszukiwanie i zgłaszanie wszelkich możliwych rozbieżności dowodowych i interpretacyjnych[22].

Wracając do możliwości rozwiązywania dylematów bezpieczeństwa, konsekwencją czego powinna być redukcja stopnia niepewności, kluczową rolę może odegrać analiza informacji, a właściwie jej efekty. Pozwala krytycznie spojrzeć na zgromadzone informacje, dokonanie ich interpretacji i co najważniejsze, wyniki pracy analityków mogą być propozycjami reakcji na te dane. Ponadto zadaniem analityka może być ostrzeżenie decydentów przed „wejściem w tunel" lub uświadomienie im takiej możliwości. Analiza może

[20] T. Romer, M. Najda, *Etyka dla sędziów. Rozważania*, Warszawa 2007, s. 105.
[21] D.R. Forsyth, *Group Dynamics*, Belmont 2009, s. 339–343.
[22] B. Kellerman, *Political Leadership*, Pittsburgh 1986, s. 327–346.

dostarczyć „świeżego", niezależnego spojrzenia na sprawę i dostępne dowody, przez wskazanie alternatywnych interpretacji i identyfikację brakujących informacji[23]. Wydaje się, że analiza informacji jako narzędzie dla redukcji poziomu niepewności, powinna być nieodłączną częścią każdego funkcjonującego systemu bezpieczeństwa, a to ze względu na korzyści, jakie może zapewnić dla utrzymania optymalnego poziomu bezpieczeństwa.

Jedną, wydaje się że oczywistą, z przeszkód poznawczych, która może przyczynić się do powstania błędów w generowaniu hipotez, jest ograniczona zdolność pracy ludzkiej pamięci, która jednocześnie może zawierać i przetwarzać limitowaną ilość hipotez, informacji, relacji między nimi[24]. Pomocnym rozwiązaniem może okazać się oprogramowanie komputerowe, które umożliwia wizualizację rozumowania w konkretnej sprawie przez zobrazowanie tego procesu przy użyciu odpowiednich schematów, wykresów, diagramów czy tabel[25]. Pojemność pamięci komputera jest nieporównywalnie większa niż rozmiar pamięci ludzkiej, a sztuczna inteligencja pozbawiona jest uprzedzeń poznawczych, wszystko można tutaj zaplanować i sukcesywnie udoskonalać. Tego typu programy jednak są kosztowne. Od dawna panuje przekonanie, że bezpieczeństwo to „pasożyt", wchłonie każdą ilość środków, a i tak bezpieczeństwo absolutne nie zostanie nigdy osiągnięte. Rolą decydenta systemu bezpieczeństwa jest więc wypracowanie takiej relacji koszt/efektywność, aby w ostatecznym rozrachunku było to opłacalne.

W rozwiązywaniu dylematów bezpieczeństwa pomocne mogą być także reguły heurystyczne, zwane czasem metaforycznie „logikami", dyktowane ogólnym sposobem widzenia świata. Są one następujące: pierwsza to logika fatalistyczna. Zakłada ona, że od współzawodniczenia o bezpieczeństwo nie ma ucieczki, a konflikt jest podstawą tego współzawodnictwa. Może tu chodzić o konflikt międzynarodowy, ale także o inne konflikty, np. pomiędzy starającym się uniknąć odpowiedzialności przestępcą a ścigającym go państwem, pomiędzy podmiotem starającym się zapobiec stratom w swoim zasobie, a kimś, kto ów zasób, w całości lub w części chciałby „prawem lub lewem" sobie przywłaszczyć. Patrzenie przez pryzmat logiki fatalistycznej nie pozostawia miejsca na międzyludzkie zaufanie, na zdolność do kompromisu, a rozwiązanie problemów bezpieczeństwa widzi przede wszystkim w sile. W stosunkach międzynarodowych głównym narzędziem zapewnienia bezpieczeństwa będzie więc odstraszanie, w polityce wewnętrznej zresz-

[23] S. van den Braak, *op. cit.*, s. 4.

