**Brunon Czabok**

# Dezinformacja w telekomunikacji

W przeszłości jedynym, a dziś nadal najbardziej popularnym, sposobem identyfikacji stron połączenia telefonicznego jest przedstawianie się osoby inicjującej połączenie, zwanej zwyczajowo abonentem A i potwierdzenie w trakcie rozmowy, iż osoba odbierająca połączenie (abonent B) jest jego właściwym adresatem. Oferowana obecnie wierność przekazywanych sygnałów akustycznych dodatkowo umożliwia znającym się abonentom rozpoznawanie siebie nawzajem na podstawie charakterystycznych cech głosu. Jest to dość skuteczna metoda, chociaż z pewnością każdemu zdarzały się pomyłki związane z błędnie rozpoznanym głosem rozmówcy. Wynika to z ograniczonego pasma przenoszenia sygnału akustycznego w sieciach telekomunikacyjnych (od 300 Hz do 3400 Hz), mimo że rzeczywisty zakres widma mowy rozciąga się od około l00 Hz do ponad 8000 Hz. Pasmo telefoniczne zostało tak dobrane, aby zapewniać zrozumiałość mowy, jednak eliminuje ono pewne częstotliwości, zmieniając charakterystyczny dla poszczególnych mówców ton i barwę głosu. Gdy do tego dodamy szumy i zniekształcenia powstałe w trakcie transmisji oraz konwersji sygnału z postaci analogowej na cyfrową i odwrotnie, to mylna identyfikacja abonenta staje się możliwa. Dlatego wyspecjalizowane służby często wykorzystują hasła lub kryptograficzne metody zapewniające uwierzytelnienie stron komunikacji elektronicznej. Przeciętny użytkownik nie stosuje tak wyrafinowanych metod weryfikacji drugiego abonenta, ale współczesne systemy telekomunikacyjne oferują daleko idącą pomoc w zakresie identyfikacji abonentów dzięki rozpowszechnieniu usługi CLIP (ang. *Calling Line Identification Presentation*), czyli prezentacji numeru połączenia przychodzącego. Sieci zintegrowane cyfrowo wykorzystują specjalny kanał sygnalizacyjny, w którym przekazywane są dane niezbędne do prawidłowej obsługi połączeń. Jest tam też miejsce na numer abonenta A oraz abonenta B. Postęp techniczny sprawił, że coraz trudniej jest znaleźć telefon bez wyświetlacza, na którym może być prezentowany numer abonenta A, o ile ten nie włączył usługi CLIR (ang. *Calling Line ldentification Restriction*), tzn. nie zastrzegł swojego numeru. Oczywiście, zastrzeżenie numeru nie eliminuje go z danych zawartych w protokole sygnalizacyjnym, a jedynie zawiera dodatkową informację dla centrali końcowej, aby nie udostępniać abonentowi B prezentacji numeru. Skoncentrujmy się jednak na najczęściej spotykanym przypadku, kiedy abonent A nie ukrywa swego numeru.

Popularność usługi CLIP wprowadziła już pewne zmiany w zasadach telefonicznego savoir-vivre'u, polegające na odstąpieniu od wspomnianego na początku przedstawiania się w przypadku, gdy dzwonimy do osób znających nasz numer, np. mających go w książce telefonicznej swojego aparatu. Widząc na wyświetlaczu nazwisko znajomego albo prezentujący się numer abonenta połączenia przychodzącego lub też nadawcy SMS-a, wierzymy w jego prawdziwość, tak jak w wynik działania wykonanego na kalkulatorze. I niestety, czasem nasze zaufanie jest nadużywane. Prezentowany numer nie jest wynikiem działania prostego algorytmu (jak np. w kalkulatorze), lecz jest przekazywany z sieci do sieci. Współczesne systemy telekomunikacyjne posiadają punkty transferu sygnalizacji (ang. *Signal Transfer Point* – STP). Sieć przyjmująca połączenie nie weryfikuje numeru abonenta A, tylko prezentuje go swojemu abonentowi końcowemu (B) lub przekazuje dalej do kolejnej sieci. Każdy na pewno pamięta przed-

szkolną zabawę w „głuchy telefon" – im dłuższy jest łańcuch pośredników, tym bardziej zniekształcona zostaje informacja końcowa. Przykład jest oczywiście przejaskrawiony, gdyż nawet w przypadku połączeń międzynarodowych rzadko się zdarza, aby na drodze połączenia znalazło się więcej niż 3 operatorów. Wystarczy jednak, że jeden będzie nierzetelny i podmieni lub ustawi atrybut numeru jako zastrzeżony i na naszym wyświetlaczu pojawi się fałszywa informacja. Dezinformacja ta może być zamierzona lub powstać jako skutek uboczny zastosowanych technologii przekazywania ruchu pomiędzy sieciami poszczególnych operatorów.

