BEZPIECZEŃSTWO 2011 nr 1 TEORIA I PRAKTYKA

Mateusz Mucha

Niektóre metody nielegalnego pozyskiwania informacji w rywalizacji konkurencyjnej przedsiębiorstw

Wprowadzenie

Wywiad gospodarczy, zwany też wywiadem konkurencyjnym, marketingowym, organizacyjnym czy ekonomicznym od lat osiemdziesiątych XX w. stał się normalnym środkiem, stosowanym w zarządzaniu przedsiębiorstwem[1]. Owa normalność polega przede wszystkim na tym, że jego istota, czyli gromadzenie informacji o podmiotach gospodarczych, jest legalna, dokonuje się z poszanowaniem prawa i dobrych obyczajów. Międzynarodowe organizacje zrzeszające zawodowych wywiadowców gospodarczych już dawno uznały legalność swoich działań jako ich minimum etyczne, wyrzekając się przy okazji podstępnego uzyskiwania informacji[2], deklaracja przestrzegania prawa miejscowego i międzynarodowego znajduje poczesne miejsce w kodeksie etycznym *Strategic and Competitive Intelligence Professionals*, podstawowa literatura na temat biznesowego wykorzystania danych z wywiadu gospodarczego w ogóle nie przewiduje pozyskiwania informacji ze źródeł nielegalnych[3]. Dlatego właśnie wywiad gospodarczy, w jego standardowym ujęciu, uchodzi za „biały", czyli wykorzystujący tylko źródła oficjalne i jawne, w szczególności zaś zawierające informacje niechronione prawnie przez ich dysponentów.

Niemniej jednak naiwnością byłoby udawanie, że rozpoznawanie konkurencji odbywa się wyłącznie w „białych rękawiczkach". Równolegle bowiem do oficjalnego

[1] M. Kwieciński, *Wywiad gospodarczy w zarządzaniu przedsiębiorstwem*, Warszawa–Kraków 1999; L. Korzeniowski, A. Pepłoński, *Wywiad gospodarczy. Historia i współczesność*, Kraków 2005.

[2] B. Martinet, Y.M. Marti, *Wywiad gospodarczy. Pozyskiwanie i ochrona informacji*, Warszawa 1999.

[3] Zob. np. L.T. Moss, S. Atre, *Business Intelligence Roadmap. The Complete Project Lifecycle for Decision-Support Applications*, Boston 2003.

nurtu wywiadu ekonomicznego realizowane są działania utajnione, nie tylko nieliczące się z interesami rozpoznawanych podmiotów, ale wprost ukierunkowane na ich szkodę, poprzez właśnie nielegalne zdobywanie zastrzeżonych informacji – przede wszystkim technologicznych lub handlowych. Tego rodzaju działalność określana bywa jako wywiad „czarny" lub po prostu, choć niezbyt ściśle, jako szpiegostwo gospodarcze. Celem tego artykułu jest przedstawienie ogólnej charakterystyki „czarnego" wywiadu gospodarczego.

Nie wchodząc w szczegóły definicyjne, należy zauważyć, że „czerń" i „biel" nie stanowią dychotomii w podziale działań wywiadowczych. Jeśli przyjąć, że poziom naruszenia prawa może być stopniowalny (a tak jest w rzeczywistości, bo dany czyn może być zakwalifikowany np. jako wykroczenie, występek albo zbrodnia, cywilizowane sądy mają także zawsze określoną ustawowo swobodę decyzji w ustalaniu wysokości kary; wydaje się również, że takiemu stopniowaniu, niezależnie od filozoficznych sporów dotyczących dorzeczności wyróżniania zła „mniejszego" i „większego", podlegają także naruszenia norm moralnych). To owa stopniowalność upoważnia do wskazania różnych odcieni, zawartych pomiędzy „bielą" a „czernią" rozważanych działań. Wywiad jest jednoznacznie „czarny", gdy od początku, świadomie i z rozmysłem prowadzony jest z zamiarem złamania prawa, chroniącego jakąś tajemnicę, w innych przypadkach nasilenie „czerni" może być mniejsze. Jakkolwiek by jednak było, rygoryzm definicyjny nie jest tu ani możliwy, ani też potrzebny, bo intuicja w proponowanej refleksji jest wystarczająca.

