dr Paweł Łabuz
adiunkt Wyższej Szkoły Prawa, Ekonomii i Nauk Medycznych w Kielcach
dr Tomasz Safjański
WSPiA Rzeszowska Szkoła Wyższa, Centrum Profilaktyki Biznesu VISNA

Działania kontrwykrywcze grup przestępczych ukierunkowane na ograniczenie skuteczności kontroli operacyjnej oraz procesowej kontroli i utrwalania rozmów

Streszczenie

Artykuł przedstawia zasadnicze aspekty taktyki i techniki przestępczej zmierzającej do ograniczenia skuteczności podsłuchu procesowego oraz kontroli operacyjnej. Scharakteryzowano w nim najistotniejsze sposoby ochrony korespondencji przestępczej. Przedmiotowa problematyka jest zagadnieniem nadzwyczaj skomplikowanym z powodu specyfiki omawianych działań. Działania kontrwykrywcze zorganizowanych grup przestępczych nie stanowiły dotąd priorytetowego obszaru zainteresowania kryminalistyki. W artykule zwrócono uwagę na korzyści wynikające ze znajomości taktyki i techniki przestępczej w zakresie zapewnienia korespondencji poufności, w szczególności w kontekście prowadzonych prac legislacyjnych w przedmiocie realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi.

Słowa kluczowe: podsłuch procesowy, kontrola operacyjna, działania kontrwykrywcze, wykrywanie, taktyka przestępcza

Wprowadzenie

Działania kontrwykrywcze prowadzone w przedmiotowym zakresie obejmują ogół przedsięwzięć podejmowanych przez osoby/grupy prowadzące działalność przestępczą we wszelkich jej formach, które zmierzają do zapewnienia skrytości i poufności prowadzonej korespondencji. Obecnie jest to szeroka gama form, metod i środków, które mogą być klasyfikowane według różnych kryteriów. W praktyce są to różne sposoby utrudniające lub uniemożliwiające organom ścigania zbieranie informacji o użytkownikach urządzeń telekomunikacyjnych, treści komunikatów, danych lokalizacyjnych (dane wskazujące położenie geograficzne urządzenia końcowego), czasie, miejscu i podmiotach korespondencji, a tym samym zebranie i zabezpieczenie materiału dowodowego w omawianym aspekcie.

Przestępcy od dawna dostrzegają korzyści wynikające z ochrony kontrwywiadowczej własnej korespondencji, która z taktyczno-kryminalistycznego punktu widzenia warunkowana jest ograniczeniem skuteczności podsłuchu procesowego oraz kontroli operacyjnej i w tym zakresie osoby, wobec których stosowana jest ta metoda, podejmują szereg przedsięwzięć kontrwykrywczych, jakimi są z ich strony działania: kamuflujące, maskujące, legendujące oraz dezinformujące.

Zasadnicze cele kontroli operacyjnej oraz podsłuchu procesowego są zbieżne i zmierzają do wykrycia i uzyskania dowodów przestępstwa. O zarządzeniu stosowania przez ustawodawcę kontroli operacyjnej (podsłuchu operacyjnego i procesowego) w czynnościach o charakterze wykrywczym zdecydowała ich wysoka wartość poznawcza oraz efektywność w walce z przestępczością.

W doktrynie wskazuje się na problem konkurencji, jaki pojawia się pomiędzy podsłuchem procesowym a kontrolą operacyjną. Natomiast niepublikowane statystyki potwierdzają zdecydowaną przewagę podsłuchów operacyjnych stosowanych przez służby policyjne i specjalne. Wydaje się jednak, że na oba środki należy patrzeć jak na instrumenty komplementarne wobec siebie. Obydwa przecież służą głównie wykrywaniu przestępstw i utrwalaniu dowodów. Przy czym nieco inny jest zakres

spraw karnych, w których podsłuchy te mogą być wykorzystywane. To z kolei stwarza okazję, przynajmniej w niektórych przypadkach, do subsydiarnego traktowania podsłuchu operacyjnego wobec podsłuchu procesowego (Bożek, 2015).

Podsłuch procesowy i kontrola operacyjna

Kontrola i utrwalanie rozmów, najczęściej określane jako podsłuch procesowy, z uwagi na procedurę wdrażania oraz eksploatacji tej kontroli, znajduje się wyłącznie w regulacjach ustawy Kodeks postępowania karnego, a nie w regulacjach ustaw kompetencyjnych służb uprawnionych do stosowania podsłuchu w czynnościach operacyjno-rozpoznawczych. Sytuacja dualizmu niejawnego kontrolowania i utrwalania rozmów, przy prowadzeniu właściwej taktyki śledczej przez prokuratora, pozwala na wykorzystanie tego elementu do wydłużenia czasookresu stosowania kontroli operacyjnej wobec jednej osoby lub – po udostępnieniu materiałów z kontroli operacyjnej stanowiącej dowód w prowadzonym postępowaniu przygotowawczym – na dalsze zastosowanie w tym przypadku podsłuchu procesowego wobec tej osoby.