## Dezinformacja zamierzona

W pierwszym przypadku mamy do czynienia z sytuacją, kiedy abonent inicjujący połączenie świadomie wprowadza nieprawdziwy numer. Protokoły sygnalizacji korygują tylko elementarne błędy na poziomie transmisji pakietów, lecz, jak już wspomniano, nie zawierają mechanizmów weryfikacji numeru. We współczesnych sieciach cyfrowych powszechnie wykorzystywany jest protokół SS7 (ang. *Signaling System No. 7)*[1], który został opublikowany w 1981 r. Prawdopodobnie nie kładziono wtedy tak dużego nacisku na uwierzytelnianie i kontrolę integralności danych. W każdym razie, protokół ten jest podatny na ingerencję, a w szczególności daje możliwość wprowadzania dowolnych danych do obszaru identyfikującego abonenta A. Jest to wykorzystywane przez podmioty, które wyspecjalizowały się w spoofingu[2].

Polski przedsiębiorca z Nysy w dniu 1 czerwca 2009 r. uruchomił serwis internetowy www.wykrecnumer.pl, który oprócz usług komunikacyjnych, takich jak wysyłanie SMS-ów i prowadzenie rozmów telefonicznych w technologii VoIP[3], oferował usługę dowolnej edycji numeru inicjującego. Na podstawie złożonego przez ABW zawiadomienia o popełnieniu przestępstwa sprawą zajęła się Prokuratura Okręgowa w Opolu, której działania doprowadziły do likwidacji serwisu z dniem 04.11.2009 r., jego właścicielowi zaś, a zarazem administratorowi, postawiono zarzuty popełnienia przestępstwa z art. art. 269 § 1 kk, 287 § 1 kk, 268 §§ 1 i 2 kk, 268a § 1 kk, 269a kk, 269b § 1 kk w zw. z art. art. 11 § 2 kk i 12 kk. W grudniu 2010 r. właściciel serwisu został formalnie oskarżony m.in. o to, że nie będąc do tego upoważnionym, dokonywał zmian istotnych danych informatycznych w postaci informacji o numerach telefonów wywołujących połączenie, mających szczególne znaczenie dla obronności kraju i funkcjonowania instytucji państwowych, których celem jest obrona porządku prawnego, oraz bezprawnie wpływał – a przez to również zakłócał – na automatyczne przetwarzanie, gromadzenie i przekazywanie przez operatorów sieci wyżej wymienionych danych, co spowodowało potencjalne zagrożenia dla skutecznej realizacji zadań z zakresu obronności, bezpieczeństwa oraz ochrony porządku publicznego państwa. Za to przestępstwo prokurator zażądał kary 2 lat pozbawienia wolności. Na podstawie art. 335 § 1 kpk oskarżony zgodził się na dobrowolne poddanie się karze łącznej (postępo-

[1] Jest wiele publikacji przybliżających protokół SS7; autor artykułu posiłkował się książką D. Kościelnika, pt. *ISDN – cyfrowe sieci zintegrowane usługowo*, Warszawa 2007, WKiŁ.

[2] Spoofing (ang. *spoof* – oszukiwać, imitować, parodiować) – określenie, które w dziedzinie IT pojawiło się jako termin oznaczający podszywanie się pod inny numer IP, tzw. *IP spoofing*.