Należy jeszcze dodać, że współcześnie, mimo stale doskonalonych środków i metod ochrony, uzyskiwaniu informacji sprzyja, wbrew pozorom, szereg następujących okoliczności:

- zasoby wywiadowcze, poddawane w czasie zimnej wojny silnym rygorom utajnienia i przeznaczone wtedy przede wszystkim do zastosowań militarnych, stały się bardziej dostępne dla biznesu,
- różne formy własności stają się coraz bardziej wirtualne, a przez to bardziej narażone na kradzież, trudniejszą do wykrycia niż „tradycyjna" kradzież rzeczy materialnej,
- w przedsiębiorstwach rośnie liczba osób, mających dostęp do firmowych tajemnic, co powoduje, że rosną możliwości wykorzystania wiedzy służbowej do osiągania osobistych korzyści materialnych[4],
- rozwój mobilnych urządzeń, służących do przechowywania i przetwarzania informacji (palmtopy, inne przenośne komputery), powodujący decentralizację baz danych i ich trudniejszą ochronę,
- wzrost liczby personelu pracującego poza biurami, co rozmywa skuteczność środków ochrony informacji, w szczególności wiele danych wrażliwych lokalizowanych jest poza granicami stref chronionych fizycznie,
- rozwój internetu, sprzyjający dokonywaniu włamań przez hackerów, i to w sposób stosunkowo łatwy i bezpieczny dla sprawców[5].

[4] H. Nasheri, *Economic Espionage and Industrial Spying*, Cambridge 2005, s. 52–55.

[5] R.L. Mendell, *The Quiet Threat. Fighting Industrial Espionage in America*, Springfield 2003, s. 6–7.

Główne podmioty prowadzące działalność w zakresie wywiadu gospodarczego

Przedstawienie podmiotów, prowadzących interesujący nas tu rodzaj działalności, należy rozpocząć od państwowych agencji wywiadowczych. Niektóre z nich, jak organizacje wywiadu francuskiego, tradycyjnie wspierają (od czasów króla Ludwika XIV) rodzimy przemysł; także dzisiaj francuski wywiad wojskowy i strategiczny (Dyrekcja Generalna Bezpieczeństwa Zewnętrznego, *DGSE*) służy taką pomocą, w przypadkach finansowo uzasadnionych[6]. Z licznych doniesień wynika także, iż w okresie zimnej wojny służby wywiadowcze państw Wschodu i Zachodu nader intensywnie prowadziły wywiad naukowo-techniczny i gospodarczy. Wywiad PRL nie należał w tym zakresie do wyjątków, a do jego zadań należało m.in. „Zdobywanie informacji i dokumentacji z zakresu najnowszych osiągnięć naukowych i postępu technicznego w krajach kapitalistycznych na zapotrzebowanie poszczególnych resortów gospodarczych i instytucji naukowych PRL"[7].

Sytuacja skomplikowała się po zakończeniu zimnej wojny. Państwa słabo rozwinięte „mogą wydać biliony dolarów i czekać dekady na rozwój własnej technologii, albo mogą wydać mniej niż milion i ukraść je jutro", jednocześnie jednak trzeba pamiętać, że zainteresowania takich państw rzadko kierują się ku technologiom najbardziej zaawansowanym, a ich działalność koncentruje się raczej na rozwiązaniach mniej nowoczesnych[8]. Inna jest sytuacja państw o statusie mocarstw, a pewnych danych można domyślać się na przykładzie USA. Wprawdzie w roku 1993 powołana tam została Narodowa Rada Ekonomiczna (*National Economic Council*), mająca m.in. promować współpracę agencji wywiadowczych z prywatnym biznesem, w celu wzmacniania gospodarki amerykańskiej[9]. CIA wydawała tajny biuletyn *Economic Intelligence Weekly* (czy wydawany jest nadal – nie wiadomo, obecnie w niewielkiej części odtajnione są jego fragmenty sprzed kilkunastu lat i można je znaleźć w internetowych wyszukiwarkach), ale cel ten, jak się zdaje, uległ modyfikacji.