Kontrola operacyjna to metoda z zakresu czynności operacyjno-rozpoznawczych polegająca na niejawnym monitorowaniu treści korespondencji, sprawdzaniu zawartości przesyłek oraz stosowaniu środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych. W praktyce sprowadza się do możliwości stosowania środków operacyjnych w odniesieniu do szerokiej gamy sposobów komunikowania się, przekazu treści czy przedmiotów pomiędzy podmiotami.

Zasadnicze uprawnienia dotyczące stosowania kontroli operacyjnej są zawarte w ustawach kompetencyjnych służb[1]. Obecnie prawo kontroli operacyjnej ma dziewięć instytucji państwowych: Policja, Straż Graniczna, Centralne Biuro Antykorupcyjne, Agencja Bezpieczeństwa Wewnętrznego, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa, Krajowa Administracja Skarbowa, Agencja Wywiadu i Służba Wywiadu Wojskowego.

Wskazane instytucje kontrolę operacyjną mogą stosować z reguły w trakcie wykonywania czynności operacyjno-rozpoznawczych. W toku kontroli operacyjnej mogą być uzyskiwane informacje dotyczące treści rozmów telefonicznych (w tym przekazywanych przez sieci telefonii komórkowej), informacje w postaci tekstów, SMS-ów, faksów czy obrazów telewizyjnych, a nawet przesyłane pocztą elektroniczną lub uzyskiwane z bezpośredniego podsłuchu (instalowanego w miejscach publicznie niedostępnych) (Herzog, 2007).

Kontrola operacyjna pozwala na zbieranie informacji o działalności przestępczej przed wszczęciem procedury karnej, w jej trakcie oraz po zakończeniu, w sposób umożliwiający ich przekształcenie w materiał dowodowy. Na gruncie wskazanych wcześniej ustaw kompetencyjnych ustawodawca zdecydował się nadać informacjom zgromadzonym w trakcie kontroli operacyjnej status materiałów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla już wszczętego postępowania. W praktyce materiały te są przekazywane do prokuratury jako załącznik do zawiadomienia o możliwości popełnienia przestępstwa, a tym samym traktowane jako środek dowodowy w postępowaniu karnym (Mąka, 2011).

Wśród organów uprawnionych do prowadzenia czynności operacyjno-rozpoznawczych występują organy postępowania przygotowawczego[2], a także inne organy[3] niemające uprawnienia do prowadzenia postępowania przygotowawczego. Na mocy przepisów ustaw określających funkcjonowanie tych organów mają one ogólną kompetencję wykonywania czynności operacyjno-rozpoznawczych (Kaczorkiewicz, 2014). Natomiast uzyskane informacje, dotyczące przestępstwa z katalogu innej ustawy kompetencyjnej, w ramach kontroli operacyjnej prowadzonej przez organy nieprocesowe często mogą zostać przekształcone w informacje operacyjne i przekazane według właściwości rzeczowej organowi celem inicjacji czynności operacyjno-rozpoznawczych, w tym

[1] Ustawy kompetencyjne to akty stanowiące podstawę prawną tworzenia poszczególnych służb, w których określa się zasadnicze kwestie dotyczące organizacji i funkcjonowania tych służb. Aktualnie obowiązujące ustawy kompetencyjne, na podstawie których działają polskie służby państwowe, to m.in.: Ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jedn.: Dz. U. z 2015 r., poz. 355), Ustawa z dnia 12 października 1990 r. o Straży Granicznej (tekst jedn.: Dz. U. z 2014 r., poz. 1402), Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn.: Dz. U. z 2010 r. Nr 29, poz. 154 z późn. zm.), Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jedn.: Dz. U. z 2012 r., poz. 621 z późn. zm.), Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2006 r. Nr 104, poz. 709 z późn. zm.), Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej (tekst jedn.: Dz. U. z 2016 r. poz. 1947).

[2] Policja, Straż Graniczna, Żandarmeria Wojskowa, Kontrola Skarbowa, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne.

[3] Służby specjalne: Agencja Wywiadu, Służba Wywiadu Wojskowego, Służba Kontrwywiadu Wojskowego.

kontroli operacyjnej służącej uzyskaniu materiału dowodowego do przyszłego postępowania karnego.

Właściwym w tym zakresie działaniem jest kontrola prokuratorska nad czynnościami operacyjno-rozpoznawczymi, mająca w szczególności na uwadze zapewnienie legalności i prawidłowości inicjowania i prowadzenia tych czynności[4].

