BEZPIECZEŃSTWO • 2015 nr 4 TEORIA I PRAKTYKA

Krzysztof Passella*, Mirosław Kwieciński**

Kontrwywiad gospodarczy w przedsiębiorstwie – od strategii działania do pracy operacyjnej z personelem

Wprowadzenie

Problematyka osłony kontrwywiadowczej zajmuje nadal mało miejsca w literaturze dotyczącej zarządzania przedsiębiorstwami. W większości, traktując o teoretycznych i praktycznych podejściach budowania oraz utrzymywania przewagi konkurencyjnej, autorzy poświęcają wiele miejsca opisowi metod i sposobów ekspansji na rynku. Zapominają przy tym o podejmowaniu koniecznych działań w imię ochrony działań ekspansywnych. Tymczasem bezpieczeństwo prowadzonego biznesu stało się już częścią koncepcji biznesowej.

Autorzy artykułu w dwóch częściach: teoretycznej i praktycznej prezentują znaczenie kontrwywiadu gospodarczego w organizacji działań przedsiębiorstwa, dbając przede wszystkim o wymiar praktyczny w opisie podejmowanych działań.

Część teoretyczna

Strategiczne podejście do funkcjonowania kontrwywiadu gospodarczego w otoczeniu przedsiębiorstwa

Agresywne otoczenie biznesowe, fiskalne i polityczne wymusza na przedsiębiorstwach o odpowiednio dużej skali inwestowanie w struktury i wiedzę kontrwywiadowczą oraz kontrszpiegowską. Wywiad gospodarczy i szpiegostwo przemysłowe,

* Magister inżynier, doktorant Uniwersytetu Ekonomicznego w Krakowie, Wydział Finansów.
** Profesor nadzwyczajny doktor habilitowany, Krakowska Akademia im. Andrzeja Frycza Modrzewskiego, Wydział Zarządzania i Komunikacji Społecznej.

korporacyjne, ekonomiczne to codzienność współczesnego biznesu, tak lokalnego, jak i globalnego[1]. Wywiad gospodarczy pozwala lepiej zrozumieć zarówno wewnętrzne, jak i zewnętrzne otoczenie firmy i jego uwarunkowania, a jego głównym celem jest dotarcie do prawdy („tylko prawda jest ciekawa, kłamstwo jest zawsze płytkie").

Atak wywiadowczy, szkodliwe oddziaływanie konkurencji i infiltracja firmy przez środowiska przestępcze mogą wynikać z braku celowych i zaplanowanych w kilkuletniej skali wydatków na ochronę informacyjną przedsiębiorstwa. Zaniechanie finansowania bezpieczeństwa informacyjnego firmy przekłada się na ryzyko utraty przez nią wartości chronionych, m.in.: wiedzy będącej wytworem własnych prac, pozycji rynkowej w branży, związków kooperacyjnych, kluczowego personelu, źródeł zewnętrznego finansowania, akcjonariatu czy udziałowców, wypracowanych przewag technologicznych, strategicznych inwestorów, marki i reputacji oraz wielu innych kluczowych czynników sukcesu.

Część zagrożeń pojawia się jako skutek procesów makroekonomicznych, niezależnych od przedsiębiorcy, ale wiele z nich jest jednak wynikiem zorganizowanych działań konkurencji, środowisk przestępczych, organów władzy krajowej, zagranicznych ośrodków władzy politycznej i gospodarczej, korporacji transnarodowych, nieuczciwych dostawców i odbiorców oraz przestępstw i nielojalności personelu[2] (pracowników, zarządzających, a nawet współwłaścicieli).

Kluczowa jest praca wewnątrz firmy, polegająca na kształtowaniu właściwych postaw pracowników (rozpoznawanie symptomów nielojalności), wykrywaniu nieformalnych powiązań zewnętrznych, braku dbałości o zasoby informacyjne i majątek firmy, analizie narastających konfliktów, skrywanego niezadowolenia, ustaleniu odpowiednio wcześnie osób z zaburzeniami społecznymi, nasłanych *defektorów*[3], i innych niewłaściwych czynników relacji pracownik – pracodawca. Kluczowe staje się zrozumienie relacji pomiędzy oczekiwaniami pracownika a miejscem zdobywania przez niego środków do życia i własnego rozwoju, jakim jest organizacja gospodarcza.

Najczęstsze zagrożenia wewnętrzne i zewnętrzne dla organizacji biznesowej, stanowiące podstawę do projektowania struktury i działań kontrwywiadu w nowoczesnym, innowacyjnym przedsiębiorstwie[4]:

- sprzeniewierzenie aktywów,
- celowe działanie na szkodę firmy, m.in. w kooperacji z konkurencją,
- szpiegostwo przemysłowe, w tym przy wykorzystaniu cyberprzestępczości,
- naruszenie (zabór) wartości intelektualnych,

---

1 S. Porteous, *Economic espionage, part I & II*, Canadian Security Intelligence Service, Ottawa 1993, http://www.csis-scrs.gc.ca.

2 Zob. przykładowe opracowania i raporty: *Report to the nations on occupational fraud and abuse: 2014 global fraud study*, Association of Certified Fraud Examiners, Austin 2014 oraz R. Nogacki, M. Ciecierski, *Oszustwa i nadużycia pracownicze plagą współczesnego biznesu*, Profesjonalny Wywiad Gospodarczy Skarbiec Sp. z o.o., Warszawa, http://www.centrum.vismagna.pl.

3 Inaczej pracowników lub współpracowników przedsiębiorstwa, którzy wykonując swoje obowiązki na rzecz macierzystej firmy, przekazują informacje stanowiące tajemnicę przedsiębiorstwa, działając na jego szkodę.

4 Opracowanie własne na podstawie M. Ciecierski, *Szpiegostwo korporacyjne. Jeden mit, wiele prawd*, Profesjonalny Wywiad Gospodarczy Skarbiec Sp. z o.o., s. 3, Warszawa, http://www.centrum.vismagna.pl.