Przesłanki przemawiające przeciwko angażowaniu agencji państwowych w wywiad gospodarczy są następujące: możliwość powstania poważnych problemów prawnych, związanych z podjęciem decyzji o operacji, trudna do przewidzenia i często wątpliwa ostateczna efektywność ekonomiczna ewentualnie uzyskanego wyniku, niedogodność wynikająca z częstej w takich sytuacjach konieczności podjęcia akcji przeciwko korporacjom międzynarodowym i wreszcie groźba wywołania konfliktu w przypadku zbyt agresywnego prowadzenia działań[10]. Pozostaje więc wycofanie się z tej działalności albo ograniczanie jej do stosowania metod „białych". Z drugiej strony, firmy amerykańskie znajdują się pod presją wywiadowczą służb zagranicznych, co wymaga przeciwdziałania. Oprócz normalnych operacji kontrwywiadowczych moż-

---

[6] I. Winkler, *Corporate Espionage*, Rocklin 1997, s. 68.

[7] P. Piotrowski, *Specyfika pracy organizacyjnej wywiadu PRL*, „Biuletyn Instytutu Pamięci Narodowej" 2007, nr 5–6 (76–77), s. 90; *Instrukcje pracy operacyjnej aparatu bezpieczeństwa (1945–1989)*, oprac. T. Rudzikowski Warszawa 2004, s. 142.

[8] I. Winkler, *op. cit.* s. 74.

[9] H. Kozioł, Systemy szpiegostwa elektronicznego, 2006, www.psz.pl/tekst-2204, dostęp: wrzesień 2011.

[10] M. Burton, *Government Spying for Commercial Gain*, „Center for Study of Intelligence: Studies Archive Indexes" 2007, t. 37, nr 2.

liwe jest wprowadzanie sankcji przeciwko krajom agresywnym, można też redukować zagrożenie na drodze traktatowej (M. Burton nie pisze wprost o stosowaniu zasady wzajemności). Wyjątkiem jest niekwestionowana celowość prowadzenia wywiadu w zakresie technologii militarnych, także tych opracowywanych i realizowanych w zagranicznych przedsiębiorstwach prywatnych, wtedy jednak działanie dyktowane jest potrzebami bezpieczeństwa narodowego i z natury rzeczy lokuje się ono w strefie wywiadu co najmniej „szarego"[11].

Wniosek wydaje się prosty: jeśli określony segment utajnionej informacji gospodarczej zostanie uznany przez dysponentów państwowej agencji wywiadowczej za istotny dla interesów państwa, wtedy decyzja o próbie uzyskania tej informacji jest bardzo prawdopodobna, o ile analiza korzyści finansowej i ryzyka politycznego wypadnie pomyślnie.

Czołowym aktorem na scenie czarnego wywiadu gospodarczego są jednak wyspecjalizowane firmy prywatne. Wprawdzie 90% dużych przedsiębiorstw amerykańskich posiadało (dane z r. 2002) komórki wywiadu gospodarczego i większość z nich przeznaczała na swą działalność ponad milion dolarów rocznie, a mniejsze podmioty, w tym także organizacje *non-profit*, również wywiad uprawiały, to jednak świadczy to przede wszystkim o docenianiu roli tego źródła informacji[12], niekoniecznie zaś o tak powszechnym angażowaniu się w czarny wywiad. Metodyka i metodologia wywiadu jawnoźródłowego były w ciągu minionej dekady, i nadal są, stale i wszechstronnie doskonalone[13]. W tej sytuacji nie ma powodów, by angażować się w ryzykowne działania, narażające na zarzut łamania prawa, korzystniej jest zlecić je komuś innemu, gwarantującemu dyskrecję i, z reguły, skuteczność. Kwestią odrębną jest konspiracja zlecenia, tu często budowany jest łańcuch pośredników, służący ukryciu podmiotu faktycznie zainteresowanego nielegalnym pozyskaniem informacji. Inną możliwością jest wykorzystanie specjalnych, tzw. czarnych sieci, które umożliwiają anonimowy kontakt zleceniodawcy i zleceniobiorcy[14].

Głównym motywem skłaniającym do podejmowania zadań szpiegowskich są oczywiście pieniądze – perspektywy honorariów, oferowanych za dostarczenie określonej wiedzy bywają oszałamiające, choć jednocześnie niemożliwe do uchwycenia w jakikolwiek zobiektywizowany sposób; nikt nie pochwali się, ile i za co zapłacił, nikt także nie przyzna się badaczowi problemu, ile i za co mu zapłacono. Warto natomiast wspomnieć, że często zdarza się, że bezpośredni dostawca informacji, z reguły nielojalny pracownik rozpoznawanej firmy, otrzymuje kwotę znikomą lub nie otrzymuje niczego, nawet niczego nie żądając w zamian za swą usługę, gdy działa na przykład powodowany chęcią zemsty na pracodawcy lub z silnych pobudek ideologicznych. W takich przypadkach całą korzyść przejmuje organizator szpiegowskiej operacji.