Systematyka działań kontrwykrywczych związanych z ochroną korespondencji przestępczej

Z teoretycznego punktu widzenia wyróżnić można taktykę oraz technikę ochrony treści korespondencji przestępczej.

Taktyka ochrony korespondencji to ogół rozwiązań i metod postępowania przestępców, mających na celu zachowanie hermetyczności grupy rozmówców, zachowanie w poufności treści prowadzonych rozmów, uniemożliwienie zidentyfikowania osób w nich uczestniczących, a tym samym ujawnienie, przeciwdziałanie oraz utrwalenie w postaci materiału dowodowego prowadzonej działalności przestępczej. Wśród działań taktycznych można wyróżnić m.in.:

1. stosowanie anonimowych systemów telefonicznych,
2. slang przestępczy,
3. szyfrowanie korespondencji,
4. samokontrolę,
5. działania dezinformacyjne,
6. zagłuszanie podsłuchu,
7. badania antyinwigilacyjne pomieszczeń.

Technika ochrony korespondencji to ogół środków technicznych (urządzeń, aplikacji) utrudniających organom ścigania namierzenie i kontrolę korespondencji przestępczej oraz jej utrwalenie i zabezpieczenie w postaci materiału dowodowego. W zakresie techniki ochrony korespondencji wskazać należy na wykorzystanie skrzynek SIM (ang. *SIM box*).

W dobie dynamicznego postępu technologicznego poszukiwane są najnowsze rozwiązania z wykorzystaniem elementu tzw. właściwości prawnej[5] serwerów internetowych, kont pocztowych, komunikatorów internetowych, które w prowadzonej działalności przestępczej służą zapewnieniu „bezpiecznej" i anonimowej komunikacji.

Anonimowe systemy telefoniczne

Zachowanie konspiracji treści komunikacji z wykorzystaniem telefonów komórkowych wymusza na przestępcach kreowanie tzw. anonimowych systemów telefonicznych, opartych na daleko posuniętej samodyscyplinie wzajemnych kontaktów.

W kontaktach tych przestrzegane są następujące zasady:

- aby pozostać niespersjoanlizowanym oraz niezidentyfikowanym, istniejące przepisy[6] umożliwiają anonimowe nabycie zarejestrowanych kart SIM na inną osobę lub podmiot, niemające żadnego związku oraz powiązań z użytkowaniem tej karty;
- rozmowy telefoniczne prowadzone są w wąskim gronie najbardziej zaufanych osób (z jednym lub też kilkoma rozmówcami), tzw. telefony jeden na jeden;
- aparaty telefoniczne i karty SIM nie mogą być wcześniej używane do prowadzenia rozmów z innymi rozmówcami;
- telefony nie mogą być wcześniej używane do obsługi innych kart SIM, tzw. bezpiecznych, niezarejestrowane na tzw. słupy;
- żaden z kręgu rozmówców nie może dokonać rejestracji karty SIM lub też doładowania karty SIM z innego telefonu czy też za pomocą konta bankowego;
- zestawy telefoniczne wymieniane są na nowe cyklicznie przez wszystkich rozmówców;
- informacje o numerach nowych zestawów przekazywane są osobiście (nie przez SMS-y z użytego poprzednio zestawu);
- stary telefon nie jest wykorzystywany przez dotychczasowego posiadacza do obsługi innej karty SIM (najczęściej jest niszczony);
- wykorzystywanie numerów telefonów zagranicznych operatorów komórkowych (ukraińskich, słowackich itd.) na terenie kraju;

[4] Tekst uzasadnienia do Projektu z dnia 12 sierpnia 2016 r., Rozporządzenia Ministra Sprawiedliwości w sprawie sposobu realizacji czynności prokuratora w ramach kontroli nad czynnościami operacyjno-rozpoznawczymi.

[5] Dane rejestrowe oraz znajdujące się na przykład na danym koncie pocztowym (e-mail) lub zarządzenie kontroli korespondencji może nastąpić wyłącznie na podstawie postanowień sądów właściwych dla właścicieli domeny: amerykańskich, rosyjskich itp.

[6] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2016 r., poz. 904). Karty prepaid rejestruje się osobiście, za okazaniem dowodu osobistego lub paszportu – skany, kopie i ksera nie są dokumentami i na ich podstawie nie dokonamy rejestracji. Dzieci, które mają swój dowód osobisty, mogą zarejestrować kartę samodzielnie, muszą jednak mieć ukończone 13 lat. Przepisy ustawy prawo telekomunikacyjne nie określają limitów liczby kupowanych kart prepaid, wprowadzają natomiast obowiązek rejestracji (podania) danych przez abonenta i autoryzacji (potwierdzenia) tych danych przez dostawcę, dla każdego z przypisanych do karty SIM numerów MSISDN. Dane za stroną: http://www.cik.uke.gov.pl/obowiazek-rejestracji-kart-prepaid-20220# [dostęp: 19.09.2017].

