BEZPIECZEŃSTWO • 2015 nr 4 TEORIA I PRAKTYKA

Jerzy Konieczny*

Bezpieczeństwo państwa a bezpieczeństwo biznesu. Studium metodologiczne

I

Przyjmuję – jak sądzę, niekontrowersyjne – następujące założenia: (1) istnieje korpus wiedzy, którego przedmiotem jest bezpieczeństwo państwa, (2) istnieje korpus wiedzy, którego przedmiotem jest bezpieczeństwo biznesu, (3) wiedza, o której mowa w (1) i (2) jest rozwijana, tzn. w pewien sposób jej zasób jest powiększany. Na podstawie (3) jest oczywiste, że rozwój wspomnianej wiedzy wymaga stosowania czynności wiedzotwórczych. Czynności te, jak wszelkie czynności tego rodzaju, są z kolei możliwe do analizy w kategoriach metodologii opisowej (gdy dążymy do uzyskania odpowiedzi na pytanie, „w jaki sposób rozważana wiedza jest rozszerzana?") lub w kategoriach metodologii normatywnej (gdy dążymy do uzyskania odpowiedzi na pytanie, „w jaki sposób rozważana wiedza powinna być rozszerzana?"). Szkic niniejszy zmierza do rozwiązania problemu:

czy metodologiczna charakterystyka wiedzy o bezpieczeństwie państwa jest specyficzna w stosunku do metodologicznej charakterystyki wiedzy o bezpieczeństwie biznesu, a jeżeli tak, to w jakim zakresie i dlaczego, przy czym analiza dotyczyć będzie tylko kwestii metodologii opisowej.

Dla porządku wspomnę, że odróżniał będę metodologię od metodyki. Metodologia, utożsamiana czasem z filozofią nauki, odpowiada na pytania o możliwość poznania, jego wartość, granice, warunki, wyróżnia funkcje nauki, takie jak opisowa (jak jest?), wyjaśniająca (dlaczego tak jest?), predykcyjna (jak będzie?), optymalizacyjna (jak powinno być, by osiągnąć określony cel?), itd. Metodykę można natomiast utożsamić z konkretną techniką badawczą; w dziedzinie bezpieczeństwa do technik

* Doktor habilitowany, profesor Uniwersytetu Opolskiego, kierownik Pracowni Kryminalistyki na Wydziale Prawa i Administracji Uniwersytetu Opolskiego.

badawczych należy np. wywiad jawnoźródłowy, analiza hipotez konkurencyjnych, metody biometryczne identyfikacji człowieka, itd. Innymi słowy, metodologia jest raczej pojęciem stosowanym w rozważaniach teoretycznych, natomiast metodyka – praktycznych.

W dalszym ciągu zakładam, że: (4) państwo jest organizacją, czyli zespołem osób, połączonych wspólnym celem działania. Mówiąc luźno (co jednak za chwilę zostanie uściślone), na bezpieczeństwo tego rodzaju organizacji składają się różne „segmenty", takie jak bezpieczeństwo polityczne, militarne, ekonomiczne, itd. Termin „biznes" z kolei może być rozumiany jako całokształt działań ekonomicznych, prowadzonych w państwie, można go jednak odnieść również do pojedynczej organizacji, prowadzącej działalność gospodarczą. Bezpieczeństwo biznesu, rozumianego jako całokształt działań ekonomicznych, prowadzonych w państwie, jest więc elementem bezpieczeństwa państwa jako całości. Ten aspekt zostanie w rozważaniach niniejszych pominięty. Przyjmuję zatem, że: (5) pojęcie bezpieczeństwa biznesu będzie odnoszone tylko do pojedynczej organizacji, prowadzącej działalność gospodarczą. Takie ujęcie wydaje się pożyteczne, przede wszystkim dlatego, że sprowadza problem na wspólną płaszczyznę – zarówno bowiem kwestię bezpieczeństwa państwa, jak i bezpieczeństwa biznesu dotyczyć będą bezpieczeństwa organizacji. Organizacje te mają szereg podobieństw, ich cele są jednak zasadniczo różne; cele państwa są polityczne, zaś cele organizacji gospodarczej – ekonomiczne. Problem rozwiązywany w tym artykule można więc skonkretyzować następująco: czy metodologiczna charakterystyka wiedzy o bezpieczeństwie organizacji o celach politycznych jest specyficzna w stosunku do metodologicznej charakterystyki wiedzy o bezpieczeństwie organizacji o celach gospodarczych?

