Maciej A. Kędzierski

Sieciowość współczesnych organizacji przestępczych funkcjonujących w obszarze przestępczości zorganizowanej i terroryzmu

Tradycyjne podejście do budowania struktur przestępczych jest oparte na ich hierarchicznej strukturze wewnętrznej, składającej się z centrum decyzyjnego (kierownictwa), pośredniego szczebla zarządzania oraz wykonawców (określanych także jako „żołnierze"), znajdujących się najniżej w hierarchii grupy przestępczej (zobrazowanej najczęściej w graficznej formie triangulacji). W takim sposobie patrzenia na organizacje przestępcze zakłada się, że funkcjonują one na zasadach: bezwzględnych, utrzymanych w hierarchicznej strukturze relacji, realizacji zleceń, minimalnych odchyleń od zakładanych celów kryminalnych, koordynacji działań wynikających ze ścisłego podziału pracy i precyzyjnych wspólnych wytycznych. Wszystkie podane cechy są konieczne do skutecznego osiągnięcia celów przez organizację, zapewnienia bezpieczeństwa organizacji i jej członkom oraz wprowadzenia wewnętrznej kontroli organizacji.

Alternatywą wobec organizacji typu hierarchicznego są **sieci przestępcze** (traktowane jako **sieci rzeczywiste/złożone**). Jest to struktura rozproszona, elastyczna, składająca się z wielu elementów (zwanych też węzłami lub ogniwami), którymi są osoby lub grupy osób, wraz z odnoszącymi się do nich wzajemnymi, dwustronnymi lub wielostronnymi, relacjami o charakterze przestępczym lub gospodarczym. Elementy te nie są powiązane w sposób stały, ale współpracują z sobą na zasadzie doboru, uwzględniając posiadane umiejętności lub możliwości finansowe. Doboru takiego dokonuje się pod kątem konkretnego zadania (przestępstwa) bądź też krótkich horyzontów czasowych[1].

Struktura sieciowa organizacji przestępczych od wielu lat przysparza organom ścigania wielu problemów związanych nie tylko z określeniem jej budowy wewnętrznej, przypisaniem skali odpowiedzialności poszczególnym członkom organizacji (węzłom sieci), lecz także z precyzyjnym wytypowaniem struktury z całości relacji społecznych[2]. Problemem jest także określenie, w jaki sposób i jakie reguły kierują doborem nowych węzłów w sieciach przestępczych, przyjęciem zasad wzajemnego sterowania czy rozliczania z realizacji zakładanych celów (ustaleniem klucza do poszukiwanie partnerów z zamiarem popełniania przestępstw). Odpowiedź na poszczególne pytania usiłuje się uzyskać przez analizę relacji zachodzących między węzłami organizacji przestępczych typu sieciowego.

---

[1] W. Filipkowski, *Przestępczość zorganizowana – ujecie prawne i kryminologiczne*, „Prokuratura i Prawo" 2006, nr 12, s. 67.

[2] K. Harężlak i M. Kozielski posługują się pojęciem sieci kryminalnej, określając ją jako: *trwały związek przestępców z luźną strukturą hierarchiczną, obejmującą swoim zakresem zarówno sieci funkcjonujące jako kartele, takie, które przypominają związki handlowe, oraz te, które zapewniają utrzymanie prostych kontaktów między jej członkami,* w: K. Harężlak, M. Kozielski, *Metody analizy sieci kryminalnych*, „Studia Informatica" 2010, nr 2A (89), s. 35–36. Zorganizowane sieci przestępcze (ang. *organised criminal network*) zostały określone przez Center for International Crime Prevention przy Narodach Zjednoczonych jako forma, w której: *osoby indywidualne podejmują wspólnie przestępczą działalność w często zmieniających się konfiguracjach personalnych; nie muszą uważać się za jedną, stałą grupę; ich pozycja i udział zależy od ich predyspozycji, umiejętności lub kapitału, jaki mogą wnieść do przedsięwzięcia; należy podkreślić, że są to zwykle – znani w środowisku – zawodowi przestępcy*, w: W. Filipkowski; *Przestępczość…*, s. 65.