– telefony znajdują się pod stałą kontrolą posiadacza.

Przestrzeganie tych zasad pozwala bardzo często w świadomości tych osób uzyskać dość szczelny i anonimowy system telefoniczny.

Slang przestępczy

Slang przestępczy to język specjalny, bazujący na odrębności środowiska przestępczego[7]. Różni się od języka ogólnego leksyką, frazeologią i zmianami znaczeń słownictwa ogólnego, a nie gramatyką. Jest to forma tworzenia zabezpieczenia kryptologicznego rozmów, mająca na celu ukrycie ich rzeczywistego sensu (konotacji semantycznej). Można wyróżnić trzy rodzaje tego typu zabezpieczeń: niskie, średnie i wysokie[8].

Używane zwroty i wyrażenia są charakterystyczne dla danego środowiska przestępczego na obszarze całego kraju lub w jego części, przykładowo w danym regionie lub województwie. Rozmowy mogą być prowadzone w bardziej zrozumiałym tzw. slangu subkulturowym (młodzieżowo-kryminalnym), charakteryzującym się m.in. uproszczonym słownictwem, skrótami myślowymi, wulgaryzmami. Taka analiza własna pozwala na określenie wzajemnych zależności, podległości i tym samym wykazuje strukturę przedmiotowej (zorganizowanej) grupy przestępczej. Bardzo często udostępniony do postępowania karnego materiał z przeprowadzonej kontroli operacyjnej stanowi także procesowy „dowód" istnienia grupy oraz elementów jej struktury, czyli systemu powiązań między tymi osobami, a także „hierarchii", czyli rodzaju podległości i zależności między konkretnymi jednostkami.

Przykładami slangu przestępczego dotyczącego obrotu narkotykami (tzw. narkoslangu) są różne określenia wskazujące rodzaj, ilość, wagę, jakość danego narkotyku, formę płatności za ich zakup. W odniesieniu do marihuany są to: *trawa*, *ziele*, *zioło*, *baka*, *maryśka*, *zielone*, *palenie*; do haszyszu: *afgan*, *czekolada*, *hasz*, *gruda*, *lepik*; do amfetaminy: *amfa*, *białe*, *władek*, *ścierwo*, *bielinka*; do kokainy: *koko*, *koks*, *biała dama*; do extazy: *kółko*, *cukierki*, *tabsy*, *pix*. Natomiast w odniesieniu do ilości i wagi: *klocek*, *dżis*, *polówka*, *sztuka*, *jedynka*[9]; w odniesieniu do formy płatności: *za hajs*, *w kredo*.

Na osobną uwagę zasługuje stosowane słownictwo slangowe związane z przerobem i produkcją oraz nielegalnym obrotem wyrobami tytoniowymi, które często charakteryzuje się niską konotacją semantyczną stosowaną przez rozmówców. Poszczególne używane określenia charakteryzują rodzaje, marki, ilości tych wyrobów, na przykład *ciemny, jasny, czarny* – wskazuje rodzaj danego tytoniu; *malwiny, marchewki* – oznaczają papierosy marki Marlboro; *tona* – zawiera tysiąc kartonów.

Oczywiście przytoczone określenia slangowe nie wyczerpują całego tego typu słownictwa. Pokazują jednak pewien mechanizm jego tworzenia i używania przez rozmówców.

W celu właściwej interpretacji kamuflażu prowadzonych rozmów telefonicznych osób objętych kontrolą operacyjną należy zawsze wziąć pod uwagę pewne stałe zasady (elementy) – występujące jako niezmienne, niekontrolowane i naturalne zachowania także w życiu codziennym. Wśród nich jest *zasada racjonalności zachowań*, gdzie przykładowo w przypadku złożenia zamówienia/planowanej transakcji (telefonicznego umówienia się na jej dokonanie/spotkanie, w której fizycznie dojdzie do przekazania narkotyków oraz odebrania pieniędzy przez sprzedającego – dealera za ich zakup) nie zachodzi sytuacja jej telefonicznego potwierdzania/informowania o fakcie zakupu/przekazania. Natomiast w *racjonalnym zachowaniu* zawsze funkcjonuje tzw. *zasada informacji zwrotnej* o niemożliwości przybycia lub rezygnacji z dokonania zaplanowanej (umówionej telefonicznie) transakcji czy ze spotkania. Oczywiście, jeśli nie ma potwierdzenia lub pewności, że komunikacja/korespondencja pomiędzy tymi osobami nie opiera się wyłącznie na numerze telefonu lub aparatu objętego kontrolą.