- manipulacje i oszustwa księgowe na szkodę lub z zyskiem dla właścicieli czy grup interesu,
- oszustwa i nadużycia podatkowe,
- czyny nieuczciwej konkurencji[5],
- wspieranie działalności przestępczej, w tym w szczególności prania brudnych pieniędzy,
- finansowanie terroryzmu i ekstremizmu,
- korupcja organów władzy wykonawczej, ustawodawczej i sądowniczej,
- *insider trading*,
- mobbing i molestowanie seksualne,
- kradzieże, wymuszenia, zastraszanie, porwania dla okupu, przekupstwo, szantaż,
- nepotyzm.

Budowa kontrwywiadu i kontrszpiegostwa gospodarczego

Podstawowym warunkiem skutecznego wdrożenia w strukturze przedsiębiorstwa komórki kontrwywiadowczej jest właściwa postawa moralna samych zarządzających i właścicieli firmy, w codziennej pracy i życiu prywatnym, a nie deklaracje składane w przyjętych strategiach biznesu, regulaminach i kodeksach etycznego postępowania, podczas uroczystości i konferencji. Dopiero po spełnieniu powyższego warunku można budować służby ochrony informacyjnej przedsiębiorstwa, czyli kontrwywiad gospodarczy. Jest to długi proces (minimum od dwóch do nawet pięciu lat) intensywnych nakładów finansowych, prac organizacyjnych, budowania i szkolenia zespołu wywiadowczego i kontrwywiadowczego[6].

Jeżeli pracodawcy stosują nieetyczne zachowania, np.:

- mobbing wobec wybranych osób i grup w przedsiębiorstwie,
- ciągłe zastraszanie utratą pracy, niejasną i niestabilną przyszłością w firmie,
- brak powszechnie obowiązujących w firmie reguł wypłaty dodatkowych wynagrodzeń,
- wywyższanie się nad pracownikami swoim statusem majątkowym, koneksjami, wpływami w lokalnym aparacie władzy,
- stosowanie w celu podniesienia rentowności wyłącznie nacisku psychicznego na zwiększenie zaangażowania pracowników, połączonego z wulgarnym zachowaniem,
- gdy normą stają się niskie zarobki, zmuszanie pracowników do zakładania własnych, jednoosobowym firm, wykorzystywanych następnie jako podwykonawcy, wyłącznie w celu obniżenia kosztów pracy (składek na ubezpieczenia społeczne) i odebrania pracownikom świadczeń urlopowych,
- organizowanie działań szpiegowskich w konkurencyjnych firmach,
- wykorzystywanie przez menedżerów, zarząd i właścicieli majątku firmy do celów prywatnych,

to wcześniej czy później staną się łatwym celem dla wywiadu gospodarczego konkurencji (legalnego) i szpiegostwa przemysłowego (nielegalnego) wspartego ruchami wewnętrznymi, odwetowymi pracowników, nieidentyfikujących się z firmą.

---

[5] Stypizowane w Ustawie z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji, Dz.U. z 1993 r., Nr 47, poz. 2011.

[6] M. Kwieciński, K. Passella, *Implementation of the business counterintelligence branch in enterprise structure*, [w:] *The economic security of business transactions, management in business*, red. K. Raczkowski, F. Schneider, Oxford 2013, s. 178.

Czym nie powinien być kontrwywiad przedsiębiorstwa

Potoczne rozumienie pojęcia kontrwywiadu gospodarczego może spowodować szereg niejasności. Zdecydowanie łatwiej jest przedstawić, czym z pewnością nie jest kontrwywiad w przedsiębiorstwie i na tej postawie na zasadzie dopełnienia spróbować zdefiniować jego cele i zadania, które jednak dla każdej traktowanej z osobna firmy lub korporacji mogą się znacząco różnić.

Kontrwywiadem gospodarczym:

- Nie są działania niejawne państwowych służb specjalnych dopuszczone prawem wobec przedsiębiorstw i osób fizycznych w nich zatrudnionych,
- Kontrwywiad gospodarczy to nie „prywatna służba specjalna" właściciela czy zarządu firmy. Jest to tylko wewnętrzna jednostka organizacyjna o zadaniach informacyjnych, analitycznych i kontrolnych,
- Komórki kontrwywiadowcze przedsiębiorstw nie mogą stosować metod sprzecznych z prawem i czynności operacyjno-rozpoznawczych przynależnych centralnym organom i urzędom administracji rządowej,
- Kontrwywiad gospodarczy firm nie jest częścią działań służb państwowych zwalczających operacje obcych służb specjalnych, choć może w niektórych zakresach współdziałać w sposób jawny lub z reguły niejawny z krajową władzą bezpieczeństwa, miedzy innymi z: agencjami wywiadu i kontrwywiadu cywilnego, jak i wojskowego (AW, ABW, SWW i SKW) oraz Centralnym Biurem Antykorupcyjnym, co regulują ustawy powołujące do życia poszczególne służby specjalne RP[7],
- Komórki kontrwywiadu przedsiębiorstw powinny współpracować z organami kontroli skarbowej, celnej, wywiadem skarbowym[8], wywiadem finansowym[9], Strażą Graniczną, Służbą Celną i Policją w zakresie ujawnia przestępstw, ale równocześnie są to dla nich przeciwnicy w walce informacyjnej, pomiędzy rozrastającą się kontrolą państwa a przynależnymi jednostce swobodami obywatelskimi do prowadzenia działalności gospodarczej,
- Nie są metody służące do restrukturyzacji firmy, sprowadzające kontrwywiad do roli narzędzia pomocnego przy redukcji personelu, poprzez poszukiwanie rzekomych dowodów na nielojalność pracowników, których stanowiska przewidziano wcześniej do likwidacji,
- Nie są metody mobbingowania pracowników prowadzące do usuwania z przedsiębiorstwa osób niewygodnych dla zarządzających firmą i innych grup interesów,
- Nie są działania mające na celu inwigilacje prywatnego życia pracowników i kooperantów, dające właścicielom i zarządzającym przewagę informacyjną nad podległym personelem,
- Nie jest to narzędzie w rękach osób odpowiedzialnych za rekrutację pracowników, służące do „złamania kandydata" i wydobycia informacji, do jakich przyszły pracodawca nie ma prawa dostępu i ich gromadzenia,

---

[7] Ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz.U. z 2002 r., Nr 74, poz. 676 z późn. zm.; Ustawa z 9.06.2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, Dz.U. z 2006 r., Nr 104, poz. 709, późn. zm. oraz Ustawa z 9.06.2006 r. o Centralnym Biurze Antykorupcyjnym, Dz.U. z 2006 r., Nr 104, z późn. zm.