II

Założenie (5) może być uznane za dyskusyjne i jako takie wymaga bliższego komentarza. Według jednej z koncepcji, bezpieczeństwo ekonomiczne państwa polega na „ochronie (*safeguarding*) strukturalnej integralności i generowaniu zdolności do wykorzystania prosperity w interesach polityczno-ekonomicznych chronionego podmiotu, w kontekście zachodzenia rozmaitych zewnętrznych ryzyk i zagrożeń, istniejących w międzynarodowym systemie ekonomicznym"[1]. W ujęciu tym akcentowana jest zatem zarówno jedna z funkcji wewnętrznych państwa (integrowanie struktury ekonomicznej), jak i jedna z zewnętrznych (neutralizowanie zagrożeń, obecnych w systemie międzynarodowym). Patrząc na kwestię bardziej szczegółowo, działania w celu zapewnienia bezpieczeństwa ekonomicznego państwa maja na celu: ogólne „dostarczanie" bezpieczeństwa, bezpieczeństwo w dostępie do rynków, bezpieczeństwo finansowo-kredytowe, bezpieczeństwo zdolności do rozwijania technologii i przemysłu, bezpieczeństwo przyjętego w państwie paradygmatu społeczno-ekonomicznego, bezpieczeństwo transgraniczne i bezpieczeństwo sojuszy[2].

---

[1] Ch.M. Dent, *Economic Security*, [w:] *Contemporary Security Studies*, ed. A. Collins, Oxford 2010, s. 239.

[2] *Ibidem*, s. 253. Jest kwestią odrębną, czy takie mnożenie najróżniejszych „bezpieczeństw" jest w ogóle dorzeczne i sensowne, zabieg taki daje się jednak obronić w zależności od przyjętego pojęcia bezpieczeństwa.

Spojrzenie przez pryzmat podejścia *human security*, które, przypomnijmy, koncentruje się na zagrożeniach stwarzanych przez państwo dla własnego społeczeństwa, problem bezpieczeństwa ekonomicznego, w stosunku do zarysowanego przed chwilą, jest niejako odwrócony. Rozważane są mianowicie kwestie braku bezpieczeństwa ekonomicznego, z konsekwencjami takimi, jak: głód, niski poziom wykształcenia obywateli i wynikająca stąd ignorancja dotycząca zagrożeń, przemoc, brak determinacji w modernizowaniu państwa, itp.[3] Widać wyraźnie, że doprowadzania do takich zjawisk jest przeciwieństwem np. troski o wspomniane „generowanie zdolności do wykorzystania prosperity w interesach polityczno-ekonomicznych", przy czym należy pamiętać, że owe interesy mogą być pojmowane przez kierownictwa państw w bardzo różny sposób, a historia, również współczesna, dostarcza wielu argumentów przemawiających za wspomnianymi odrębnościami.

Ponadto wydaje się, że miejsce bezpieczeństwa ekonomicznego w ogólnej wizji bezpieczeństwa państwa uzależnione jest od podejścia do tego bezpieczeństwa. Inaczej postrzegać będzie kwestię zwolennik realizmu, kładącego nacisk na siłę militarną państwa, inaczej przedstawiciel konstruktywizmu społecznego, analizujący bezpieczeństwo państwa w kontekście ideologii, aksjologii i norm, zarówno w stosunkach wewnętrznych, jak i międzynarodowych, jeszcze inaczej do sprawy podejdzie ktoś wyznający poglądy liberalne, rozumiane tu jako najdalej idąca akceptacja dla demokracji, praw człowieka, wolności gospodarczej i międzynarodowej współpracy ekonomicznej, jako czynników przesądzających o bezpieczeństwie państwa[4].

Natomiast cele, jakie w zakresie bezpieczeństwa stawiają sobie organizacje gospodarcze (korporacje, spółki, itp., dalej, dla uproszczenia – przedsiębiorstwa), są inne. W zakres celów (nierozłącznych!) w zapewnianiu bezpieczeństwa konkretnej, pojedynczej organizacji gospodarczej wchodzą zazwyczaj prewencja (ograniczanie, redukcja, eliminacja) strat, będących konsekwencjami braku lojalności zatrudnianego personelu, następstwami utraty własnych informacji chronionych, strat powodowanych przemocą w miejscach pracy, przestępczości „białych kołnierzyków" (defraudacji i związanej z nią korupcji), działalności zorganizowanych grup przestępczych, wyspecjalizowanych w przestępczości gospodarczej, a także kryminalnej przestępczości pospolitej, szczególnie włamań i kradzieży. Nie jest to oczywiście lista kompletna, ale w tej chwili ma to znaczenie drugorzędne.