Kolejną zasadą powszechnie stosowaną we wszelkiej komunikacji interpersonalnej jest *zasada oszczędności słownej* (językowej). Podczas prowadzenia (stałych lub doraźnych) przestępczych transakcji (narkotykowych itd.) nie zachodzi sytuacja pełnego wyrażania (określania) nazw, także slangowych, tych rzeczy[10] oraz ich cen, ilości itd. Bardzo często określane są one

[7] Przestępczości kryminalnej – na przykład: oszustw, pobić, napadów, handlu bronią palną, czerpania korzyści z cudzego nierządu. Przestępczości narkotykowej – na przykład: produkcji, przemytu oraz obrotu środkami odurzającymi i substancjami psychotropowymi. Przestępczości ekonomicznej – na przykład: przemyt i obrót wyrobami akcyzowymi, wyłudzenia i oszustwa bankowe, podatkowe.

[8] Określają stopień zaszyfrowania, gdzie dane zwroty są charakterystyczne dla konkretnego środowiska przestępczego oraz używany język bardziej lub mniej jednoznacznie wskazuje na określony profil przestępczości, na przykład handel narkotykami.

[9] http://www.narkoslang.pl/slowniczek_wyrazen.html [dostęp: 24.08.2016].

[10] Rzeczy, przedmiotów pochodzących z przestępstwa, ulegających przepadkowi albo których wytwarzanie, posiadanie, przewożenie lub którymi obrót są zabronione, a także przyjęciu lub wręczeniu korzyści majątkowej.

wyrażeniami skrótowymi[11], natomiast ich właściwe/prawdziwe znaczenie może także wynikać z kontekstu wcześniejszej korespondencji (rozmowy).

Używanie w korespondencji wyspecjalizowanego slangu przestępczego nierzadko powoduje konieczność powołania biegłego sądowego z zakresu kryminologii slangu przestępczego[12] w celu interpretacji materiałów uzyskanych w wyniku podsłuchu procesowego lub kontroli operacyjnej.

Szyfrowanie korespondencji

Popularnym działaniem kontrwywiadowczym jest szyfrowanie komunikacji, które obejmuje tradycyjne formy szyfrowania, nowoczesne środki techniczne oraz swoiste szyfry.

Szyfrowanie tradycyjne to zwykłe używanie słów w kontekście uniemożliwiającym lub skrajnie utrudniającym ich zrozumienie przez osobę nieposiadającą dodatkowej informacji, czyli tzw. klucza.

W ramach działań kontrwywiadowczych zorganizowane grupy przestępcze wykorzystują również nowoczesne technologie informatyczne i komunikacyjne służące do łatwego porozumiewania się w czasie rzeczywistym w postaci narzędzi szyfrujących lub zabezpieczonych stron internetowych.

Specyficzną formą szyfrowania przekazu jest używanie bardzo rzadkich dialektów (np. ujgurski, nieniecki, adygejski, maryjski czy choćby gruziński).

Samokontrola

Przykładem samokontroli w zakresie ochrony korespondencji przestępczej jest częsta wymiana kart prepaid w użytkowanych telefonach komórkowych. W praktyce dla organów ścigania powoduje to nie tylko konieczność ustalenia nowego numeru telefonu, lecz również obowiązek, zgodny z procedurą ustawową, zarządzenia kolejnej kontroli operacyjnej na ustalony nowy numer telefonu. Uświadomieni przestępcy wiedzą, że procedura wdrożenia kolejnej kontroli operacyjnej trwa, co potencjalnie daje czas na „bezpieczną" działalność przestępczą.

W omawianym kontekście działaniem doraźnym jest czyszczenie pamięci urządzeń mobilnych po zakończeniu korespondencji, zapobiegające w przypadku zabezpieczenia tego urządzenia przez organy ścigania uzyskaniu danych (treści) prowadzonej korespondencji oraz danych kontaktowych.

Używanie skrzynek SIM

Skrzynki SIM (ang. *SIM box*) zawierają jedną lub więcej kart SIM; są nazywane również urządzeniami FCT (ang. *Fixed Cellular Terminal*) lub bramkami GSM (ang. *GSM gateways*). Na rynku dostępnych jest kilka rodzajów urządzeń służących do transferu ruchu telekomunikacyjnego, m.in.: adaptery GSM, bramki GSM, serwery SIM. Najprostsze z nich stanowią jedynie interfejs pomiędzy centralą abonencką a zakończeniem sieci GSM i wymagają dołączenia standardowego telefonu GSM. Natomiast najbardziej skomplikowane umożliwiają połączenie do sieci stałej za pomocą łączy 2 Mbit/s i umożliwiają jednoczesne użycie kilkudziesięciu kart SIM.