[8] Departament Wywiadu Skarbowego Ministerstwa Finansów.

[9] Departament Informacji Finansowej Ministerstwa Finansów.

- Nie jest to narzędzie służce do ukrywania czynów niezgodnych z prawem w przedsiębiorstwie, poprzez stosowanie dezinformacji i maskowania niewygodnych faktów oraz niszczenia dowodów przestępstw,
- Kontrwywiad w firmach nie inspiruje personelu do działań sprzecznych z prawem wobec konkurencji i własnych pracowników, z których strony stwierdzono prowadzenie wywiadu gospodarczego czy nawet szpiegostwa,
- Kontrwywiad gospodarczy, to nie jedyna struktura, metoda czy środek służący do zidentyfikowania wewnątrz przedsiębiorstwa działalności wywiadowczej, szpiegostwa i wykrycie przestępstw. Są nimi w równym stopniu systematyczne i doraźne kontrole, audyt wewnętrzny i zewnętrzny, monitoring techniczny i nadzór informatyczny, samorzutne zawiadomienia kierowane do organów ścigania i organów kontroli skarbowej o popełnionych czynach przestępczych przez własnych pracowników lub osoby z otoczenia firmy, wykrycie przez przypadek malwersacji, np. podczas kontroli dokumentacji projektu, czy porównania dowodów księgowych i zapisów na kontach do wyciągów bankowych, a nawet dobrowolne przyznanie się sprawcy do popełnionego przestępstwa lub wykroczenia.

Podsumowując, kontrwywiad gospodarczy przedsiębiorstwa nie jest działalnością niejawną, sprzeczną z prawem, ale nie oznacza to, że metody, zebrane informacje i dowody rzeczowe oraz sporządzane analizy bezpieczeństwa są powszechnie dostępne w firmie czy są obowiązkowo udostępniane organom władzy wykonawczej i opinii publicznej oraz konkurencji.

Kontrwywiad gospodarczy a inwestycje w aktywa firmy

Jeżeli przyjmiemy, że właściwie funkcjonujący w przedsiębiorstwie kontrwywiad gospodarczy powstał w wyniku własnych prac organizacyjnych, to można go uznać, na gruncie rachunkowości zarządczej, za pojęciowo zbliżony do *know how* firmy. Jednakże w rachunkowości finansowej *know how* to składnik aktywów – majątku trwałego, ściślej wartości niematerialnych i prawny (WNiP), który został zakupiony, otrzymany nieodpłatnie lub wniesiony aportem. Jeśli struktury i metody kontrwywiadu powstały własnych nakładem prac przedsiębiorstwa, wówczas zapewne nie jest to *know how* firmy, choć ekonomiczna użyteczność informacji kontrwywiadu gospodarczego jest niewątpliwie dłuższa niż jeden rok i jego działania przynoszą korzyści ekonomiczne przedsiębiorstwu, ograniczając koszty, w tym ryzyko powstania strat nadzwyczajnych.

Tak samo kontrwywiad nie jest składnikiem wartości firmy – *goodwill* (WNiP), albowiem ta, zgodnie z Ustawą o rachunkowości, pochodzi z transakcji nabycia innej jednostki lub zorganizowanej jej części[10].

Profesjonalny kontrwywiad gospodarczy w obszarach ryzyka przedsiębiorstwa

„Wszystko co ukryte zostanie w końcu pokazane, wszystko co zostało powiedziane zostanie ujawnione". Ta opinia odnosi się również do działań kontrwywiadu gospodarczego. **Cel strategiczny kontrwywiadu**: niedopuszczenie do wycieku z firmy

[10] Art. 33 ust. 4 Ustawy z 29.09.1994 r. o rachunkowości, Dz.U. z 1994 r., nr 121, poz. 591 z późn. zm.

informacji stanowiących tajemnicę firmy lub informacji niejawnych, mogących zagrozić pozycji rynkowej przedsiębiorstwa.

Cel operacyjny kontrwywiadu rozumiany w sposób prosty: rozpoznawanie i zbieranie dowodów na nielojalność i przestępstwa popełniane przez pracowników, osoby zarządzające i właścicieli firmy oraz kooperantów działających na szkodę organizacji.

Oparcie się tylko na powyższym celu operacyjnym, bez przestrzegania nadrzędności celu strategicznego, sprowadzi się tylko do ratowania sytuacji po porażce służb bezpieczeństwa informacyjnego i organów zarządzających firmą, które dopuściły do wycieku informacji wrażliwych. Nie potrafiły przewidzieć zagrożeń wewnętrznych i zewnętrznych dla integralności informacyjnej organizacji i podjąć zawczasu czynności chroniących własne zasoby firmy, poprzez neutralizację osób lub grup prowadzących wywiad gospodarczy lub działalność przestępczą, w tym szpiegostwo gospodarcze.

Na czym polega kontrwywiad gospodarczy w firmie?

Jest to pewna wyspecjalizowana i mająca szeroką autonomię wewnętrzna struktura informacyjno-analityczno-kontrolna przedsiębiorstwa, ale też system działań, spełniając zadania przewidywania, wczesnego wykrywania i neutralizacji zagrożeń dla bezpieczeństwa informacyjnego, pochodzących ze świata zewnętrznego firmy[11] i od strony wewnętrznych, destrukcyjnych działań w samej firmie. Jest to więc zorganizowany i dobrze przygotowany oraz wyposażony zespół ludzki, który:

- ostrzega i spełnia funkcję bufora, wyławia i chroni informacje wrażliwe, stanowiące unikatową wartość dla firmy,
- zwalcza metodami dopuszczonymi prawem wszelką działalność wywiadowczą, szpiegowską i przestępczą wobec organizacji,
- potrafi wypracować hipotezy, znaleźć metody poprawy i dokonać wdrożenia, odnośnie do eliminacji słabych punktów obrony przedsiębiorstwa,
- identyfikuje i skutecznie odseparowuje potencjalnych sprawców przejęcia informacji, procedur, praktyk istotnych dla przetrwania i rozwoju firmy na konkurencyjnym rynku,
- potrafi wypracować metody oceny ryzyka i przeprowadzić analizę sytuacji.