Wskazanie zróżnicowania w związanych z bezpieczeństwem celach państwa i przedsiębiorstwa ma znaczenie merytoryczne. Pora więc odnieść się do jego znaczenia metodologicznego.

III

Jak trafnie zauważa P.D. Williams, podstawowe pytania, wymagające odpowiedzi w toku studiów nad bezpieczeństwem, są następujące: (i) czym jest bezpieczeństwo?, (ii) o czyim bezpieczeństwie mówimy?, (iii) co zaliczymy do problemów

---

[3] P. Hough, *Understanding Global Security*, London–New York 2009, s. 92 i n.

[4] Przegląd teoretycznych podejść do bezpieczeństwa państwa znajdzie Czytelnik np. w pracy: *Security Studies. An Introduction*, ed. P.D. Williams, London–New York 2008.

bezpieczeństwa?, (iv) jak bezpieczeństwo może być osiągnięte?[5] Odpowiedzi na pytania (ii) i (iii) zostały już zarysowane, pytanie (iv) znajduje się zasadniczo poza zakresem niniejszego artykułu, pozostaje więc odpowiedzieć na pytanie (i).

Pojęć bezpieczeństwa jest, jak wiadomo, bardzo wiele i wybór jakiejś koncepcji roboczej jest trudny. Ze zrozumiałych względów wykorzystam definicję: „bezpieczeństwo określonego podmiotu jest stanem, w którym podmiot ten, w sytuacji konfliktu wartości, w zakresie posiadanego przez siebie zasobu dóbr, ma zdolność do suwerennego podejmowania i realizowania legalnych decyzji, zgodnych z uznawaną przez siebie hierarchią wartości"[6]. Rozważmy teraz konsekwencje tego ujęcia dla naszych analiz. Na uwagę zasługuje w szczególności kwestia, czy przytoczona definicja, traktowana jako sprawozdawcza, nadaje się do zastosowania w opisie problemów bezpieczeństwa obu typów analizowanych tu podmiotów, tj. państwa i przedsiębiorstwa. I tak:

- definicja wymaga dokładnego wskazania podmiotu, którego bezpieczeństwo jest przedmiotem studium (zauważmy, iż jest to zgodne z (ii) pytaniem P.D. Williama);
- pojęcia „stanu" i „sytuacji" są w omawianym kontekście niespecyficzne, nie wymagają więc eksplikacji, można je traktować jako pierwotne;
- w „konflikt wartości, w zakresie posiadanego przez siebie zasobu dóbr" może wejść zarówno państwo, jak i przedsiębiorstwo;
- „zdolność do suwerennego podejmowania i realizowania legalnych decyzji, zgodnych z uznawaną przez siebie hierarchią wartości" ma zarówno państwo, jak i przedsiębiorstwo, przynajmniej w jakimś fundamentalnie istotnym zakresie; kwestie ograniczenia suwerenności pomijam. Ważniejszy w tym kontekście wydaje się problem legalności działania, a to ze względu na możliwość sekurytyzacji, czyli przekroczenia (złamania) obowiązujących norm wobec konieczności neutralizacji zagrożenia, uznanego za egzystencjalnie ważne, to jednak również kwestia odrębna[7].

Jeśli zatem przyjąć, że przedstawiona definicja jest adekwatna do opisu koncepcji bezpieczeństwa państwa i przedsiębiorstwa, wówczas można uznać, że metodologiczne problemy wiedzy o bezpieczeństwie obu rozważanych typów podmiotów są względem siebie niespecyficzne. Szczegóły na ten temat omówiłem w cytowanej już pracy i obecnie podtrzymuję sformułowane tam propozycje[8]. Tutaj przypomnę tylko, że ich konsekwencjami są spostrzeżenia, iż:

- budowa unitarnego (uniwersalnego) pojęcia bezpieczeństwa, tzn. pojęcia użytecznego w analizie zróżnicowanych rodzajowo podmiotów jest możliwa;
- nauka (nauki) o bezpieczeństwie, metodologicznie biorąc, mieszczą się w paradygmacie nauk stosowanych, rozwiązujących zasadniczo problemy „jak powinno być, by osiągnąć określony cel?", czyli takich, których finalnym celem jest optymalizacja rozwiązań praktycznych. Można więc przyjąć, że na poziomie strategicznym celem nauk o bezpieczeństwie jest wyznaczenie optymalnego dla danego podmiotu poziomu bezpieczeństwa, na poziomie taktycznym natomiast – optymalne stosowanie poszczególnych środków bezpieczeństwa.