Podstawowym przeznaczeniem tego typu urządzeń jest umożliwienie abonentom instytucjonalnym dysponującym prywatną siecią telefoniczną (firmy, urzędy) podłączenia do sieci komórkowej. Skrzynki SIM łączą w sobie funkcjonalność urządzeń końcowych (terminali) sieci komórkowej oraz sieci stacjonarnej, dzięki czemu mogą być używane także do transferowania ruchu telekomunikacyjnego (przekierowywania połączeń z innych sieci telekomunikacyjnych do sieci mobilnej, z pominięciem międzyoperatorskiego punktu styku tych sieci). W wyniku takiego przekierowania połączenie z sieci stacjonarnej do mobilnej (ang. *fixed-to-mobile*) z punktu widzenia operatora sieci mobilnej widziane jest jako rozmowa inicjowana w jego sieci mobilnej (ang. *on-net*) (Kłosowski, 2007).

Ruch, który jest transferowany poprzez skrzynki SIM pochodzić może z kilku różnych źródeł:

1. od operatorów międzynarodowych kierujących do Polski ruch pochodzący z zagranicznych sieci stacjonarnych i komórkowych, w tym również od abonentów polskich operatorów komórkowych korzystających z usługi roamingu w sieciach zagranicznych;
2. od operatorów krajowych świadczących usługi w krajowej sieci stacjonarnej;
3. od abonentów usług telefonii internetowej (tzw. *Voice over IP*) realizujących połączenia za pomocą tzw. soft-phone'ów (jak komunikatory internetowe) lub za pomocą zwykłych aparatów telefonicznych poprzez wdzwonienie się do systemu telefonicznego operatora (często używany jest w tym celu model sprzedaży poprzez tzw. karty-zdrapki). Warto w tym miejscu zauważyć, iż abonenci, których połączenia są transferowane, mogą być tego faktu świadomi i wówczas świadomie wybierają usługi podmiotów oferujących takie usługi, jak również mogą być nieświadomi – może to się odbywać bez ich zgody oraz zgody ich operatora (co dobrze widać na wymienionym powyżej przykładzie abonentów będących w roamingu).

Należy w tym miejscu podkreślić, że skrzynki GSM wykorzystywane prawidłowo w celu, w którym zostały stworzone, tj. do podłączania abonentów do sieci

[11] Przykładowo: *to, co ostatnio; tamto* itp.

[12] http://www.narkoslang.pl/narko_adm/uploads/files/biegly_sadowy_jacek_wrona.jpg [dostęp: 24.08.2016].

GSM, nie stanowią żadnego utrudnienia podczas działań związanych z ochroną bezpieczeństwa i porządku publicznego. Ewentualne problemy dla pracy wykrywczej pojawiają się dopiero w wyniku użycia tych urządzeń do transferu ruchu, a więc niezgodnie z przeznaczeniem.

Połączenia kierowane do sieci komórkowych za pomocą skrzynek SIM mają zablokowaną przez użytkownika prezentację numeru (tzw. CLIR – *Calling Line Identification Restriction*). W efekcie zastosowania skrzynek SIM brak jest informacji o numerze abonenta wywołującego dane połączenie telefoniczne. Przekazywany jest jedynie (prawdziwy lub nieprawdziwy) numer karty SIM, za pośrednictwem której dane połączenie kierowane jest do sieci mobilnej. W związku z tym ani operator sieci mobilnej, ani też abonent odbierający połączenie nie są informowani o numerze abonenta inicjującego połączenie lub też są informowani błędnie. Oznacza to, że abonent odbierający połączenie otrzymuje informację o numerze, z którego dane połączenie pochodzi, a w rzeczywistości nie jest to numer abonenta inicjującego, lecz numer karty SIM w skrzynce SIM, przez którą to połączenie jest kierowane.

W przypadku wykorzystania skrzynki SIM operator sieci mobilnej uzyskuje informacje jedynie o właścicielu urządzenia (numer karty SIM oraz lokalizację skrzynki). Nie posiada on jednak informacji o osobie, która zainicjowała połączenie. Aby była ona dostępna, właściciel skrzynki SIM musiałby gromadzić informacje o ruchu wewnątrz własnej sieci oraz posiadać informacje na temat przypisania poszczególnych urządzeń końcowych w tej sieci do osób wykorzystujących urządzenia.