Kontrwywiad powinien mieć zdolność zrozumienia i uchwycenia w otoczeniu firmy i jej wewnętrznych strukturach poczynań wywiadu konkurencyjnego i działalności przestępczej, czyli identyfikować ludzi, którzy pragną pozyskać legalnie i nielegalnie informacje[12] gospodarcze ochranianej firmy.

Można nawet postawić tu tezę, iż kontrwywiad gospodarczy to wewnętrzna ucząca się struktura czy mikroorganizacja, doskonaląca metody skutecznego przeciwdziałania próbom naruszenia integralności i bezpieczeństwa informacyjnego firmy.

---

[11] M.in. wywiad konkurencyjny, wywiad polityczny i ekonomiczny, różnorodna przestępczość, w tym szpiegostwo przemysłowe.

[12] Na potrzeby niniejszej pracy pojęcia dana i informacja będą stosowane zamiennie.

Część praktyczna

Różnica między kontrwywiadem a kontrszpiegostwem gospodarczym leży w umiejętności rozróżnienia, w jaki sposób firma jest analizowana przez pracowników lub kontraktorów konkurencyjnego wywiadu gospodarczego, a jakie podejście obowiązuje w działaniach inicjowanych przez świat przestępczy czy przez służby specjalne obcych państw. Jest to także dla zarządzających i właścicieli firmy konieczność wypracowania odpowiedzi na pytanie o rolę profesjonalnego kontrwywiadu gospodarczego w obszarach ryzyka przedsiębiorstwa.

Wykrywanie działań przeciwko firmie na podstawie pracy ze źródłami osobowymi

Obszarem generującym najszerszy obszar ryzyka był, jest i będzie czynnik ludzki, którego wpływ na bezpieczeństwo informacyjne firmy został omówiony w części pierwszej artykułu. Autorzy postawili sobie za cel przedstawianie zagadnień dotyczących bezpieczeństwa również w sposób praktyczny, użyteczny dla kadry menedżerskiej. Szczególnie ważne jest wykrywanie nielojalności pracowników oraz aktów dezintegrujących i przestępczych generowanych w przedsiębiorstwie.

Zachowania, które zdaniem autorów prowadzą do zwrócenia uwagi na osoby podejrzewane o działalność na szkodę firmy:

1) życie ponad stan, powodujące konieczność szybkiego uzupełniania zasobów finansowych,
2) znaczące pogorszenie dyscypliny pracy,
3) niedające się szybko rozwiązać trudności finansowe,
4) zbyt bliskie relacje z klientami/dostawcami/kooperantami,
5) ciągły opór przed kontrolami,
6) niechęć do dzielenia się obowiązkami,
7) wymaganie nadmiernej autonomiczności,
8) problemy rodzinne i zdrowotne, stosowanie przemocy, rozwody, osamotnienie,
9) zachowania kombinatorskie wyniesione z poprzednich miejsc pracy i na skutek nieodpowiedniego wychowania w domu,
10) chęć zemsty za wyolbrzymione krzywdy w pracy,
11) drażliwość, podejrzliwość, postawa obronna,
12) problemy z uzależnieniami,
13) narzekanie na wynagrodzenie i budowanie wśród współpracowników atmosfery wrogości do zarządzających firmą,
14) tworzenie wewnątrz organizacji koterii, działającej na zasadzie „my i oni",
15) ujawniona negatywna historia z poprzednich miejsc prac i jej wpływ na bieżące zatrudnienie i życie prywatne (długi z przekroczonym terminem spłaty, zła opinia zawodowa i prywatna – środowiskowa, konflikty, sprawy dyscyplinarne, kradzieże, korupcja, niewypłacone wynagrodzenia dochodzone na drodze sądowej).

Ostatni z powyższej wymienionych czynników zwykle jest spowodowany zaniedbaniami, które powstają już na etapie rekrutacji i selekcji, gdy nie przykłada się znaczenia do chociażby dokładnego sprawdzenia informacji podawanych przez

kandydata w CV i liście motywacyjnym[13]. Nie prowadzi się weryfikacji listów referencyjnych i świadectw pracy oraz poświadczeń o ukończonych kursach i szkoleniach. Czasami jedyną możliwością ustalenia intencji kandydata jest przeprowadzenie za jego zgodą badań poligraficznych przez specjalistów. Są to istotne czynności w takich newralgicznych obszarach działalności gospodarczej jak: bankowość, przemysł obronny, usługi na rzecz bezpieczeństwa publicznego, miejsca, gdzie są gromadzone i przetwarzane informacje niejawne oraz występuje narażenie na próby infiltracji przez obce służby specjalne, świat zorganizowanej przestępczości i korporacje transnarodowe.

Należy wyodrębnić miejsca ryzyka w strukturze zarządzania firmą, szczególnie podatne na ataki wywiadowcze i próby pozyskiwania personelu do tajnej współpracy na szkodę firmy, takie jak: wyższe szczeble zarządzania, działy informatyczne (IT), sprzedaż i zaopatrzenie, księgowość, obsługa posprzedażowa klienta, wydziały badawczo-rozwojowe (R&D), ochrona i utrzymanie obiektów.

Potocznie mówi się o molach lub kretach[14] – czyli o osobach umieszczonych w rozpracowywanej organizacji, które za pieniądze lub inne korzyści majątkowe lub zawodowe, przekazują konkurencji lub służbom specjalnym obcego kraju informacje stanowiące tajemnice przedsiębiorstwa, informacje niejawne czy też inne wrażliwie dane mogące zachwiać pozycją rynkową firmy, zdyskredytować markę, obniżyć skuteczność prowadzonych akcji marketingowych czy przekreślić celowość prowadzenia innowacyjnych badań.