---

5 P.D. Williams, *Defining a field of inquiry: four fundamental questions*, [w:] *Security Studies*..., s. 5.

6 J. Konieczny, *O pojęciu bezpieczeństwa*, „Bezpieczeństwo. Teoria i Praktyka" 2012, nr 1(VI), s. 17.

7 Pojęcie sekurytyzacji zostało wprowadzone w ramach prac Szkoły Kopenhaskiej, bliżej na ten temat zob.: B. Buzan, O. Wæver, J. de Wilde, *Security. A New Framework for Analysis*, Boulder 1998.

8 J. Konieczny, *op. cit*.

Uwagi te wolno jednak (ewentualnie) uznać za trafne tylko na bardzo wysokim poziomie ogólności rozważań. Schodząc bowiem na poziom szczegółów, dotyczących budowy konkretnych systemów bezpieczeństwa, widać wyraźnie, że rozłożenie akcentów, dotyczących konkretnych aspektów bezpieczeństwa, jest zróżnicowane, czasem nawet bardzo silnie. Podanie przykładów nie jest trudne. Poziom ochrony informacji niejawnych w skali państwa jest o wiele bardziej restryktywny niż poziom ochrony informacji stanowiących tajemnicę przedsiębiorstwa, przynajmniej patrząc na te problemy z punktu widzenia normatywnego. Podobnie rzecz ma się z kompetencjami i zakresem działania służb siłowych – uprawnienia sił armii i policji są nieporównanie większe od możliwości działania struktur ochrony fizycznej w przedsiębiorstwie. Z drugiej strony, kontrola dostępu na terytorium państwa, przynajmniej w przypadku niektórych przybyszów, jest prowadzona bardzo liberalnie, zaś dostęp na „terytorium" przedsiębiorstwa może być czasem skrajnie restryktywny. Co jednak ważniejsze – w licznych przypadkach dochodzi do współpracy instytucji państwowych z przedsiębiorstwem, w zakresie zapewnienia bezpieczeństwa temu ostatniemu. Nie od rzeczy będzie też zapytać, czy oba rozważane tu typy podmiotów mogą czerpać wzajemne korzyści z wymiany doświadczeń płynących z działania ich systemów bezpieczeństwa[9]. Dlatego dalsza część artykułu zmierzać będzie do odpowiedzi na pytania: jaki jest zakres współpracy publiczno-prywatnej w dziedzinie bezpieczeństwa omawianych typów organizacji, czy współpraca ta jest/może być wzajemnie korzystna, oraz czy problemy, wynikające z owej współpracy mają wpływ na metodologiczne aspekty rozszerzania wiedzy o bezpieczeństwie.

IV

Przyjmuje się, że ataki 11 września 2001 r. rozpoczęły nową epokę w sposobach myślenia o bezpieczeństwie państwa, a jedna z fundamentalnych zmian w owym myśleniu dotyczyła wzajemnych relacji pomiędzy państwem a przedsiębiorstwem, a ściślej – w podziale obowiązków pomiędzy tymi typami podmiotów. Dotychczasowa zasada „płacę podatki – oczekuję bezpieczeństwa" odeszła do lamusa. Owszem, przedsiębiorstwa bardzo często uzupełniały na własny koszt zakres ochrony dostarczanej przez państwo, zawsze też dokonywały transferu określonych ryzyk poprzez korzystanie z ubezpieczeń, teraz jednak ich udział w zapewnieniu własnego bezpieczeństwa stał się wyraźnie (choć oczywiście nie w stopniu pełnym) zintegrowany z systemem bezpieczeństwa państwa.

Na zmianę okazały się szczególnie podatne dwa obszary bezpieczeństwa, związane mianowicie z terroryzmem i przestępczością zorganizowaną. Nie jest to niczym nowym, ale zakres wzajemnych relacji publiczno-prywatnych w neutralizacji związanych z tymi zjawiskami zagrożeń znacznie się rozszerzył. Przyczyny tego stanu są

[9] W pewnym sensie taka wymiana doświadczeń następuje w sposób naturalny wówczas, gdy członkowie personelu instytucji państwowych, specjaliści w zakresie bezpieczeństwa, po zakończeniu służby, podejmują pracę w przedsiębiorstwach, wykorzystując w niej swoją wiedzę, kontakty, itd. Na ogół nie ma w tym niczego złego. Zjawisko to bywa określane jako tradycja „drzwi obrotowych" (zob. L. Johnson, *Private investigation*, [w:] *Handbook of Criminal Investigation*, eds. T. Newburn, T. Williamson, A. Wright, Cullompton 2007, s. 292.