Ze względu na niemożność ustalenia przez uprawnione podmioty numeru, z którego wywołano połączenie, a w konsekwencji również tożsamości osoby wywołującej połączenie, utrudnione staje się zrealizowanie takich celów analizy kryminalnej, jak:

1. ustalenie wzajemnych połączeń pomiędzy numerami telefonów;
2. ustalenie numerów telefonów, z którymi kontaktował się dany numer telefonu w określnym czasie;
3. wyselekcjonowanie numerów telefonicznych, z którymi najczęściej kontaktował się dany numer telefonu w określonych dniach i godzinach;
4. sporządzenie wykazu najczęściej realizowanych połączeń dla danego numeru telefonu;
5. ustalenie innych niż bezpośrednie połączenia powiązań pomiędzy numerami telefonów;
6. pozycjonowanie numeru telefonu względem masztów przekaźnikowych w danym czasie;
7. wnioskowanie o trybie życia.

Wskazane przeszkody mogą utrudniać prowadzenie podsłuchu lub kontroli.

Działania dezinformacyjne

Działania dezinformacyjne polegają na wprowadzeniu organów ścigania w błąd; sprawdzenie ich zainteresowania osobą lub grupą oraz sprawności i aktywności może następować poprzez ukierunkowane przekazywanie fałszywych informacji. Dezinformowanie może mieć miejsce podczas stosowania kontroli operacyjnej lub podsłuchu procesowego.

W odniesieniu do przekazu informacji, która ma stać się faktyczną dezinformacją, przybierają one formę świadomego pomijania pewnych informacji, sugerowania pewnych informacji poprzez kolejność ich przedstawiania, kłamstwa, pozoracji, upraszczania czy wręcz oszustwa. Taka właściwie manipulacja informacją przez przestępców ma wywołać wiele skutków, tj. podać:

- informacje nieprawdziwe;
- informacje nieważne lub mało ważne, z pominięciem najważniejszych;
- informacje bardzo ważne, przekazywane jako mało ważne lub bez znaczenia;
- informacje spreparowane w wyniku celowych interwencji, informacje wieloznaczne, aby utrudnić ich zrozumienie;
- informacje przekazywane w nadmiarze, aby spowodować chaos dezinformacją;
- pseudoinformacje – będące informacjami dostarczanymi przez różne komunikaty, lecz dotyczącymi tego samego przedmiotu;
- parainformacje – będące informacjami subiektywnymi wynikającymi z mylnej interpretacji treści zawartych w komunikatach[13].

Zagłuszanie podsłuchu

W celu zagłuszenia podsłuchu wykorzystywany jest sprzęt do generowania szumu radiowego na tej samej częstotliwości i przy użyciu tej samej modulacji co fala pierwotna. Dzięki temu niwelowane jest działanie urządzeń podsłuchujących.

Ponadto wykorzystywane są systemy zniekształcające nagrane dźwięki, dzięki czemu są one niezrozumiałe i niemożliwe do użycia.

Badania antyinwigilacyjne

Badania antyinwigilacyjne mają za zadanie sprawdzenie pomieszczeń pod kątem występowania obcych systemów optycznych (kamery, aparaty fotograficzne itp.), aktywnych lub nieaktywnych podzespołów elektronicznych (nadajniki, rejestratory itp.), emisji sygnałów w zakresie podczerwieni (nadajniki Infra-red), emisji sygnałów radiowych w zakresie do 25 GHz, emisji sygnałów radiowych w zakresach niskich

[13] http://www.ktime.up.krakow.pl/symp2011/referaty2011/babik.pdf [dostęp: 25.08.2016].

częstotliwości (poniżej 1 MHz), emisji zidentyfikowanych sygnałów radiowych w zakresie do 3 GHz, emisji sygnałów częstotliwości podnośnych w sieci telefonicznej oraz 220 V.

Funkcja działań kontrwykrywczych w działalności przestępczej

Stosowanie działań kontrwykrywczych stanowi reakcję obronną na prowadzone przez organy ścigania specjalne działania wykrywcze w postaci podsłuchu procesowego lub kontroli operacyjnej. Mają one charakter działań defensywnych, czyli służą wzmocnieniu własnej grupy w celu uniknięcia jej neutralizacji. Czynnikami warunkującymi skuteczność działań kontrwykrywczych są m.in.:

1. właściwe wyposażenie techniczne (np. skanery, aplikacje szyfrujące);
2. sytuacja operacyjna związana z prowadzoną działalnością przestępczą, która może wymagać jednorazowego zastosowania jednego rodzaju działań lub wielokrotnego użycia kombinacji wielu działań kontrwykrywczych;
3. doświadczenie i wyszkolenie przestępców w stosowaniu danego rodzaju działań;
4. czynnik szybkiego osiągnięcia celu przestępczego (im dłużej trwa działanie przestępcze, tym większe ryzyko wykrycia);
5. możliwości finansowe zorganizowanej grupy przestępczej.