Istotnym elementem prowadzenia analiz tych struktur jest przede wszystkim przyjęty wewnętrznie sposób organizowania się w celu popełniania przestępstw powstający z przekształcenia się z poziomu hierarchiczności na poziom sieci (struktur płaskich). Takie rozwiązania organizacyjne powinno być widoczne głównie w obszarze przestępczości finansowej, popełniania przestępstw w cyberprzestrzeni i przestępczości gospodarczej[3]. W tych obszarach następuje zgodna kreacja postaw przestępczych przy wykorzystaniu nowoczesnych instrumentów usług i przepływów środków finansowych oraz najnowszych technik przekazu (którego przedmiotem mogą być środki finansowe lub informacje) na odległość. Zachodzące zmiany powodują przechodzenie z zachowań opartych na zasadzie własności i podporządkowania do zachowań polegających na czerpaniu korzyści z przepływu usług i łączenia zasobów zewnętrznych przez sieć w nowe wartości[4]. Nowe rozwiązania stosowane przy organizowaniu przestępstw nie wymuszają tworzenia tradycyjnych sposobów budowania infrastruktury organizacyjnej, istnienia quasi-przedsiębiorstw kryminalnych, a jedynie odnalezienia bezpiecznego zbioru instrumentariów na potrzeby wykonawcze i ograniczonego nadzoru koordynacyjno-kierowniczego nad działaniami wykonawczymi (do tego rodzaju zachowań będzie można zaliczyć tworzenie sieci przestępczych i budowanie relacji między węzłami)[5].

Wzajemne „uczenie się" organizacji terrorystycznych i kryminalnych doprowadziło do wykreowania takich struktur, w których poszczególne elementy organizacyjne stają się bardziej anonimowe, a utrata jednego z węzłów nie destabilizuje całości organizacji. Pozwala to na dalsze skuteczne realizowanie wyznaczonego celu przestępczego. Przy tego typu konstrukcjach funkcjonowanie organizacji nie wymaga stałej aktywności przywództwa i prowadzenia bieżącego nadzoru nad wykonawstwem. Na taki sposób budowania struktur organizacyjnych, służących popełnianiu przestępstw, znaczny wpływ miały następujące czynniki: globalizacja zachowań przestępczych, ukształtowanie się i wprowadzenie do powszechnej struktury sieciowej obrotu finansowego, stworzenie nowoczesnych technik szybkiego przepływu informacji, a także znalezienie bezpiecznych sposobów zapewniających trwałość organizacyjną i izolację od wpływu organów ścigania.

Instrumenty elektroniczne przydatne w zrzeszaniu się anonimowych wobec siebie osób, wymiany informacji, prowadzenia dyskusji na takich forach, jak: blogi, Skype'y, aukcje, zakładanie kont w e-bankach czy świadczenie usług w e-urzędach, stały się także elementem wykorzystywanym przez organizacje kryminalne. W praktyce mamy więc do czynienia z warstwowaniem się (nakładaniem się) różnych sieciowych relacji wynikających z umieszczenia sieci przestępczych w szeroko rozumianych sieciach społecznych (rodzinnych, finansowych, biznesowych, religijnych, państwowych, samorządowych itp.). Dlatego też legalne sieci społeczne stają się kamuflażem dla sieci przestępczych. Tym samym do czynników wpływających na nową jakość przestępczości należałoby

[3] Cecha ta wiąże się z oferowaniem znacznej ilości i różnorodności instrumentów służących zgodnemu z prawem wspieraniu rozwoju obrotu kapitałowego.

[4] W. Kurowski, *Globalna gospodarka usług przestępczych,* w: wkład do badań statutowych SGH pt.: *Serwicyzacja gospodarki jako szansa przyspieszenia wzrostu konkurencyjności przedsiębiorstw w Polsce,* oprac. zbior. pod kier. nauk. A. Hermana, SGH, Warszawa 2009, s. 3.