następujące. Jak wiadomo, podstawowym czynnikiem sprzyjającym zapobieganiu aktom terroryzmu jest możliwie szeroko prowadzone rozpoznanie, inaczej: wywiad. Służby państwowe wywiad taki oczywiście prowadzą, ale jego skuteczność jest mocno uwarunkowana współpracą z przedsiębiorstwami, szczególnie finansowymi, takimi jak banki, mogącymi dokładnie, na bieżąco, wykrywać i monitorować transakcje podejrzane, z których przynajmniej niektóre związane bywają z finansowaniem terroryzmu czy jakimiś formami przestępczości zorganizowanej. Stworzenie warunków prawnych do przekazywania tego rodzaju informacji służbom państwowym z pewnością sprzyja analizie informacji wywiadowczych, uzyskiwanych również z innych źródeł. Służby te są również zainteresowane wzmacnianiem ochrony przeciwterrorystycznej w portach lotniczych, w transporcie żywności, obrocie materiałami chemicznymi i medycznymi, w ochronie infrastruktury krytycznej, czy wreszcie w bezpieczeństwie sieci teleinformatycznych. Z drugiej strony, przedsiębiorstwa nie mogą czekać i wypatrywać co państwo zrobi dla ich ochrony[10]. Wręcz przeciwnie, w ich najlepiej pojętym interesie leży wzajemnie korzystna współpraca z instytucjami państwowymi.

Kluczowym czynnikiem służącym zapewnieniu bezpieczeństwa, a krytycznie obecnym na styku państwo–przedsiębiorstwo, jest wywiad, co zostało już podkreślone. Oczywiście, zasadnicze cele wywiadu prowadzonego przez służby państwowe i przedsiębiorstwa są inne, ale odmienność ta ma swoje granice. Jeśli uznać, że wywiad, w sensie rodzaju działalności, jest utajnioną aktywnością państwa, mającą na celu zrozumienie i/lub uzyskanie wpływu na podmioty, stanowiące realne czy potencjalne zagrożenie, a także na identyfikację okazji i szans dla rozwoju[11], wówczas okaże się, że cele wywiadu gospodarczego, prowadzone przez przedsiębiorstwa są analogiczne, tyle że prowadzone, przynajmniej oficjalnie, metodami jawnoźródłowymi i oczywiście „skrojonymi" na miarę potrzeb przedsiębiorstwa; wywiad państwowy, szczególnie przeciwterrorystyczny, jest „totalny", ponieważ terrorystą jest lub może stać się każdy. Stąd z punktu widzenia służb państwowych wywiad może obejmować każdego, dotyczyć wszystkiego, wszędzie, i to bez szczególnego powodu[12].

Mimo zróżnicowanych celów, a także różnic metodycznych (od wywiadu „białego", po operacyjny, w tym agenturalny), istnieje bardzo istotna zbieżność metodologiczna wszystkich metodyk wywiadowczych. Świadomość tego faktu datuje się od czasu stosunkowo niedawnego, przypada bowiem na początek bieżącego stulecia. Chodzi o to, że status poznawczy informacji wywiadowczej jest taki sam, niezależnie od źródła, z której informacja pochodzi. Tak więc informacje uzyskana np. w wywiadzie kryminalnym, przeciwterrorystycznym, antykorupcyjnym, skarbowym, w kontrwywiadzie, w wywiadzie zagranicznym, a także w jawnoźródłowym wywiadzie gospodarczym, mają takie same charakterystyki metodologiczne, a metodyka ich pozyskania czy też instytucja pozyskująca nie mają znaczenia

---

[10] I. Gyarmati, *Security and the responsibilities of the public and private sectors*, [w:] *Business and security. Public – Private Sector Relationships in a New Security Environment*, eds. A.J.K. Bailes, I. Frommelt, Oxford 2009, s. 30.

[11] Por. M. Warner, *Wanted: A Definition of 'intelligence'*, [w:] *Secret Intelligence. A Reader*, eds. Ch. Andrew, R.J. Aldrich, W.R. Wark, Routledge, London–New York 2009, s. 9.