[3] Z ang. *Voice over Internet Protocol* – technologia umożliwiająca przesyłanie głosu za pomocą łączy internetowych lub innych sieci wykorzystujących protokół IP.

wanie obejmowało również inne przestępstwa) 4 lat pozbawienia wolności z warunkowym zawieszeniem jej wykonania na okres próbny 6 lat oraz karze grzywny. W tej sprawie istotny jest również fakt, iż w ramach śledztwa prokurator zabezpieczył dyski komputerowe, na których zostały zarejestrowane dane związane z zestawianiem poszczególnych połączeń i wysyłaniem SMS-ów. Może to mieć znaczenie w przypadku ewentualnych śledztw w sprawie przestępstw popełnionych przy pomocy korzystania z serwisu www.wykrecnumer.pl, gdyż dane te pozwalają na ustalenie, kto był sprawcą przestępstwa, tzn. jaki numer był podmieniony, jaki był prezentowany na dalszej drodze połączenia i kiedy miało to miejsce. Z danych tych wynika, że najczęściej podszywano się pod numer 997.

Serwis został zlikwidowany, a sprawca, niezależnie od tego, czy sąd przychyli się do wniosku o dobrowolne poddanie się karze, czy też przeprowadzi rozprawę, niewątpliwie zostanie ukarany. Jest to niekwestionowany sukces polskiego wymiaru sprawiedliwości, ale zwycięstwo w tym jednym przypadku nie przesądza o sukcesie w walce z całym procederem. Ze względu na możliwość udostępniania tego typu usług za pośrednictwem internetu, który nie respektuje granic państwowych, przeciwdziałanie temu zjawisku jest trudne i w związku z tym nadal istnieje możliwość korzystania z usług przedsiębiorców oferujących podmianę numeru. Intencją autora artykułu nie jest promowanie tego typu usług, dlatego nie zostaną tu przytoczone konkretne adresy, jednakże po wpisaniu w wyszukiwarkę hasła np. „ID spoofing" można bez trudu znaleźć kilkanaście serwisów umożliwiających wysyłanie SMS-ów lub telefonowanie z jednoczesnym podszywaniem się pod wybrany numer. Analogiczna sytuacja dotyczy również poczty elektronicznej oraz adresów IP.

Wyżej wymieniony proceder jest bardzo niebezpieczny, pozwala bowiem oszustom podszywać się nie tylko pod numery osób fizycznych, ale również ważnych instytucji (m.in. Policji, Straży Pożarnej) oraz firm, w szczególności banków, by w ten sposób wyłudzić cenne informacje lub wpływać na zachowanie się ofiary oszustwa. Możliwość podszywania się pod dowolny numer nie tylko daje duże możliwości popełniania przestępstw w sferze gospodarczej i obyczajowej, ale też może wprowadzać w błąd wymiar sprawiedliwości, służby odpowiedzialne za bezpieczeństwo państwa i bezpieczeństwo publiczne oraz poważnie utrudniać im pracę. Na podstawie ustawowych uprawnień podmioty te często przeprowadzają analizę raportów połączeń (bilingów). Raport połączeń przychodzących zawiera takie numery, jakie zostały dostarczone za pomocą protokołu sygnalizacyjnego przedsiębiorcy telekomunikacyjnemu obsługującemu abonenta B. Gdy będziemy mieli do czynienia ze *spoofingiem*, będą to numery nieprawdziwe, wprowadzające dany organ w błąd. Fałszywe numery na bilingu mogą bardzo skomplikować przedsięwzięcia operacyjne, śledcze czy analityczne, nawet gdy daną sprawą zajmuje się doświadczony oficer. Ustalenie prawdy obiektywnej absorbuje siły, środki, a przede wszystkim czas, więc nietrudno dowieść, że negatywnie wpływa to na bezpieczeństwo. Spreparowane numery mogą również podważyć znaczenie bilingu jako dowodu w procesie sądowym. Aby mieć absolutną pewność co do danych zawartych w raporcie połączeń, należy zestawić dane zawarte w bilingu przychodzącym z danymi z bilingów wychodzących poszczególnych numerów. Przedstawione metody podszywania się pod dowolny numer nie wpływają na wiarygodność bilingu wychodzącego. Każdy przedsiębiorca telekomunikacyjny, również w swoim interesie, skrupulatnie rejestruje połączenia generowane przez abonentów korzystających z zakończeń jego sieci, dlatego biling połączeń wychodzących pozostaje wiarygodnym źródłem informacji. Należy jednak dodać, że jest on dostępny w zasadzie tylko w przy-

padku połączeń generowanych przez abonentów przedsiębiorców telekomunikacyjnych prowadzących działalność na terenie RP[4].