Nielojalny pracownik firmy może zostać także agentem dezinformacji lub co jest bardzo wyrafinowanym sposobem szkodzenia – agentem wpływu, ukierunkowując swoim działaniami politykę inwestycyjną, sprzedażową, badawczo-rozwojową a nawet politykę zatrudnienia, na pozycje korzystne wyłącznie z punktu widzenia konkurencji, czy zagranicznych instytucji rządowych.

Przeglądając poradniki dotyczące bezpieczeństwa biznesu, szczególnie wydawane przez instytucje kontrwywiadowcze podległe Dyrektorowi Zarządzającemu Narodowym Kompleksem Wywiadowczym USA[15] lub prywatne firmy konsultingowe, można ułożyć listę zachowań wskazujących na obecność kreta w firmie:

- przesyłanie niejawnych danych, korespondencji i dokumentów do osób wewnątrz firmy, które nie mają autoryzacji do korzystania z nich lub nie są w żaden sposób związane z realizowanym przedsięwzięciem i objęte procedurą obiegu tych dokumentów,
- pominięcie drogi służbowej w ubieganiu się o dostęp do informacji będących tajemnicą przedsiębiorstwa lub do informacji jawnych, ale niepublikowanych, tj. udostępnianych na zewnątrz tylko na pisemną prośbę,

---

[13] J. Konieczny, *Wprowadzenie do bezpieczeństwa biznesu*, Warszawa 2004.

[14] Termin z języka branżowego państwowych służb specjalnych; odnosi się do własnych pracowników wywiadu i kontrwywiadu, zwerbowanych do tajnej, nielegalnej współpracy na korzyść zagranicznych służb specjalnych (wywiadowczych, kontrwywiadowczych czy antykorupcyjnych).

[15] DNI (Director of National Intelligence), przykładowo: *Protecting key assets: a corporate counterintelligence guide*, National Counterintelligence and Security Center, Director of National Intelligence, Washington 2011; *Foreign spies stealing US economic secrets in cyberspace*, Report to Congress on Foreign Economic Collection and Industrial Espionage, Office of the National Counterintelligence Executive, National Counterintelligence and Security Center, Director of National Intelligence, Washington 2011.

- prośby o potwierdzenie podpisem udziału w zniszczeniu niejawnych dokumentów lub stanowiących tajemnicę przedsiębiorstwa, których to czynności nie byliśmy świadkami,
- zaobserwowane przypadki operowania przy dokumentach i ekranach komputerów aparatami fotograficznymi, kamerami, skanerami, laptopami, szczególnie w pomieszczeniach, gdzie są przechowywane niejawne lub wrażliwe informacje, tj. w sekretariatach, w biurach projektowych, centrach obliczeniowych, miejscach spotkań biznesowych i narad projektowych, pomieszczeniach drukarek sieciowych, w magazynach z dokumentacją technologiczną i księgową,
- częste wypożyczanie do pracy w domu dokumentacji bez powiadamiania przełożonych i rejestracji wynoszenia materiałów poza siedzibę firmy: dokumentów, służbowych laptopów, dysków komputerów, archiwów na różnorodnych nośnikach danych. To samo dotyczy użytkowania dokumentacji firmy podczas delegacji służbowych, konferencji, kursów oraz tzw. wyjazdów integracyjnych,
- posiadanie przez „kolegów i koleżanki" z pracy urządzeń elektronicznych niewiadomego zastosowania, a następnie słyszalne w głośnikach zakłócenia elektroakustyczne i widoczne na ekranie komputerów zakłócenia elektromagnetyczne, które mogą świadczyć o założonych urządzeniach podsłuchowych i elektronicznego przechwytu danych (razem nazywanych inwigilacją/wywiadem elektronicznym),
- przechowanie dokumentów i plików z tajemnicami przedsiębiorstwa i informacjami niejawnymi w miejscach do tego nieprzeznaczonych, tj. w biurku, ogólnodostępnej szafie, w domu, samochodzie, niekwalifikowanym komputerze służbowym, komputerze prywatnym,
- prośby o dostęp do informacji poufnych osób do nich nieuprawnionych, motywowane np. oszczędnością czasu z pominięciem formalnych procedur, koleżeńską prośbą, twierdzeniami o braku „istotności informacji w nich zawartych", a nawet sugestiami, że „opór przy ich udostępnianiu nie spodoba się kierownictwu, które bardzo liczy na przyspieszenie prac nad projektem",
- przesyłanie dokumentów chronionych poza biuro z wykorzystywaniem służbowych, ale niechronionych e-maili, faksów, telefonów komórkowych, komunikatorów, portali społecznościowych, dostępnych na zewnątrz firmy sieci komputerowych, pod pozorem wyjazdów służbowych, konferencji, pracy w domu, kontaktów z klientami i dostawcami,
- prośby o użycie służbowego komputera kolegi i telefonu komórkowego w mało istotnych sprawach, w które wypożyczający nie jest zaangażowany,
- częste korzystanie z faksu, kserokopiarki, komunikatorów i telefonów służbowych do celów prywatnych, nadużywanie użytkowania Internetu, w tym szczególnie poza godzinami służbowymi,
- prowadzenie rozmów dotyczących poufnych zagadnień przez nieszyfrowane łącza telefoniczne, komunikatory i rozmowy internetowe,
- usuwanie z dokumentów elektronicznych i papierowych oznaczeń wskazujących, że zawierają informacje niejawne lub tajemnicę przedsiębiorstwa,
- ukrywanie częstych, lecz krótkotrwałych wyjazdów zagranicznych, a po ich ujawnieniu przedstawianie różnych i niespójnych wyjaśnień.