[12] Ch. Boukalas, *Homeland Security, its Law and its State. A Design of Power for the 21st Century*, London–New York 2014, s. 143.

merytorycznego[13]. Takie same reguły obowiązują też w szacowaniu wiarogodności źródła oraz ewaluacji informacji i jej przepływu. Niespecyficzny metodologicznie wydaje się również problem analizy informacji wywiadowczej. W każdym z wymienionych przypadków analiza ta zmierza, najogólniej biorąc, do uzyskania odpowiedzi na pytania „co?" (co się wydarzyło, co wiemy na określony temat, co jeszcze należałoby wiedzieć) i „co z tego?" (jakie są następstwa powstałej sytuacji?, jak je rozumieć (interpretować), co może wydarzyć się w przyszłości? jakie decyzje należy podjąć?[14]), a trafność tych odpowiedzi przesądza o wartości analizy. Nie ulega więc wątpliwości, że rozszerzanie wiedzy na temat wywiadu, w sensie metodologicznym, podlega tym samym regułom w wywiadzie prowadzonym przez instytucje państwowe i przez przedsiębiorstwa.

V

Wydaje się, że łatwo wskazać także inne analogie metodologiczne w rozwijaniu wiedzy, dotyczącej bezpieczeństwa państwa i przedsiębiorstwa, wskazując mianowicie na aspekt optymalizacyjny wiedzy o tych zjawiskach, będący zresztą, jak już wiadomo, konsekwencją statusu nauki/nauk o bezpieczeństwie jako nauk stosowanych. Przypomnijmy, że twierdzenia (prawa) optymalizacyjne to wyrażenia o postaci: jeżeli występują takie to a takie warunki, to realizacja takiej to a takiej czynności prowadzi do wystąpienia badanej wielkości w stopniu określonym. Stopień ten dla dysponenta systemu bezpieczeństwa może być satysfakcjonujący albo nie. Jeśli nie jest, wymaga to prowadzenia dalszych badań. Zwrot „występują takie to a takie warunki" należy rozumieć w sposób następujący. Na każdą badaną wielkość w systemie bezpieczeństwa działają dwa typy czynników. Pierwszy z nich obejmuje czynniki, którymi dysponent systemu może manipulować, tzn. może regulować ich natężenie, sposób działania, kryteria podjęcia decyzji o ich stosowaniu, itd. Do czynników drugiego typu należą te, na które dysponent systemu nie ma wpływu. Należą tu przede wszystkim (choć nie tylko) formy aktywności przeciwnika, takie jak stosowane przezeń ataki socjotechniczne, mające na celu przełamywanie lojalności personelu obsługującego system bezpieczeństwa (np. werbunki, korupcja), stosowanie technicznych środków, godzących w system (np. podsłuchy), itd. Oczywiście, wystąpienie czynników tego typu można i należy przewidywać, ale uzyskiwanie wpływu na ich wystąpienie jest bardzo trudne, a zazwyczaj niemożliwe; często możliwe jest tylko podjęcie akcji, zmierzającej do neutralizacji, dopiero po stwierdzeniu ich zachodzenia. Dlatego kluczowa jest kwestia wiedzy na temat działania czynników manipulowanych i potem, na jej podstawie, budowa twierdzeń optymalizacyjnych. Nie widać jednak żadnych powodów, by opisywane procedury poznawcze miały być odmienne w bezpieczeństwie państwa i w bezpieczeństwie biznesu.

Aspekt metodologiczny wprowadzania zmian, unowocześniających systemy bezpieczeństwa, rozważała J. Wood[15]. Autorka stwierdziła, że ogólna koncepcja me-

---

[13] Zob. Ch.P. Nemeth, *Homeland Security: An Introduction to Principles and Practice*, Boca Raton 2010, s. 280–281.

[14] T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 25.

[15] J. Wood, *Research and innovation in the field of security: a nodal governance view*, [w:] *Democracy, Society and the Governance of Security*, eds. J. Wood, B. Dupont, Cambridge 2006, s. 217.

todologiczna, pozwalająca na projektowanie, wprowadzanie i rozpowszechnianie innowacji w dziedzinie bezpieczeństwa, polega na uwzględnieniu trzech kluczowych komponentów, które można też traktować jako etapy tworzenia rozwiązań innowacyjnych. Pierwszym jest wyczerpujące, empiryczne badanie aktualnego stanu bezpieczeństwa w jakimś rozważanym kontekście. Drugi obejmuje oszacowanie luk i ograniczeń (także etycznych oraz normatywnych), występujących w systemie. Po ich rozpoznaniu można przejść do etapu trzeciego, polegającego na projektowaniu i wprowadzaniu nowości w dostarczaniu bezpieczeństwa. J. Wood pisze, iż proponowana metodologia może być stosowana zarówno na poziomie mikro, np. miasta, jak i makro, obejmującym całe państwo[16]. Z naszego punktu widzenia to ostatnie stwierdzenie jest najważniejsze, potwierdza bowiem tezę o braku specyfiki metodologicznej badań nad bezpieczeństwem w zależności od podmiotu bezpieczeństwa.