[5] W dokumentach międzynarodowych definiujących „grupę terrorystyczną" mówi się o „ustrukturalizowanej" organizacji. Termin „ustrukturalizowana" (ang. *association structure*) wyjaśnia się przez zaprzeczenie, jakich cech organizacja taka nie musi posiadać. Nie jest to więc z jednej strony organizacja, którą zawiązuje się przez przypadek, w celu natychmiastowego popełnienia przestępstwa. Z drugiej jednak strony nie musi ona posiadać formalnie określonych ról poszczególnych jej członków, stałego składu oraz opracowanej struktury, zob. E. Zielińska, *Zwalczanie terroryzmu – standardy europejskie*, Warszawa 2002, Instytut Wymiaru Sprawiedliwości, s. 9–10.

zaliczyć wszechobecność w społeczeństwie różnych rozwiązań dotyczących sieci teleinformatycznych i społecznych wzajemnego komunikowania się, ale też zabawy, spotkania towarzyskie, doskonalenie zawodowe czy bieżące realizowanie zadań na poziomie obsługi obywateli i utrzymywania struktur państwowych. Relacje występujące głównie w tzw. małych światach powstają przede wszystkim pod wpływem osobistych kontaktów. Budowanie sieci przestępczej jest więc możliwe dzięki relacjom nawiązywanym podczas wspólnego przebywania w określonym miejscu i w tym samym czasie (szkoła, dzielnica, wspólne zainteresowania, praca itp.).

Obecnie nie jest już żadnym zaskoczeniem, że przestępstwa są popełnianie anonimowo wyłącznie w sieciach informatycznych, dzięki czemu uzyskuje się znaczne środki finansowe. Szybko zmieniające się otoczenie technologiczne stale implikuje zmiany strategii i taktyki działania zorganizowanych grup przestępczych działających w tym obszarze. Zagrożenie wzrasta również z tego powodu, że na sieci organizacyjne grup przestępczych czy organizacji terrorystycznych nałożyły się sieci teleinformatyczne, które służą im jako instrumenty technicznego wsparcia. Dzięki nim, zwłaszcza grupom kryminalnym, zostaje zapewniony warunek anonimizacji zachowań indywidualnych (członków) i zespołowych (organizacji, w której pozostają aktywni). Słusznie wypowiada się M. Whine stwierdzając, że: *nowe technologie medialne umożliwiają przejście od „bezwzględnych hierarchii do sieci"*.[6]

Omawiane zmiany organizacyjne w znacznej mierze pozwalają wyeliminować zagrożenie wynikające ze słabości organizacji opartej wyłącznie na czynniku ludzkim[7]. Nowe środowisko sprzyja tworzeniu nie tylko organizacji kryminalnych, lecz także międzynarodowych sieci, których podstawą są lokalne grupy terrorystyczne. W rzeczywistości nie ma już czegoś takiego jak lokalne grupy terrorystyczne lub miejscowe zagrożenia terrorystyczne. Lokalne zagrożenie terrorystyczne jest teraz nie tylko regionalne, ale ma także charakter globalny[8]. Oprócz tego sama budowa sieci terrorystycznych ma przynajmniej dwa wymiary: duchowy (inspiracyjny pod względem idei działania) oraz wykonawczy (w celu spełnienia założonej idei, np. przez dokonywanie aktów terrorystycznych). Budowa sieciowa ma spowodować większą sprawność działania (osiągnięcie celu) przy jednoczesnym zapewnieniu bezpieczeństwa organizatorów (trwałości struktury w czasie). Zachowanie takiej konstrukcji nie wymaga ciągłego kontrowania zachowań poszczególnych członów odpowiedzialnych za wykonawstwo. Przywództwo organizacji dostarcza jedynie motywacji do aktywności przestępczej[9]. Kierownictwo staje się więc nie bezpośrednim nadzorcą, ale doradcą lub cichym udziałowcem odpowiedzialnym za planowanie przedsięwzięć, kreowanie nowych „pomysłów" mających wpływ na taktykę (ewentualnie jej zmianę) i kierunek działań przestępczych. Pomiędzy nim a wykonawcami powiększa się dystans informacji, wiedzy i znajomości.