## Dezinformacja niezamierzona

Zdarzają się również sytuacje, kiedy w rejestrze połączeń przychodzących zapisywane są numery inne niż te należące do abonenta inicjującego połączenie bez jego złej woli i, w większości przypadków, bez jego wiedzy. Taka sytuacja występuje podczas stosowania bramek GSM lub wykorzystywania central końcowych do nielegalnego terminowania ruchu międzynarodowego w krajowych sieciach stacjonarnych. Transfer ruchu zagranicznego z pominięciem przeznaczonych do tego międzyoperatorskich łączy telekomunikacyjnych (interkonekt) stanowi podstawową przyczynę pojawiania się fałszywych danych w rejestrach połączeń przychodzących, przez co bardzo negatywnie wpływa na wiarygodność danych zapisywanych w systemach bilingowych. Być może określenie d e z i n f o r m a c j a n i e z a m i e r z o n a jest zbyt eufemistyczne, gdyż podmioty realizujące tego typu usługi wiedzą, że fałszują numer abonenta inicjującego połączenie, i godzą się na to. Jednak nie ulega wątpliwości, że gdyby technologia przekazywania połączeń za pomocą bramek GSM lub systemów konwertujących ruch przesyłany za pośrednictwem internetu do telefonicznych sieci stacjonarnych pozwalała przenosić pierwotny numer abonenta A, to byłoby to powszechnie praktykowane.

Nielegalne kierowanie ruchu zagranicznego bezpośrednio do sieci stacjonarnej wymaga zestawienia łącza o dużej przepustowości do jednego z krajowych operatorów sieci stacjonarnej oraz świadczenia innych usług telekomunikacyjnych pozwalających uzasadnić podpisanie umowy i budowę wspomnianego łącza. Ten sposób nielegalnego terminowania ruchu zagranicznego jest zazwyczaj realizowany przez przedsiębiorców telekomunikacyjnych, którzy wykraczają poza ramy umów podpisanych z operatorami stacjonarnymi, niejako „przemycając" ruch międzynarodowy łączem przeznaczonym do obsługi ruchu lokalnego. W procesie tym prawdziwy numer abonenta A jest zastępowany numerem krajowym z puli numeracji wykupionej przez operatora nielegalnie transferującego ruch lub numerem fikcyjnym, niezwiązanym z żadnym zakończeniem sieci. Przypadki terminowania ruchu „z internetu" bezpośrednio do sieci telefonii stacjonarnej są o wiele rzadsze niż poprzez bramki GSM. Dlatego dalsze rozważania będą dotyczyły przypadków wykorzystywania właśnie tych bramek, zwanych również FCT-ami[5] lub SIMBOX-ami[6]. Należy jednak mieć na uwadze fakt, że w obydwu technologiach nielegalnego transferowania ruchu rezultatem tego procederu jest rejestracja fałszywych danych w bilingu przychodzącym oraz nieprawdziwa informacja pojawiająca się na wyświetlaczu aparatu abonenta B.

U schyłku lat 90. XX wieku nikt nie widział zagrożenia w stosowaniu bramek GSM w centralkach PBX (ang. *Private Branch Exchange*), a sami operatorzy mobilni zachęcali klientów do tego typu rozwiązań. Pozwalało to obniżyć koszt połączeń do sieci mobilnych oraz zapewniało redundantne wyjście do sieci publicznej na wypadek awa-

[4] W niektórych przypadkach można wystąpić w tym zakresie o pomoc do odpowiednich instytucji zagranicznych, ale ze względu na czasochłonność procedur w zestawieniu z krótkim okresem retencji danych, zazwyczaj jest to nieskuteczne.