VI

Dobrym przykładem daleko idących analogii metodologicznych w dziedzinie badań nad bezpieczeństwem są problemy związane z rozpoznawaniem zagrożeń, formułowania oszacowań określonych stanów rzeczy, itd. Warto w tym kontekście wymienić *Maryland Scientific Methods Scale*, bardzo proste i uniwersalne narzędzie, pozwalające na skuteczną ewaluację efektywności wdrażanych środków bezpieczeństwa. Mówiąc najogólniej, metoda polega na uzyskaniu odpowiedzi na pytania: co działa?, co nie działa?, co jest rozwiązaniem, prowadzącym w dobrym kierunku?, czego nie wiemy? Autorzy metody podają precyzyjną, wykorzystującą metody statystyczne, procedurę interpretacji wyników. Skala ta może być stosowana zarówno na poziomie lokalnym, jak i dalece ogólniejszym, w zależności od potrzeb i jest przeznaczona dla teoretyków, polityków i praktyków[17].

Czymś podobnym, choć nieco bardziej skomplikowanym, jest *Actionable Mining and Predictive Analysis for Public Safety and Security*. Punktem wyjścia jest sformułowanie problemu („wyzwania"), po którym następuje gromadzenie, łączenie i kodowanie danych, wybór zmiennych, ich charakterystyka, budowa modelu, ewaluacja wyników i przełożenie ich na dyrektywy działania. Podstawą tego podejścia jest również analiza statystyczna, choć dostosowana w każdym przypadku do jego specyfiki. Również w tym przypadku skala (rozmiar) badanych zjawisk może być bardzo zróżnicowana[18].

Zarówno do celów państwowych, jak i biznesowych opracowany został *Gateway Remote Access Service Provider.* Gdy korporacja lub agencja rządowa zamierza wesprzeć proces decyzyjny i gromadzi dostępne informacje, zwykle nie ogranicza się do jednej bazy danych, lecz stara się wykorzystać ich wiele, co właśnie umożliwia wspomniany system, pozwalając jednocześnie na budowę sieci powiązań rozpoznawanego

[16] *Ibidem*, s. 219.

[17] D.P. Farrington, D.C. Gottfredson, L.W. Sherman, B.C. Welsh, *Maryland Scientific Methods Scale*, [w:] *Evidence-Based Crime Prevention*, eds. L.W. Sherman, D.P. Farrington, B.C. Welsh, D.L. MacKenzie, London–New York 2006, s. 13.

[18] C. McCue, *Data Mining and Predictive Analysis. Intelligence Gathering and Crime Analysis*, Amsterdam 2007, s. 53.

obiektu. Procedura może zostać wykorzystana do celów bezpieczeństwa w szerokim kontekście i jest narzędziem gromadzenia informacji oraz ich analizy[19].

W szeroko rozumianym bezpieczeństwie państwa i bezpieczeństwie biznesu (a także w działaniach marketingowych) swoje dobrze ugruntowane miejsce ma analiza źródeł internetowych. Specyficzne metodyki badawcze pozwalają w tym zakresie na dokonywanie istotnych ustaleń, w rodzaju identyfikacji i dynamiki zagrożeń, trendów rozwojowych określonych zjawisk, analizę sieci powiązań, badanie opinii, itd.[20]

Jest jasne, że wspomniane tu metody są jedynie przykładami, ich ewolucja i rozwój następuje bardzo szybko, jest jednak przy tym bardzo interesujące, że źródła internetowe uchodzą nie tylko ciągle za nowe, ale – co więcej – ich eksploatacja staje się podstawową (i bardzo trudną w wykorzystaniu) bazą informacyjną w pełni profesjonalnych, państwowych agencji wywiadowczych, a to za sprawą informacji, znajdujących się w warstwach „głębokich" i „ciemnych" Internetu[21].

VII

Jednakże przypuszczenie, że najdalej idąca zbieżność metodologiczna w rozwijaniu wiedzy o bezpieczeństwie państwa i bezpieczeństwie biznesu powoduje istnienie jakiejś „wspólnoty interesów" w prowadzeniu badań, byłoby, przynajmniej częściowo, fałszywe[22]. Istnieje kilka przyczyn tego stanu rzeczy.