---

[11] *Ibidem*.

[12] H. Nasheri, op. cit., s. 75.

[13] Zob. np. J. Liebowitz, *Building Organizational Intelligence. A Knowledge Management Primer*, Boca Raton 2000; G.J. Miller, D. Bräutigam, S.V. Gerlach, *Business Intelligence Competency Centers. A Team Approach to Maximizing Competitive Advantage*, Hoboken 2006; R. King, *Business Intelligence Software's Time Is Now*, „Bloomberg Businessweek", March 2, 2009, www.businessweek.com/technology/content/mar2009/tc2009032_101762.htm, dostęp: wrzesień 2011.

[14] D.L. Pipkin, *Bezpieczeństwo informacji. Ochrona globalnego przedsiębiorstwa*, Warszawa 2002, s. 232.

Trzon kadrowy firm zajmujących się „czarnym" wywiadem stanowią zazwyczaj osoby legitymujące się wcześniejszym stażem w służbach specjalnych. Jest to zrozumiałe – eks-oficerowie mają stosowne kwalifikacje, znają techniki działania, potrafią przewidywać i rozwiązywać problemy specyficzne dla ich profesji, niejednokrotnie także korzystają z – bywa, że przestępczej – pomocy kolegów, pozostających w służbie, zazwyczaj w postaci dostępu do specjalistycznych, niejawnych baz danych, co znakomicie ułatwia pracę. W gruncie rzeczy w zatrudnianiu w firmach (zwykle deklarujących się jako detektywistyczne lub konsultingowe, doradcze) byłych pracowników państwowych agencji wywiadowczych nie ma niczego dziwnego, temat ten jednak obrasta w sensacyjne doniesienia i domysły, jak zawsze w przypadku działań ukrytych przed opinią publiczną (a tworzona na tej kanwie publicystyka czy literatura faktu może liczyć na szerokie zainteresowanie czytelnicze; przykładem takiego dzieła jest książka: E. Javers 2010).

Wśród podmiotów organizujących i realizujących „czarne" przedsięwzięcia rozpoznawcze trzeba też wymienić zorganizowane grupy przestępcze. Motywy działania są różne, raz może chodzić o pozyskanie informacji o nieprawidłowościach (np. podatkowych) w firmie, co potem da się wykorzystać do szantażowania przedsiębiorcy (to właśnie biznesmeni oszukujący fiskusa stają się najłatwiejszymi ofiarami wymuszania haraczy), czasem firmy są penetrowane przez zorganizowaną przestępczość, szukającą okazji do prania pieniędzy lub innych form legalizacji zysków (poprzez np. kapitałowe wejście w spółkę, z perspektywą jej przejęcia), czasem zaś uzyskana informacja jest traktowana jako towar na „czarnym" rynku wywiadowczym. Rzecz charakterystyczna, że grupy terrorystyczne zainteresowane bywają nie tylko informacjami mającymi wartość gospodarczą, lecz ponadto pozyskują dane na temat osobistych właściwości menedżerów, ich stylu życia, sposobów spędzania wolnego czasu, stosunków rodzinnych itp., tak by „wiedzieć wszystko" o swoich potencjalnych ofiarach[15].

W tym kontekście trzeba wspomnieć, że przedsiębiorstwa chronią swoje informacje nie tylko ze względów prawnie (i społecznie) akceptowalnych. Powody takiej „powściągliwości" w ujawnianiu wiedzy na swój temat mogą być następujące: ograniczenie możliwości działania komorników, zamiar poprawy obrazu rynkowego firmy poprzez ukrywanie informacji dla niej niekorzystnych, przygotowania do podjęcia działalności nielegalnej (np. przestępstwa/przestępstw podatkowych czy gospodarczych), względy polityczne, światopoglądowe lub inne, także osobiste[16].

Na końcu wymienić trzeba media, czasem niepohamowane w dążeniu *per fas et nefas* do uzyskania atrakcyjnych informacji, często w myśl zasady *„bad news is good news"*. O tym, że uwaga ta nie jest gołosłowna, świadczy chociażby ostatnio globalnie głośna afera koncernu R. Murdocha.