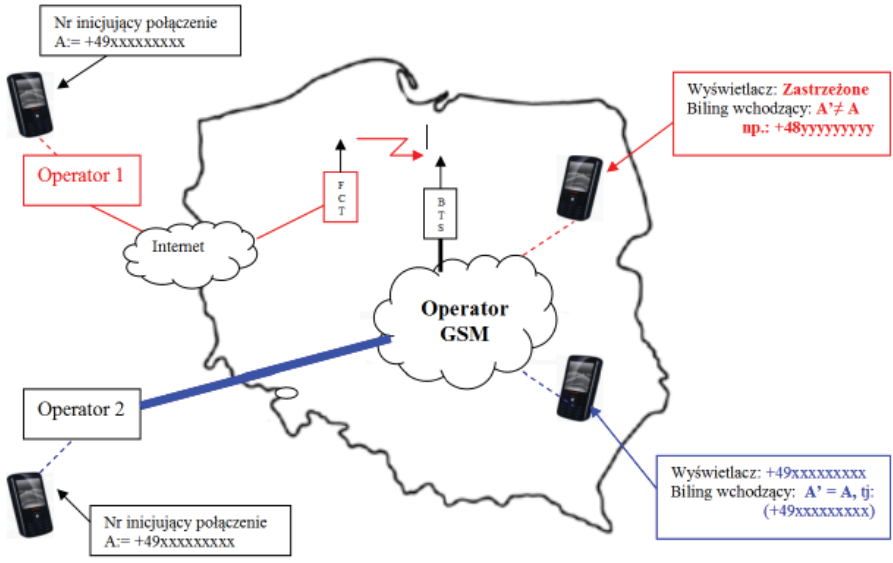
[5] FCT (ang. *Fixed Cellural Terminal*) – stacjonarny terminal komórkowy.

[6] SIMBOX – od nazwy karty SIM (ang. *Subscriber Identity Module*) oraz od ang. słowa *'box'* – skrzynka, czyli urządzenie elektroniczne umożliwiające współpracę z kartami SIM.

rii łącza przewodowego. Tego typu wykorzystanie FCT-ów jest nadal bardzo popularne i powszechnie akceptowane. W takich przypadkach trudno doszukać się jakichkolwiek uchybień prawnych, gdyż w bramkach wykorzystywane są zazwyczaj karty SIM zakupione w ramach umów abonamentowych zawartych z operatorem komórkowym przez podmiot, który za pomocą bramki udostępnia usługi dostępu do sieci mobilnych tylko abonentom wewnętrznym swojej centralki zakładowej. Połączenie z aparatu stacjonarnego na telefon komórkowy zawsze było droższe niż z jednego aparatu komórkowego na drugi, szczególnie gdy te znajdowały się w sieci jednego operatora. Uwzględniając darmowe minuty lub oferowane w niektórych taryfach darmowe połączenia wewnątrz sieci, warto podłączyć do centralki zakładowej np. cztery bramki GSM lub jedno urządzenie FCT z kilkoma kartami SIM, tj. po jednej dla każdego operatora mobilnego.

Ekspansja sieci komórkowych i wprowadzona przez operatorów komórkowych konkurencja cenowa sprawiły, że pojawiły się podmioty, które dostrzegły możliwość zarobkowania na różnicy wysokości stawek pomiędzy połączeniami z sieci stacjonarnej do mobilnej (F2M), a połączeniami wewnątrz sieci mobilnej (M2M). Innym bardzo istotnym czynnikiem dla rozwoju usług terminowania ruchu za pomocą bramek FCT był rozwój technologii VoIP, który dodatkowo pozwolił omijać drogie łącza międzynarodowe.

Najpowszechniejszy model działania przedsiębiorcy terminującego ruch za pomocą FCT-ów przedstawiono na zamieszczonym niżej rysunku.




**Rys. 1. Schemat konwencjonalnej i terminowanej za pomocą FCT-u drogi połączeniowej. Kolorem czerwonym zaznaczono typową drogę połączenia nielegalnie terminowanego za pomocą urządzenia FCT, niebieskim zaś standartową drogę połączenia zestawionego z wykorzystaniem oficjalnych łączy międzyoperatorskich (interkonekt).**

Same urządzenia FCT również ewoluowały od prostego interfejsu pozwalającego podłączyć zwykły telefon komórkowy, poprzez oferowane przez producentów central telefonicznych dedykowane karty z anteną i slotem na kartę SIM, aż po terminale