W pracy komórek kontrwywiadu i kontrszpiegostwa gospodarczego istnieją pewne potwierdzone wieloletnią praktyką[16] bardzo pomocne wskazania na osoby, które podejrzewa się, że są zaangażowane w działalność szpiegowską, przykładowo:

- Udzielanie wyjaśnień z powodu zmiany sytuacji majątkowej, które nie mają oparcia w dotychczasowej aktywności zawodowej i sytuacji rodzinnej, w sposób zwiły: otrzymaniem nagłego wsparcie finansowego od obcej firmy z branży w zamian za wykonanie dodatkowego projektu, świadczeniem usług konsultingowych dla zagranicznych i krajowych organizacji biznesu, otrzymaniem szczególnie dochodowego stypendium zagranicznego lub krajowego, wygraną w grze hazardowej, uruchomieniem bardzo zyskownego, dodatkowego biznesu realizowanego od niedawna poza godzinami pracy, otrzymaniem pomocy finansowej od dalszej rodziny, o której podejrzana osoba nigdy nie wspominała, zwrotem pożyczki od dalszej rodziny lub pracownika obcej firmy, otrzymaniem spadku po dalekich krewnych. W konsekwencji umożliwiło to pracownikowi przykładowo:
  - zakup nowego domu, samochodu, wyposażenia, sprzętu sportowego znacznej wartości,
  - nabycie pakietu papierów wartościowych,
  - obnoszenie się z drogocennymi ozdobami,
  - spłatę długów w banku i zniesienie hipoteki,
  - nagłą spłatę prywatnych pożyczek,
  - wyjazdy na ekskluzywne wakacje z całą rodziną, dotychczas niedostępne z przyczyn finansowych,
  - wysłanie dzieci na krajowe lub zagraniczne studia na renomowane uczelnie,
  - zakończenie spraw sądowych niespodziewanymi ugodami.
- Wzmiankowane w rozmowach bez świadków znajomości w służbach specjalnych, organizacjach zajmujących się bezpieczeństwem biznesu, partiach i stowarzyszeniach politycznych,
- Częste zgłaszanie się „na ochotnika" do projektów, które wymagają dostępu do informacji niejawnych lub tajemnic przedsiębiorstwa, co nie wynika z normalnego zakresu obowiązków, wykształcenia i umiejętności pracownika,
- Bardzo częste przesyłanie informacji chronionych w firmie pomiędzy jej oddziałami, biurami, placówkami zagranicznymi, kooperantami, dostawcami za pomocą faksu, wewnętrznych sieci komputerowych (Intranetu), telefonów służbowych, komunikatorów, czego nie wymaga sytuacja pracy nad projektem,
- Ukrywanie przeszłości o charakterze przestępczym, w szczególności podejrzeń o korupcję, szpiegostwo gospodarcze, przemysłowe i ekonomiczne, kradzieże, defraudacje,
- Podawanie fałszywych informacji odnośnie pracy w poprzednich firmach, kłamstwa dotyczące powodów zmiany pracodawcy, utajnione konflikty personalne,
- Pominięcie w danych osobowych niektórych miejsc pracy, nieukończonych szkół, studiów, kursów, przynależności do organizacji gospodarczych i politycznych,

---

[16] *CORE: Counterintelligence reporting essentials: a practical guide for reporting counterintelligence and security indicators, Defense Personnel Security Research Center (PERSEREC)*, [w:] *DoD instruction no. 5240.6. Counterintelligence Awareness, Briefing, and Reporting Programs*, US Department of Defense, August 2004.

- Powtarzająca się praca poza godzinami funkcjonowania biura, szczególnie bez obecności innych osób, przy braku zlecenia na pracę w godzinach nadliczbowych oraz bez ubiegania się o dodatkowe wynagrodzenie („praca dla dobra i rozwoju firmy"),
- Uczestnictwo w imprezach, spotkaniach, kursach organizowanych przez zagraniczne placówki dyplomatyczne, konkurencyjne firmy i wspierane przez nie stowarzyszenia branżowe i kulturalne.

Identyfikacja siatki szpiegostwa przemysłowego w firmie przez kontrwywiad

Zainfekowanie firmy przez działającego w jej wewnętrzu defektora (kreta, mola) powoduje z biegiem czasu rozszerzanie jego działalności, niczym wirusa niszczącego poszczególne bariery obronne nieświadomego organizmu przedsiębiorstwa. Niemniej możliwości jednego zdrajcy szybko ulegają wyczerpaniu. Stąd pojawia się konieczność ciągłego poszerzenia źródeł, z których defektor czerpie dane, lub dla potrzymania efektów swojej działalności powinien awansować w strukturze zaatakowanej firmy i być zaangażowany w kluczowe projekty. Kontrwywiad musi się więc liczyć ze stałym zagrożeniem, polegającym na wciągnięciu do współpracy wywiadowczej czy szpiegowskiej kolejnych pracowników i kooperantów firmy.

Kret buduje swoją siatkę według schematów wypracowanych przez mocodawców z zewnątrz lub korzystając z własnej inwencji. Obiektem starań kreta może równie dobrze być kolega lub koleżanka z pracy, niezwiązana zależnościami służbowymi, a także przełożony, podwładny, kooperant-dostawca, odbiorca, współpracownik, konsultant: Trzy etapy werbunku potencjalnie nielojalnego pracownika:

- FAZA 1 – POZYSKANIE
  - szczególnie miłe traktowanie w pracy, okazywanie na każdym kroku empatii,
  - preferowanie przy premiach, nagrodach, awansach,
  - udzielanie referencji w różnych środowiskach zawodowych, społecznych i prywatnych,
  - częste wysyłanie na atrakcyjne wyjazdy służbowe,
  - udzielanie dodatkowych urlopów,
  - coraz droższe prezenty.
- FAZA 2 – UZALEŻNIENIE
  - bezzwrotne wsparcie finansowe w trudnej sytuacji życiowej,
  - angażowanie w przedsięwzięcia, gdzie wykonanie obowiązków jest zawsze zależne od wsparcia oferenta-kreta,
  - stałe wyświadczanie różnych przysług prywatnych i zawodowych,
  - częste, nieuzasadnione premiowanie pracownika z pominięciem innych osób.
- FAZA 3 – ATAK
  - żądanie natychmiastowej zwrotu prywatnej pożyczki,
  - zastraszenie cofnięciem referencji czy poparcia w zarządzie firmy,
  - posługiwanie się groźbą ujawnienia kompromitujących faktów z życia prywatnego, o których oferent dowiedział się rozbudowując relacje z osobą (obiektem ataku),
  - sugestie ujawnienia zawinionych błędów w pracy, które były zaplanowane przez werbującą osobę, a ofiara nie mogła ich uniknąć, gdy zaczęła zajmować się projektem,

- szantażowanie złożeniem doniesienia o kradzieży, korupcji, molestowaniu,
- wskazywanie na brak możliwości rozwoju dalszej kariery czy otrzymania zleceń, zamówień przy odmowie dalszej współpracy,
- groźba odcięcia od premii, awansów, przysług, atrakcyjnych wyjazdów.