Dodajmy jeszcze, że rozpoznaniem, także metodami „czarnymi", mogą być zainteresowani np. kooperanci przedsiębiorstwa. Nie będzie to rozpoznawanie prowadzone w celach wrogich, ale dla swoistego sprawdzania kondycji kooperanta, jako formy prewencji na wypadek pojawienia się zagrożeń, w rodzaju jego niewypłacalności.

---

[15] *Ibidem*, s. 235.

[16] Szerzej: K. Turaliński, *Wywiad Gospodarczy i Polityczny. Metodyka, taktyka i źródła pozyskiwania informacji*, Radom 2011, s. 47–53.

Podstawowe źródła i metody pozyskania informacji

Przegląd metod stosowanych w „czarnym" wywiadzie gospodarczym rozpoczniemy od uwagi, że do uzyskania informacji niezbędna jest osoba, która w sposób kapturowy odegra rolę intruza w rozpoznawanym obiekcie. Dla uproszczenia przyjmijmy, że postać intruza jest tożsama z postacią agenta; teoretycznie wydaje się to dopuszczalne, chociaż w praktyce role te często są realizowane przez różne osoby stosunku do podmiotu, będącego celem ataku. Intruz może być zewnętrzny lub wewnętrzny[17].

Intruz zewnętrzny jest specjalistą realizującym zlecenie lub werbuje inną osobę (np. włamywacza, hackera do wynajęcia), która wykona zadanie, samodzielnie albo wspólnie z intruzem. W takich przypadkach chodzi zazwyczaj o profesjonalistów.

W wielu przypadkach korzystne jest jednak pozyskanie intruza wewnętrznego. Nadaje się do tego celu osoba spełniająca dwa warunki: posiadanie naturalnego dostępu do interesujących zleceniodawcę informacji oraz motywacja do udostępnienia ich intruzowi. Pomijając kwestię możliwego wykorzystania kogoś do uzyskania informacji bez świadomości, że ktoś taki łamie lojalność wobec pracodawcy widać, że pierwszym celem intruza jest wytypowanie osoby, która mogłaby stać się celem swoistego werbunku, czyli spełniającej warunek pierwszy. Stworzenie motywacji należy do organizatora przedsięwzięcia.

Znane są kategorie osób szczególnie podatnych na wyrażenie gotowości do działania przeciwko pracodawcy. Należą do nich:

- pracownicy mający kłopoty materialne, szczególnie tacy, którzy swoje problemy ukrywają przed otoczeniem (co jest możliwe ze względu na genezę owych kłopotów, szczególnie gdy chodzi o lekkomyślny styl życia, uzależnienie od hazardu, alkoholu itp.),
- osoby mające w biografii epizody, czyniące z nich potencjalne ofiary szantażu czy innych form nacisku; powzięcie przez intruza wiedzy o takich zdarzeniach bardzo sprzyja jego misji. Jednocześnie nie wolno zapominać, że w zakresie standardowych poniekąd umiejętności profesjonalisty leży sprawność, polegająca na stworzeniu okoliczności, których następstwem będzie możliwość wywarcia nacisku (łącznie z szantażem) na atakowaną osobę,
- osoby znajdujące się pod wpływem skrajnych ideologii, np. politycznych, subkulturowych, ekologicznych, religijnych; takie zjawiska świetnie nadają się do wykorzystania przez bezwzględnego manipulatora,
- niezadowoleni pracownicy, szczególnie osoby doznające poczucia krzywdy ze strony pracodawcy, obciążeni nienawiścią i/lub żądzą zemsty[18].

Najgroźniejsza jest ta ostatnia kategoria.

Według amerykańskich badań, podstawowym czynnikiem, który doprowadzał do skuteczności werbunku ze strony służb obcych osób zatrudnionych w agendach rządowych USA była osobista satysfakcja z wykonywanej pracy; względy finansowe ulokowały się dopiero na kolejnym miejscu, po wpływie sytuacji rodzinnej i otoczenia towarzyskiego pracowników – niemal połowa Amerykanów, którzy zgodzili się na

[17] D.L. Pipkin, *op. cit.,* s. 223 i n.

[18] Por. J. Konieczny, *op. cit.,* s. 164–165; I. Winkler, *op. cit.*

szpiegowanie przeciwko swemu krajowi, nie dostała w zamian ani centa. Okazało się przy tym, że wpływ na poziom satysfakcji osobistej w administracji jest niespecyficzny w stosunku do innych organizacji zhierarchizowanych i w gruncie rzeczy obserwowane tam zachowania są analogiczne do zachowań osób zatrudnionych gdzie indziej[19].