o dużej przepustowości, umożliwiające obsługę dużej liczby kart SIM. W stosunku do tych ostatnich bardziej pasuje określenie SIMBOX, odróżniające je od prostych urządzeń zwanych bramkami lub ogólnie FCT-ami. Należy jednak zastrzec, że w literaturze brak jednoznacznego potwierdzenia dla takiego podziału nazewnictwa. Najbardziej zaawansowane są serwery SIM, czyli SIMBOX-y, w których oddzielono część radiową urządzenia od pozostałej części obsługującej karty SIM. Na rynku dostępne są serwery wyposażone w oprogramowanie ułatwiające zarządzanie (badanie stanu kont, rotacyjne wykorzystywanie, analiza ruchu) tysiącami kart SIM zainstalowanymi w jednym miejscu. Jako moduły radiowe mogą służyć zwykłe telefony GSM, do których zamiast karty podłączany jest emulator SIM pobierający uprawnienia z kart zainstalowanych w serwerze za pomocą modułu SIM-klient, wykorzystującego protokół transmisyjny TCP/IP (ang. *Transmission Control Protocol/ Internet Protocol*)[7]. Daje to nie tylko możliwość manipulacji numerami (kartami SIM), ale również informacją o położeniu urządzenia końcowego. Zgodnie z przepisami[8] przedsiębiorca telekomunikacyjny musi udostępniać uprawnionym podmiotom informacje dotyczące lokalizacji zakończenia sieci. W przypadku serwerów SIM operator sieci komórkowej zarejestruje geograficzne położenie modułu radiowego, który kontaktował się z pozostającym w jego sieci BTS-em (ang. *Base Transceiver Station*), przy czym sam serwer z kartami SIM może być oddalony o setki kilometrów, gdyż dane z karty SIM niezbędne do logowania się do sieci komórkowej mogą być przesyłane za pomocą sieci WAN (ang. *Wide Area Network*). W takim przypadku operator sieci komórkowej może na przykład zarejestrować połączenie zrealizowane za pośrednictwem BTS-u zlokalizowanego w Warszawie, a już po kilku minutach „ten sam telefon" zaloguje się do BTS-u zlokalizowanego w Krakowie.

Przedstawione wyżej czynniki ekonomiczne i techniczne doprowadziły do pojawienia się na tyle dużej liczby podmiotów obsługujących ruch F2M za pomocą bramek GSM, że zjawisko to stało się dokuczliwe dla dużych operatorów, którzy zaczęli ponosić wymierne straty finansowe. W przypadku operatorów komórkowych zaś zaczęło się to niekorzystnie odbijać na ich wizerunku, gdyż FCT-y mają negatywny wpływ na jakość usług telefonicznych. Najwięksi operatorzy, w trosce o swoje interesy, podjęli różne próby zwalczania tego problemu (poprzez restrykcyjne zapisy w umowach, blokowanie kart *prepaid*, lobbing czy spory sądowe). Skala tego zjawiska była i nadal jest trudna do precyzyjnego określenia, gdyż większość podmiotów terminujących ruch za pomocą FCT-ów w ogóle nie jest zarejestrowana jako przedsiębiorcy telekomunikacyjni i prowadzi działalność niezgodną z przepisami[9]. Problem ten dostrzegł również Urząd Komunikacji Elektronicznej, który w lipcu 2007 r. zajął oficjalne stanowisko[10] i jako podłoże takiego stanu rzeczy wskazał wysokie stawki interkonektowe za zakańczanie ruchu przychodzącego z sieci stacjonarnych do mobilnych oraz dużą dysproporcję pomiędzy stawkami hurtowymi i detalicznymi tych usług. Ponadto Prezes UKE zadeklarował prawną i rynkową analizę problemu oraz zapowiedział organizację debaty

[7] Spośród wielu publikacji na temat protokołu TCP/IP szczególnie interesująca jest publikacja K. S. Siyana i T. Parkera zatytułowana *TCP/IP. Księga eksperta* (wyd. II, Gliwice 2002, Helion).

[8] Wymagania te wynikają z art. art. 180a i 180c *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* (Dz.U. z 2004 r., Nr 171, poz. 1800).

[9] Obowiązek zgłoszenia do rejestru przedsiębiorców telekomunikacyjnych został zawarty w art. 10 wyżej wymienionej ustawy.