Nielojalny pracownik, który do tej pory samodzielnie działał na szkodę firmy, przekazując konkurencji lub obcym służbom specjalnym[17] informacje, stara się rozbudować własne źródła informacji, tj. utworzyć sieć zależności personalnych i punktów dostępowych. Może zostać jednak ujawniony w wyniku pracy komórki kontrwywiadu czy bezpieczeństwa informacyjnego firmy, albowiem pozostawia pewne znamienne ślady. Inaczej musi poczynić dodatkowe kroki dla osiągnięcia swoich dalekosiężnych celów wywiadowczych i przestępczych. Należy zwrócić uwagę na symptomy, niejako ukryte w procesie codziennej pracy przedsiębiorstwa:

- Prośby czy wymuszanie od osoby objętej atakiem, aby od kolegów/koleżanek z firmy, przełożonych lub menedżerów z innych jednostek organizacyjnych przedsiębiorstwa pozyskała dostęp do dokumentów służbowych (tajemnic firmy, informacji niejawnych, dokumentów służbowych, analiz zewnętrznych), sugerując przy tym użycie nieformalnej drogi przekazania informacji poprzez:
  - osobisty kontakt w biurze zewnętrznej organizacji, miejscu publicznym (restauracji, pubie, podczas konferencji, targów, w markecie, pod pozorem koleżeńskiego spotkania ze znajomym menedżera/szefa),
  - użycie prywatnego e-maila, telefonu komórkowego, komunikatora internetowego,
  - transmisję danych z prywatnego komputera,
  - dostarczenie elektronicznego nośnika danych do skopiowania,
  - przesłanie faksem informacji w publicznym punkcie usług ksero lub wysłanie przez pocztę,
  - wizytę w ośrodku wypoczynkowym, zorganizowaną przez odbiorcę materiałów,
  - wspólne szkolenie krajowe, a najlepiej zagraniczne,
  - udział w studiach podyplomowych,
  - spotkanie w luźnej atmosferze podczas atrakcyjnego wyjazdu wakacyjnego dofinansowanego przez odbiorcę, „pod przykryciem" kursu, na który można też zabrać rodzinę.
- Kret posługuję się „twarzą i miejscem", z którego są dostarczane dane, przynależną do innej osoby,
- Defektor rozbudowujący siatkę szpiegostwa przemysłowego może stosować swoistą taktykę związaną z takimi działaniami:
  - pomoc koleżeńska w przygotowaniu pracy dyplomowej,
  - pomoc dla zaprzyjaźnionej firmy, z którą niedługo rodzime przedsiębiorstwo/wydział/grupa projektowa „na pewno będzie i tak współpracować",

[17] Z punktu widzenia zarządzających korporacjami transnarodowymi każda państwowa służba specjalna może być traktowana, jako zagrożenie dla poufności prowadzenia działań gospodarczych i finansowych. Dzieje się tak z uwagi na czasami występującą sprzeczność interesów pomiędzy rządem, którego celem powinna być ochrona interesów ekonomicznych państwa, realizowana przy wykorzystaniu służb wywiadowczych, kontrwywiadowczych i antykorupcyjnych, a procesami biznesowymi prowadzonymi przez korporacje transnarodowe niezależnie, gdzie mają swoją siedzibę i właściwość podatkową – teza autorów.

- przyrzeczenie premii, awansu, atrakcyjnego wyjazdu zagranicznego, poprzez użycie własnych wpływów w zarządzie lub u bezpośredniego przełożonego,
- wskazanie na wspólne działanie w grupie, która w przyszłości będzie miała duże znaczenie w firmie,
- sugerowanie, że takie działanie ma cichą aprobatę zarządu lub właścicieli firmy, którzy niebawem zmienią osoby w zarządzie,
- przyrzeczenie dodatkowego, „łatwego" do wykonania zlecenia od zewnętrznego odbiorcy dokumentów w ramach nieoficjalnej współpracy firm,
- użycie argumentów w rodzaju: „mała pomoc nic nie kosztuje, a może tylko przynieść korzyść dla nas wszystkich", „drobne gratyfikacje są nieistotne i przez nikogo niezauważalne", „przydadzą się środki na rodzinę, studia dzieci, drobne remonty w domu, wsparcie na zakup nowego samochodu", „takich kwot w ogóle nie trzeba zgłaszać do opodatkowania", „to tylko mały rewanż za przyjacielską przysługę", „wszyscy musimy sobie pomagać w tych ciężkich czasach", „warto mieć na przyszłość oddanych przyjaciół w firmie", „i tak o tym wszyscy wiedzą", „wszyscy to robią", „już tyle w tej firmie dla ciebie zrobiłem", „nikt cię oprócz mnie tu nie docenia", „twoi koledzy też to robią",
- szybkie wycofanie się z oferty, gdy obiekt ataku użyje sformułowań typu: „jednak muszę spytać o zgodę osób odpowiedzialnych", „zapytam o zdanie szefa", „sprawdzę w zarządzie twoje pełnomocnictwo w tej sprawie", „to chyba nie jest twój zakres obowiązków",
- oferowanie prywatnej pożyczki, np. nieoprocentowanej, bezterminowej, bez umowy, bez opodatkowania, na pokrycie bieżących wydatków.