[24] P. Pirolli, S. Card, *The Sensemaking Process and Leverage Points for Analyst Technology as Identified through Cognitive Task Analysis*, McLean 2005, s. 5.

[25] F. Bex et al., *Sense-Making Software for Crime Investigation: How to Combine Stories and Arguments?*, „Law, Probability and Risk" 2007, No. 6, s. 145.

tą również, manifestując się np. w formie nastawionej na surową represję polityki karnej.

Drugą koncepcją jest „logika" łagodzenia. Jej założeniem jest teza, że chociaż współzawodnictwo, konkurowanie w zakresie bezpieczeństwa, jest nieuniknione, to jednak może ono być ograniczane i łagodzone. Konkurujące podmioty nie muszą odwoływać się do środków skrajnych przez np. deklarację ograniczenia użycia siły, rezygnację ze stosowania kary śmierci itp.

Koncepcją trzecią jest „logika przekraczania" naturalnej rzekomo tendencji człowieka do wchodzenia w konflikt, czyli odrzucenia zasady *homo domini lapus*. Traktuje ona społeczność międzynarodową i społeczeństwa lokalne jako podmioty zdolne do dokonywania wyborów, budowania na skłonności do unikania konfliktów i wzajemnym zaufania, oczywiście przy utrzymaniu jakiegoś elementu siły[26].

Trzeba też pamiętać, że mówiąc o konflikcie, niekoniecznie ma się na myśli konflikt zbrojny czy w ogóle konflikt wymagający użycia siły. Konflikt interesów ekonomicznych może wszak zachodzić nawet między przyjaciółmi. Redukcja niepewności zawsze jednak wymaga uzyskania informacji, które kontrpartner stara się ukryć. Chodzi przede wszystkim o fakty, a potem, na ich podstawie, o przeprowadzenie precyzyjnych, wiarogodnych i dokładnych analiz[27].

Tradycyjne ujęcia wiązały niepewność z szacowaniem ryzyka. Wiedza o szacowaniu, określaniu i pomiarze ryzyka w bezpieczeństwa jest bardzo rozległa i skomplikowana. Tymczasem, rzecz ciekawa, najnowsze ujęcia tej kwestii zdają się sugerować odejście od traktowania ryzyka jako kategorii centralnej. Jest ona zastępowana właśnie poszukiwaniem informacji na temat kierunków, tendencji i przyczyn zmian w zachodzących procesach, istotnych z punktu widzenia bezpieczeństwa. W bezpieczeństwie międzynarodowym chodziłoby zatem o wykrywanie zmian w prowadzonej przez poszczególne podmioty polityce, w bezpieczeństwie wewnętrznym i bezpieczeństwie biznesu zmian w sytuacji kryminologicznej. I w jednym i w drugim obszarze ciągle zachodzą zmiany i stosowane modele w określaniu ryzyka dezaktualizują się, wraz z ich zachodzeniem, powstają bowiem nowe problemy, dostarczające „nowych niepewności". Potrzebnych informacji mogą dostarczać tradycyjne i nowe formy działań rozpoznawczych, ale widać wyraźnie, że wśród form gromadzenia relewantnej wiedzy, jest wielkie pole dla nauki, szczególnie dla badań empirycznych.

[26] K. Booth, N. Wheeler, *op. cit.*, s. 139.

[27] R.M. Clark, *Intelligence Analysis. A Target-Centric Approach*, Los Angeles 2013, s. 3.

Podsumowując należy powtórzyć: niepewność towarzyszy wszystkim relacjom międzyludzkim. Co więcej, próba jej minimalizacji również ma przymioty niepewności ze względu na podważalny charakter rozumowań wykorzystywanych podczas procesu redukcyjnego. Występuje także w obszarze bezpieczeństwa, którego podmiotami mogą być osoby posiadające zasób dóbr oraz zdolność do podejmowania suwerennych decyzji dotyczących tego zasobu. Sposób radzenia sobie z dylematami bezpieczeństwa warunkuje poziom niepewności, który może być redukowany istniejącymi od dawna narzędziami analitycznymi lub „dobrym wywiadem". Dla decydenta podstawą powinna być wiarygodna informacja, a to, co z nią ma uczynić, winno być jedną ze składowych sytemu bezpieczeństwa.