[10] Szczegółowe informacje na ten temat można znaleźć w serwisie internetowym UKE: www.uke.gov.pl.

poświęconej korzystaniu z FCT-ów. Debata ta, zatytułowana: *Wykorzystanie urządzeń Fixed Cellular Terminal w połączeniach międzyoperatorskich* odbyła się 19.09.2007 r., a komunikat Prezesa UKE poświęcony jej wynikom oraz wszelkie materiały z tego spotkania zostały udostępnione w Biuletynie Informacji Publicznej UKE[11]. Niezależnie od powyższego, środowisko telekomunikacyjne zarzuca UKE, że nie robi nic, licząc na to, że ponieważ problem FCT-ów maleje, to sam zniknie wraz ze wzrostem konkurencji na rynku telekomunikacyjnym.

Dotychczasowe spory wokół stosowania FCT-ów miały głównie podłoże biznesowe, mało natomiast mówiło się o zagrożeniach dla obronności, bezpieczeństwa państwa oraz bezpieczeństwa publicznego wynikających ze stosowania tych technologii do transferowania ruchu pomiędzy sieciami. Nie oznacza to jednak, że kwestie bezpieczeństwa pozostały niezauważone. Dobrym przykładem może być dostępna w internecie obszerna opinia Artura Kołosowskiego na temat wpływu FCT-ów na realizację zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego[12]. Autor opinii wykazał jednoznacznie, że FCT-y *nie tylko utrudniają, lecz często wręcz uniemożliwiają realizację przez operatorów zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.*

Wracając do użytego w tytule artykułu pojęcia d e z i n f o r m a c j a , trzeba zauważyć, że podmioty wprowadzające ruch do sieci komórkowych za pośrednictwem FCT-ów ukrywają numer za pomocą funkcji CLIR, co oznacza, że abonent B jest „delikatnie oszukiwany", otrzymując informację „numer zastrzeżony", nawet jeśli abonent A udostępnia prezentację numeru. Nie daje to możliwości popełniania przestępstw związanych z podszywaniem się pod inne osoby, ale z punktu widzenia służb zajmujących się obronnością i bezpieczeństwem państwa skutek stosowania FCT-ów niesie takie same zagrożenia, jak wcześniej opisany serwis pozwalający podszywać się pod dowolny numer. Przede wszystkim FCT-y powodują to, że ukrywane są faktyczne kontakty osób wchodzących w zainteresowanie wyżej wymienionych służb (tzw. figurantów) poprzez wprowadzenie złudzenia porozumiewania się z różnymi abonentami. W szczególności ukrywane są stałe kontakty figuranta, gdyż karty SIM podlegają w FCT-ach dużej rotacji, co sprawia, że kolejne połączenia inicjowane z tego samego numeru A będą rejestrowane w bilingu przychodzącym abonenta B jako różne numery. Połączenia zagraniczne terminowane za pomocą FCT-ów są zawsze rejestrowane w bilingach operatorów mobilnych jako krajowe. Ułatwia to osobom zaangażowanym w szpiegostwo oraz działalność terrorystyczną ukrywanie kontaktów zagranicznych. Należy również wspomnieć o pośrednich zagrożeniach wynikających z wiązania sił i środków służb oraz o wyżej opisanej deprecjacji bilingu jako dowodu w sprawie sądowej.

## Podsumowanie

W artykule tym przedstawiono najbardziej powszechne sposoby wprowadzania do obiegu telekomunikacyjnego mylących informacji o numerach inicjujących połączenie. Opisana działalność często jest niezgodna z obowiązującym prawem i może

[11] Tamże.

[12] Zob.: http://www.piit.org.pl/_gAllery/73/71/7371/20080418_Opinia_FCT_2008.04.16.pdf.