Szpiegostwo przemysłowe – zagrożenia niezwiązane z cyberprzestępczością

Nowoczesne środki przesyłania danych i komunikacji elektronicznej skupiły na sobie medialne odium, w którym cyberprzestępczość jest podawana jako główna przyczyna dezintegracji informacyjnej przedsiębiorstwa. W rzeczywiści jest to tylko jeden z kanałów „ulotu informacji wrażliwej" z firmy do konkurencji i otoczenia zewnętrznego. Właściwe jest spojrzenie niebiorące pod uwagę dostępnych technologii komunikacji i przetwarzania danych, z uwzględnieniem czynnika ludzkiego oraz metod, za pomocą których profesjonaliści wywiadu gospodarczego i państwowych służb wywiadowczych, a także środowiska zorganizowanej przestępczości, mogą zdobywać osobowe źródła informacji[18]. Poniżej podajemy proste schematy postępowania, na które kontrwywiad gospodarczy powinien zwrócić szczególną uwagę[19]:

- Najprostszą formą prowadzenia wywiadu gospodarczego, ale również ekonomicznego i politycznego, jest prośba o udzielenie informacji[20] skierowana bezpośrednio od osoby czy konkurencyjnej firmy lub przy wykorzystaniu pośrednika, np. pochodzącego z kraju, instytucji, firmy, do której obiekt ataku ma zaufanie.

---

[18] Ang. *human sources*, wchodzące w skład tzw. wywiadu osobowego HUMINT – *Human Intelligence*.

[19] Por. roczne raporty *Annual report to Congress on foreign economic collection and industrial espionage, FY 1995–2008*, Office of the National Counterintelligence Executive (ONCIX), Washington oraz przekrojową publikację B. Martinet, Y.M. Marti, *Wywiad gospodarczy: pozyskiwanie i ochrona informacji*, Warszawa 1999, s. 195–261.

[20] RFI – *Request for Information*.

Prośba może z pozoru dotyczyć informacji ogólnodostępnych[21]. Natomiast kolejne zapytania o uszczegółowienie danych odnoszą się już do informacji wrażliwych, niejawnych i objętych zakazem eksportu technologii podwójnego zastosowania (cywilnego i wojskowego)[22]. Wówczas pracownik nieopatrznie przekazuje na zewnątrz firmy tajne, szczegółowe dane, będąc przekonanym, że tylko precyzuje lub wyjaśnia wątpliwości dotyczące spraw powszechnie znanych. Forma jest tutaj dowolna, zarówno komunikacja elektroniczna, jak i wypytywanie podczas częstych rozmów telefonicznych lub spotkań prywatnych i biznesowych. Obecnie ataki z wykorzystaniem źródeł i komunikacji otwartej przebiegają wielotorowo i wieloosobowo w stosunku do chronionego potencjału firmy,

- Poszukiwanie przez firmy zewnętrzne, podstawione przez konkurencje przedsiębiorstwa lub służby wywiadowcze[23], możliwości uruchomienia wspólnych projektów biznesowych tylko w celu uzyskania dojścia do tajemnic firmy i informacji niejawnych, czy też zainstalowania u konkurenta własnej agentury,
- Wykorzystanie przez wywiad gospodarczy i obce służby specjalne wszelkiego rodzaju konferencji, pokazów i szkoleń, aby tą drogą uzyskać dostęp do osób w firmie podatnych na werbunek, wykraść przenoszone na nośnikach danych i laptopach informacje biznesowe i technologiczne oraz wyłowić z prezentacji i podczas kuluarowych rozmów brakujące dane, które następnie pozwolą na całościowe opracowanie interesującego wywiad zagadnienia biznesowego czy technologicznego[24],
- Oficjalne wizyty zagranicznych ekspertów, naukowców, przedstawicieli organizacji biznesowych, uczelni wyższych i stowarzyszeń branżowych mające na celu, „pod przykryciem" uruchomienia wspólnych programów badawczych, uzyskanie nieuprawnionego dostępu do tajemnic firmy i danych objętych ochroną informacji niejawnych, które następnie zostaną przekazane konkurencji lub wywiadowi obcych państw,
- Ciche włamania i kopiowanie danych z przenośnych komputerów, telefonów komórkowych i innych nośników elektronicznych, pozostawionych podczas delegacji przez pracowników w hotelach, samochodach, w salach konferencyjnych, obiektach sportowych i wypoczynkowych wraz ze śledzeniem wytypowanych wcześniej osób i nagrywaniem ich rozmów. To samo dotyczy dokumentów w formie papierowej pozostawionych bez należytego zabezpieczenia,
- Próby uwikłania pracowników firmy w relacje seksualne, które później mogą być podstawą do werbunku na podstawie kompromitujących materiałów z wykorzystaniem szantażu. Podobny schemat obejmuje uzależnienie finansowe, przy wykorzystaniu skłonności pracownika do hazardu, życia ponad stan, nieopanowanej chęci posiadania dóbr luksusowych,
- Wykorzystanie publikacji w czasopismach naukowych lub branżowych czy w sieciach społecznościowych jako punktu zaczepienia do nawiązania najpierw niewzbudzającej podejrzeń indywidualnych konsultacji, a później do przeprowadzenie werbunku lub uczynienia z pracownika nieświadomego informatora.

---

21 OSCINT – *Open Source Intelligence*, wywiad jawnoźródłowy.

22 Powszechnie określone z j. ang. *dual-use technologies*.

23 Tzw. z j. ang. *front companies*.

24 TECHINT – *Technological Intelligence*, wywiad technologiczny (naukowy).

Podsumowanie

Osiąganie pozytywnych rezultatów przez przedsiębiorstwo na rynku wymaga skoncentrowanego wysiłku wielu ludzi i komórek organizacyjnych. Autorzy starali się pokazać znaczenie benedyktyńskiej pracy z zatrudnionym personelem w celu minimalizowania zagrożeń w postaci przejęcia informacji. Praca ta wymaga profesjonalizmu, wiedzy, wyobraźni, umiejętności nawiązywania i podtrzymywania kontaktów oraz wyciągania wniosków i rozumienia motywacji działań szkodzących rozwojowi przedsiębiorstwa. Oznacza to w skrócie umiejętność przewidzenia pojawienia się sytuacji niepożądanej, sprokurowanej wrogą działalnością personelu przedsiębiorstwa. Oznacza to również ogromne doświadczenie w rozpoznawaniu natury człowieka – uczestnika procesów ekspansji przedsiębiorstwa.