Trzeba pamiętać przy tym, że w ogóle działania pracowników na niekorzyść pracodawców są zjawiskiem powszechnym. Według dostępnych (i zapewne zaniżonych) statystyk, odpowiedzialność pracowników własnych za szkody przedsiębiorstwa, spowodowane działaniami przestępczymi, realizowanymi samodzielnie lub we współpracy z osobami z zewnątrz, sięgają 80% tego typu strat. Jakkolwiek zatem brzmiałoby to paradoksalnie, największym zagrożeniem dla przedsiębiorstwa jest jego pracownik – działający sam lub w zmowie z intruzem zewnętrznym. Pozyskanie pracownika, szczególnie niezadowolonego, do sprzedaży informacji objętych tajemnicą przedsiębiorstwa (czyli ustanowienie „kreta") nie jest więc zadaniem szczególnie trudnym, zwłaszcza dla kogoś, kto wie, jak zabrać się do rzeczy.

Jak wspomniano, możliwe jest również wykorzystanie osoby do uzyskania informacji bez świadomości, że została ona wykorzystana do celów niezgodnych z interesami pracodawcy. Metody te ogólnie określane są (raczej eufemistycznie) metodami inżynierii społecznej; w istocie polegają one na stosowaniu podstępu. Wykorzystywane są naturalne skłonności natury ludzkiej: do udzielania pomocy, uczynności, gotowości do kooperacji, do dobrego wykonywania obowiązków, czasem też do ofiarności. Zawsze polegają one na podbudowanym znajomością podstaw psychologii zastosowaniu kłamstwa i manipulacji[20].

Tego rodzaju wykorzystujące cechy osobowe ofiar intruza, sposoby ataku na rozpoznawany obiekt nazywają się wtargnięciami społecznymi. Ponadto wyróżnić można wtargnięcia fizyczne i wtargnięcia techniczne[21].

Te pierwsze polegają na osobistym pojawieniu się intruza w atakowanym obiekcie, gdzie może on realizować (lub współrealizować) wtargnięcie społeczne albo zastosować inne formy działania. Typowym i zapewne najczęściej stosowanym jest kradzież nośnika informacji, w tym celu intruz niejednokrotnie posługuje się wynajętymi specjalistami, np. włamywaczami lub sam kreuje sytuację dogodną do dokonania kradzieży. Lista możliwości działania jest praktycznie nieograniczona i zależy od pomysłowości intruza, wymienić należy wywoływanie zdarzeń nadzwyczajnych (np. zorganizowanie fałszywego alarmu bombowego i wykorzystanie powstałego zamieszania do penetracji obiektu), a także znaną „od zawsze" bardzo pożyteczną sztuczkę, polegającą na badaniu śmieci, oraz wiele innych[22].

Wtargnięcie techniczne polega na wykorzystaniu metod inwazyjnych bez (zasadniczo) angażowania personelu atakowanego obiektu. W grę wchodzą przede wszystkim metody hakerskie, gdy poszukiwana informacja znajduje się w zasobie informatycznym atakowanego podmiotu (pozbawionego skrupułów hakera można wynająć i na ogół nie ma z tym problemu), do wykorzystania też pozostaje szeroka gama

[19] M. Varouhakis, *An Institution-Level Theoretical Approach for Counterintelligence*, „International Journal of Intelligence and Counter Intelligence" 2011, t. 24, nr 3.

[20] Szerzej: K.D. Mitnick, W.L. Simon, *Sztuka infiltracji*, Warszawa 2006.

[21] D.L. Pipkin, *op. cit.*, s. 220.

[22] K. Turaliński, *op. cit.*, s. 295 i n.

środków technicznych, umożliwiających podsłuch i podgląd pomieszczeń – są one dostępne w otwartym handlu, niedrogie i gwarantujące skuteczność, pod warunkiem ich prawidłowego zastosowania. Problemem może być wykorzystanie tzw. ulotu elektromagnetycznego, czyli rejestracji emisji promieniowania generowanego np. przez komputery, a będącego wartościowym nośnikiem informacji. Prywatny intruz raczej nie zdobędzie pieniędzy na zakup stosownej aparatury, ale można się domyślać, że dla państwowej organizacji wywiadowczej sprawa jest raczej niekłopotliwa.