ułatwiać popełnianie przestępstw, powodować uszczuplanie dochodów u niektórych przedsiębiorców telekomunikacyjnych, obniżać jakość usług telekomunikacyjnych, ale przede wszystkim niesie realne zagrożenia dla bezpieczeństwa państwa. Dlatego należy zwalczać wszelkie formy działalności pozwalające na podszywanie się pod innego abonenta podczas korzystania z usług telekomunikacyjnych. Jak wynika z opisanego przykładu, polski system prawny posiada narzędzia pozwalające skutecznie walczyć z serwisami oficjalnie oferującymi usługę podmiany numeru. Walka z terminowaniem ruchu za pomocą FCT-ów na pozór również wydaje się prosta, ponieważ przepisy regulujące działalność telekomunikacyjną[13] zabraniają nieuprawnionego przetwarzania danych transmisyjnych. Informacja adresowa o numerze abonenta A i B nie powinna być zmieniana na całej drodze połączeniowej. W praktyce sprawa jest o wiele bardziej skomplikowana, gdyż większość podmiotów transferujących ruch za pomocą FCT-ów nie jest zarejestrowana w prowadzonym przez UKE rejestrze przedsiębiorców telekomunikacyjnych, a więc nie mogą one być kontrolowane i ewentualnie karane przez ten organ. Ponadto, w odróżnieniu od serwisów oferujących *spoofing*, przedsiębiorcy transferujący ruch za pomocą FCT-ów nie rozgłaszają swojej działalności, a częsta zmiana anonimowych kart SIM (*prepaid*) sprawia, że ich działalność jest niemal niezauważalna. Podmioty te mogłyby być ścigane na zasadach ogólnych za przestępstwo z art. 268 § 1 kk, ale w tym przypadku ściganie następuje na wniosek pokrzywdzonego. I tu rodzi się pytanie: kto powinien wnioskować o ukaranie sprawcy? Obywatel, który na wyświetlaczu telefonu nie widział numeru rozmówcy, a jakość połączenia pozostawiała wiele do życzenia? Służba, która została wprowadzona w błąd i nie zdołała zapobiec popełnieniu przestępstwa bądź wykryciu sprawcy? Czy raczej państwo lub społeczeństwo, które doznało krzywdy na skutek, na przykład, zamachu terrorystycznego?

Agencja Bezpieczeństwa Wewnętrznego przeprowadziła cykl konsultacji z innymi służbami odpowiedzialnymi za bezpieczeństwo państwa oraz bezpieczeństwo i porządek publiczny, największymi przedsiębiorcami telekomunikacyjnymi oraz Urzędem Komunikacji Elektronicznej w celu wypracowania rozwiązań pozwalających na zminimalizowanie zagrożenia wynikającego ze stosowania FCT-ów. Obecnie prowadzone są konsultacje z Ministerstwem Infrastruktury poświęcone ocenie możliwych do wprowadzenia zmian prawnych pozwalających skuteczniej zwalczać wszelkie formy podmiany numerów stron połączenia telefonicznego.

Z punktu widzenia służb odpowiedzialnych za bezpieczeństwo państwa działalność telekomunikacyjna powinna być prowadzona tak, aby w razie potrzeby uprawnione podmioty mogły zidentyfikować strony połączenia, uwzględniając uwarunkowania prawne, w szczególności okres retencji danych stowarzyszonych ze świadczonymi usługami telekomunikacyjnymi.

[13] Zagadnienie to zostało uregulowane w art. 31 i 126 wymienianej już *Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* oraz doprecyzowane w wydanym na jej podstawie *Rozporządzeniu Ministra Infrastruktury z dnia 9 stycznia 2008 r. w sprawie szczegółowych wymagań dotyczących zasad adresowania dla właściwego kierowania połączeń* (Dz.U. z 2008 r., Nr 14, poz. 84).

## Streszczenie

Artykuł podejmuje temat wiarygodności danych identyfikujących zakończenia sieci telekomunikacyjnych, z których inicjowane są połączenia. Przedstawiono w nim przypadki i najbardziej typowe sposoby nieuprawnionej modyfikacji tych danych. Szczególny nacisk położono na zagadnienia związane z nielegalnym terminowaniem ruchu za pomocą bramek GSM, tzw. FCT-ów (*Fixed Cellular Terminal*). Autor przedstawia i uzasadnia tezę, iż tego typu działalność rodzi zagrożenia dla bezpieczeństwa państwa oraz wskazuje na konieczność podjęcia działań zmierzających do wyeliminowania wszelkich przypadków modyfikacji danych adresowych związanych z przesyłanymi przekazami telekomunikacyjnymi.

## Abstract

The article addresses the issue of reliability of data related to the telecommunication network endpoints, acting as the points of origin of the connection. Cases and the most typical methods of unauthorized modification of this data are presented in the article. Particular emphasis was put on the illegitimate telecommunication traffic termination with the FCT (Fixed Cellular Terminal) GSM gates. The author presents and justifies the thesis that such activity poses threat to the state security, that is why appropriate countermeasures should be taken to eliminate and prevent all illegitimate modification of address data related to telecommunication transfers.