W celu uniknięcia działań zapobiegających służb państwowych, które uzyskały ze stosowanej w tym czasie kontroli operacyjnej wyprzedzającą informację o planowanym przestępstwie, przykładowo zaplanowanej (umówionej) transakcji narkotykowej, osoba taka stosuje szereg czynności kontrwykrywczych (zapobiegawczych), tj.:

– na spotkania z dostawcami – odbiorcami narkotyków umawia się bardzo często w miejscach trudnych (sprawdzonych, na otwartej przestrzeni, trudno dostępnych – prywatnych itp.), przykładowo do przygotowania przez służby zasadzki w celu zatrzymania sprawców na gorącym uczynku;
– spotkania w miejscach, z których możliwe jest prowadzenie kontrobserwacji przez osoby z nią współpracujące;
– w przypadku konieczności zmienia w ostatniej chwili miejsca spotkania, informując za pomocą innego środka korespondencji.

Rolą działań kontrwykrywczych jest zmniejszenie skuteczności działań organów ścigania w fazie operacyjnego zbierania informacji oraz utrudnienie działań podejmowanych przez organy ścigania w fazie właściwego przekształcania materiału operacyjnego w procesowy. Ponadto utrudnienie nie tylko zidentyfikowania i zlokalizowania działalności kryminalnej, ale również ograniczenie możliwości zebrania i zabezpieczenia materiału dowodowego (np. dowodów wynikających z podsłuchu telefonicznego) czy udowodnienie zorganizowanego charakteru grupy.

Podsumowanie

Działalność kontrwykrwycza przestępcza jest zasadniczo nieodzowna w każdej działalności przestępczej, stanowiąc „filar własnego bezpieczeństwa", bezkarności w podejmowaniu przedsięwzięć przestępczych. Zachowanie daleko idących środków ostrożności, stosowanie tzw. samokontroli ma – w przekonaniu tych osób – gwarantować większe bezpieczeństwo prowadzonych interesów. Największym osiągnięciem w działalności przestępczej jest całkowita anonimowość oraz utajnienie samej działalności przestępczej. Opisany system zachowań przestępczych można właściwe określić jako technika i taktyka kontrwykrywcza. Poznanie oraz właściwe zdiagnozowanie tych działań przez organy ścigania pozwala na odpowiednie zastosowanie techniki i taktyki wykrywczej zarówno na płaszczyźnie operacyjnej, jak i procesowej.

Bibliografia

1. Bożek, M. (2015). Charakterystyka ustawowych uprawnień operacyjnych służb specjalnych. *Rocznik Administracji Publicznej*, *1*.
2. Babik, W. (2011). O manipulowaniu informacją w prywatnej i publicznej przestrzeni informacyjnej, http://www.ktime.up.krakow.pl/symp2011/referaty2011/babik.pdf [dostęp: 25.08.2016].
3. Dolecka, A., Łodziana, T. (2015). Taktyczne aspekty stosowania kontroli operacyjnej. W: E.W. Pływaczewski, W. Filipkowski, Z. Rau, (red.), *Przestępczość w XXI wieku – zapobieganie i zwalczanie*. Warszawa: Wolters Kluwer Polska.
4. Drajewicz, D. (2011). Glosa do postanowienia Sądu Najwyższego z dnia 25 marca 2010 r., sygn. I KZP 2/10. *Prokuratura i Prawo*, *9*.
5. Herzog, A. (2007). Wykorzystanie materiałów operacyjnych w postępowaniu dyscyplinarnym prokuratorów. *Prokuratura i Prawo*, *2.*
6. http://www.narkoslang.pl [dostęp: 25.08.2016].
7. Kaczorkiewicz, D. (2014). Granice inwigilacji społeczeństwa w zakresie czynności operacyjno-rozpoznawczych. W: E. Cała-Wacinkiewicz, K. Flaga-Gieruszyńska, D. Wacinkiewicz, (red.), *Obywatel – państwo – społeczność międzynarodowa*. Warszawa: C.H. Beck.
8. Kłosowski, A. (2007). Opinia specjalistyczna w zakresie wpływu transferu ruchu z pominięciem punktów styku sieci telekomunikacyjnych (za pomocą urządzeń FCT) na realizację

przez operatorów telekomunikacyjnych zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. Warszawa.
9. Mąka, J. (2011). Kontrola operacyjna i podsłuch – ocena na tle praktycznego stosowania. *Przegląd Bezpieczeństwa Wewnętrznego, 4*/11.
10. Skorupka, J. (2011). Krytycznie o stanowisku Sądu Najwyższego w kwestii legalności kontroli rozmów telefonicznych. *Prokuratura i Prawo, 4*.
11. Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, Dz. U. z 2001 r. Nr 123, poz. 1353.
12. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, Dz. U. z 2016 r., poz. 1749. (tekst jedn.).
13. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, Dz. U. z 1997 r. Nr 89, poz. 555 (z późn. zm.).