Akademickie kursy, dotyczące bezpieczeństwa państwa, przygotowują przyszłych zawodowców na teoretycznej podstawie stosunków międzynarodowych i ogólnej wiedzy o „działaniu świata". Wykorzystywane przy tym koncepcje są na ogół dobrze utrwalone w literaturze, konserwatywne, pełne wiedzy konwencjonalnej i siłą rzeczy dość odpornej na nowości. Celem nauczania jest implantowanie studentom raczej widzenia strategicznego i umiejętności budowania „wielkich obrazów". Służby państwowe są zresztą nastawione na zatrudnianie osób o takim profilu kwalifikacji profesjonalnych. Tymczasem potrzeby korporacji w zakresie bezpieczeństwa są inne: lokalne, specyficzne dla spółek, i najczęściej o charakterze taktycznym. Na to nakłada się problem finansowania bezpieczeństwa. O ile w skali państwa ciężary te są ponoszone przez ogół podatników i rozkład wydatków podlega pewnej elastyczności w ramach budżetu, o tyle korporacje swoje unikalne potrzeby muszą zaspokajać same, co istotnie wpływa w ogóle na myślenie o bezpieczeństwie.

W przypadku państwowych służb wywiadowczych głównym celem gromadzenia informacji jest identyfikacja zagrożeń, a poziom dzielenia się tymi informacjami z biznesem prywatnym – bardzo ograniczony, zwykle do jednostkowych, konkretnych sytuacji. Tymczasem wywiad gospodarczy skoncentrowany jest na kwestiach

---

19 J. Mena, *Investigative Data Mining for Security and Criminal Detection*, Amsterdam 2003, s. 327.

20 Wiele ważnych informacji na ten temat znajdzie Czytelnik w pracy: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, red. W. Filipkowski, W. Mądrzejowski, Warszawa 2012.

21 Zob. A. Rolington, *Strategic Intelligence for the 21st Century. The Mosaic Method*, Oxford 2013, s. 83.

22 Problem ten bardzo wnikliwie analizowali C. Stapley, S. Grillot, S. Sloan, *The Study of National Security Versus The Study of Corporate Security: What Can They Learn From Each Other?*, [w:] *The Handbook of Security*, ed. M. Gill, Houndmills 2006, s. 45.

konkurencji rynkowej, a jeśli dotyczy bezpieczeństwa przedsiębiorstwa, to zwykle obejmuje ochronę stanu posiadania, informacji i zasobów ludzkich i materialnych. Wywiad gospodarczy jest ponadto ograniczony metodycznie: ze względów prawnych głęboki HUMINT (*human intelligence*, w praktyce – wywiad agenturalny) jest praktycznie niemożliwy, a przynajmniej bardzo ryzykowny.

Inne są także miary poziomu bezpieczeństwa. Bezpieczeństwo państwa wymaga przede wszystkim rozpoznania przeciwników, ich intencji i możliwości, kwestią bardzo istotną są także działania kontrwywiadowcze i przeciwterrorystyczne. Liczą się zatem wyniki służb w tym zakresie, i to głównie na poziomie strategicznym. Bezpieczeństwo przedsiębiorstwa natomiast jest strategicznie angażowane w stopniu niewielkim. Główne wysiłki skierowane są kwestie taktyczne, dotyczące neutralizacji konkretnych i często specyficznych zagrożeń. Literatura dotycząca bezpieczeństwa biznesu koncentruje się niemal wyłącznie na sposobach prowadzenia działań zmierzających do redukcji wyeksponowania zasobów przedsiębiorstwa na określone zagrożenia[23].

Podsumowując, warto raz jeszcze podkreślić, że:

- bezpieczeństwo państwa i bezpieczeństwo biznesu są możliwe do opisu jednym ujęciem definicyjnym;
- ostatecznym celem rozszerzania wiedzy w obydwóch typach podmiotów jest wytwarzanie twierdzeń optymalizacyjnych, co jest charakterystyczne dla nauk stosowanych;
- nauki o bezpieczeństwie są naukami stosowanymi;
- z metodologicznego punktu widzenia zachodzi tożsamość pomiędzy nauką o bezpieczeństwie państwa i nauką o bezpieczeństwie przedsiębiorstwa;
- cele działania państwa są odmienne od celów działania przedsiębiorstwa;
- przedmiot badań w zakresie bezpieczeństwa państwa jest więc, częściowo, odmienny od przedmiotu badań w bezpieczeństwie biznesu.

[23] *Ibidem*, s. 52–59.