Być może jednak niepewność w bezpieczeństwie determinowana jest przez jeden dylemat „nadrzędny" – lokalizacją granicy pomiędzy bezpieczeństwem a wolnością. Kluczowa dla zrozumienia i redukcji niepewności może być obserwacja i analiza przesunięć i konsekwencji zmian tej granicy, w obrębie poszczególnych podmiotów bezpieczeństwa. Przypomnieć tu można słowa Adama Mickiewicza:

W innych krajach, jak słyszę, trzyma urząd drabów,
Policyjantów różnych, żandarmów, konstabów,
Lecz jeśli miecz tam tylko bezpieczeństwa strzeże,
Żeby w tych krajach była wolność, nie uwierzę.

Abstract
Uncertainty in security systems

Uncertainty is an existential phenomenon that lies in all human relations, will accompany the analysis and decisions taken in any security system. The most important and typical manifestations of uncertainty in security are: the dilemma of interpretation about motives, intentions and capabilities of other; and the dilemma of response related to the issue of how to respond to threats. The problem of uncertainty in the security systems generally is considered to be unsolvable even talk certainty of uncertainty, however, there are philosophical and empirical approaches and analytical methods for reducing uncertainty in the course of decision-making. The paper presents the theoretical aspects of uncertainty in security systems, discusses the meaning of these dilemmas, and has potential for reducing extent of the problem.

Literatura

Bex F. et al., *Sense-Making Software for Crime Investigation: How to Combine Stories and Arguments?*, „Law, Probability and Risk" 2007, No. 6.

Bex F., *Evidence for a Good Story: A Hybrid Theory of Arguments, Stories and Criminal Evidence*, Rijksuniversiteit Groningen, Groningen 2009.

Booth K., Wheeler N., *Uncertainty*, [w:] *Security Studies. An Introduction*, red. P. Williams, Routledge, London 2008.

Braak S. van den, *Sensemaking software for crime analysis*, „SIKS Dissertation Series No. 2010-12", Universiteit Utrecht 2010.

Clark R.M., *Intelligence Analysis. A Target-Centric Approach*, SAGE, Los Angeles 2013.

Forsyth D.R., *Group Dynamics*, Wadsworth, Cengage Learning, Belmont 2009.

Kellerman B., *Political Leadership*, University of Pittsburgh Press, Pittsburgh 1986.

Konieczny J., *O pojęciu bezpieczeństwa*, „Bezpieczeństwo. Teoria i Praktyka" 2012, nr 1 (VI).

Pirolli P., Card S., *The Sensemaking Process and Leverage Points for Analyst Technology as Identified through Cognitive Task Analysis*, „Proceedings of the 2005 International Conference on Intelligence Analysis", McLean VA 2005.

Romer T., Najda M., *Etyka dla sędziów. Rozważania*, Wolters Kluwer Polska, Warszawa 2007.

Steinberg J.B., *The Policymaker's Perspective: Transparency and Partnership*, [w:] *Analyzing Intelligence. Origins, Obstacles, and Innovations*, red. R. Z. George, J.B. Bruce, Georgetown University Press, Washington 2008.

Stelfox P., *Criminal Investigation. An Introduction to Principles and Practice*, Willan Publishing, Portland 2009.

Szmyd J., *Bezpieczeństwo jako wartość. Refleksja aksjologiczna i etyczna*, [w:] *Zarządzanie bezpieczeństwem*, red. P. Tyrała, Kraków 2000.

Turvey B.E., *Criminal Profiling. An Introduction to Behavioral Evidence Analysis*, Academic Press – Elsevier, Amsterdam 2008.

www.senseaboutscience.org/data/files/resources/127/SAS012_MSU_ONLINE.pdf.