Widać wyraźnie, że możliwe są kombinacje typów wtargnięć i przytoczony podział ma charakter porządkujący i pomocniczy. Można bowiem np. prowadzić pozorne negocjacje (handlowe, o współpracy) z rozpoznawaną firmą, jednocześnie okradając jej zasoby, podsłuchując jej personel i angażując w jej wnętrzu niezadowolonego „kreta", korumpując lub szantażując innych.

Podsumowanie

„Czarny" wywiad, uzasadniany moralnością Kalego, może więc być prowadzony przeciwko organizacji gospodarczej przez szerokie spektrum podmiotów: od firm zaprzyjaźnionych, poprzez konkurencyjne (to najczęściej), aż po państwowe agencje wywiadowcze. W tym ostatnim przypadku gospodarczy aspekt rozpoznania staje się drugorzędny; wprawdzie konkretnym celem ataku są informacje, np. technologiczne, ale jeśli technologia ta może mieć zastosowanie militarne (lub również militarne – chodzi o tzw. technologie podwójnego zastosowania), wtedy motywy podejmowanych operacji wiążą się z celami wojskowymi, a w rezultacie politycznymi, bo dotyczącymi bezpieczeństwa państwa – dysponenta agencji wywiadowczej. Trzeba też pamiętać, że państwa mniej rozwinięte zapewne zawsze zainteresowane będą wzmacnianiem swoich gospodarek również metodami nielegalnymi, a dotyczyć to może szczególnie takich segmentów jak przemysł farmaceutyczny, informatyka, łączność, komunikacja, transport i szereg innych. Wskazuje to na ostateczny brak specyfiki „czarnego" wywiadu gospodarczego wobec innych typów wywiadu.

Także metody omawianego tu procederu są niespecyficzne w stosunku do metod wywiadu „czarnego", prowadzonego w dziedzinach niegospodarczych, czyli, mówiąc w największym, ale trafnym (i niekoniecznie rozłącznym) skrócie – manipulacja, korupcja, kradzież i szantaż.

Wniosek o braku podmiotowej i metodycznej specyfiki „czarnego" wywiadu gospodarczego wydaje si ważny, bo (1) nie był on, jak dotychczas, formułowany w literaturze przedmiotu i (2) spostrzeżenie to rzutuje wprost na strategię i taktykę ochrony informacji własnych, wskazując na uniwersalną aktualność metod kontrwywiadowczych (oczywiście dostosowanych do warunków organizacji gospodarczej[23].

Nie wiemy i nigdy nie będziemy wiedzieli, jaka jest faktyczna skala szpiegostwa gospodarczego ani lokalnie (np. w kraju), ani tym bardziej globalnie. Można powiedzieć tak: prowadzenie biznesu wymaga zaufania, gospodarka – lepiej czy gorzej,

[23] Zob. M. Rozwadowski, *Ochrona strategicznych informacji w przedsiębiorstwie z wykorzystaniem kontrwywiadu gospodarczego*, [w:] *Wywiad i kontrwywiad gospodarczy wobec wyzwań bezpieczeństwa biznesu*, red. J. Kaczmarek, M. Kwieciński, Toruń 2010, s. 273 i n.

ale funkcjonuje, żaden kryzys gospodarczy nie został spowodowany działalnością szpiegowską. Może więc ogólne zagrożenie wywołane tym zjawiskiem nie jest aż tak wielkie? Afery szpiegowskie zdarzały się, zdarzają i będą się zdarzać, z dramatycznymi nieraz konsekwencjami dla atakowanego podmiotu, jednak mieszczą się one w skali jednostkowej. I tak zapewne pozostanie, o ile nie sprawdzi się prognoza Alvina Toffflera: „Dwudziesty pierwszy wiek będzie naznaczony wojną informacyjną oraz wzrostem ekonomicznego i finansowego szpiegostwa. Wszystkie rodzaje wiedzy staną się strategicznymi zasobami w walce o dominację i siłę. Wyścig po informację wszelkiego typu będzie motywowany nie tylko chęcią przewodzenia, ale także podyktowany obawami przed pozostaniem na uboczu. Informacja będzie siłą napędową w dwudziestym pierwszym wieku”[24].

Czy Toffler ma rację – pokaże przyszłość. Ale przynajmniej reguły gry są znane.

[24] Cyt. za: H. Nasheri, *op. cit.*, s. 38.