Z punktu widzenia przyjętego podziału sieci zorganizowane grupy przestępcze i organizacje terrorystyczne powinny być traktowane w kategorii **sieci deterministycz-**

[6] M. Whine, *Cyberspace - A New Medium for Communication, Command, and Control*, „Studies in Conflict and Terrorism" 1999, nr 22, 231–45.

[7] Należałoby się zastanowić, na ile dzisiejsze rozwiązania stosowane przez organy ścigania, np. instytucja świadka koronnego, będą skuteczne w sieciach przestępczych.

[8] S. Tekwani; *The LTTE's Online Network and its Implications for Regional Security*, Singapore 2006, Nanyang Technological University, s. 7

[9] Zob. D. Penzar, A. Srbljinović, *About modelling of complex networks with applications to terrorist group modelling*, „Interdisciplinary Description of Complex Systems" 2005, nr 3 (1), s. 31.

nych, niezakładających elementu losowości, a złożoność strukturalnego funkcjonowania. Wynika to między innymi z potrzeby zapewnienia sprawności organizatorskiej, zaufania i zapewnienia bezpieczeństwa uczestników.

W strukturze sieciowej można wyróżnić dwa obszary. Pierwszy z nich jest związany z technicznym dokonywaniem przestępstw. Jest to wspomniany obszar sieci informatycznych, przepływu informacji, rozliczeń finansowych, telekomunikacji itp. Drugi obszar jest związany z kształtowaniem się sieci kryminalnych pod kątem organizacyjnym (obszar przynależności personalnej) w ramach sieci społecznych. Wyróżnia się tu płaszczyznę struktury fizycznej osób pozostających pomiędzy sobą w sieciowej konfiguracji kryminalnej oraz płaszczyznę technologiczną, budowaną zarówno na czynniku ludzkim, jak i na dostępności do urządzeń informatycznych czy telekomunikacyjnych. Ten drugi obszar jest wymuszany nie tylko pierwszym (dokonywaniem przestępstw), lecz także zmieniającą się rzeczywistością społeczną, ucieczką od nadzoru oraz realizowaniem potrzeb organizacyjnych związanych z generowaniem realnych zysków finansowych. Stąd też sieci przestępcze będzie można zaliczyć do **sieci ewoluujących** zarówno w czasie, jak i pod kątem ich struktury.

Organizacje przestępcze wkomponowane w funkcjonowanie poszczególnych kategorii podmiotów dążą do wypracowania nie tylko sieciowego podejścia do budowy organizacyjnej, lecz także do taktyki prowadzonych działań przestępczych. Analiza ich zachowań jest coraz częściej dokonywana na podstawie oceny sieci przestępczych, mimo że część z nich ma hierarchiczną budowę (dotyczy to także organizacji hybrydowych hierarchiczno-sieciowych). Z myślą o bezpieczeństwie społecznym taki stan rzeczy wymusza na organach ścigania stworzenie sposobu uniwersalnego porozumiewania się, przygotowywania procesów decyzyjnych, świadczenia usług urzędniczych i handlowych, obrotu towarowego i korporacyjności finansowej. Stąd też istnieje potrzeba nowego podejścia do oceny funkcjonowania organizacji przestępczych, gdzie należałoby na nie patrzeć jako na sieci, a nie na hierarchicznie zbudowane struktury. Taki też powinien być dalszy kierunek rozwoju analizy struktur zorganizowanych, niewykluczających w swojej budowie także hierarchicznego sieciowego podejścia[10]. Ponadto podejście takie jest ważnym elementem analizy i badań relacji zachodzących na styku: organizacja przestępcza–otoczenie tej organizacji, zwłaszcza, że coraz bardziej, w ocenie społecznej, granica ta zanika.

Trudności w definiowaniu sieci przestępczych powodują dalsze problemy związane chociażby z określaniem odpowiedzialności karnej poszczególnych jej uczestników. Klasyczne podejście do ustalania odpowiedzialności członka grupy lub kierującego grupą przestępczą zaczyna nie wytrzymywać próby czasu. Dotychczasowe, tradycyjne podejście odnosiło się głównie do strony sprawczej czynu: zakładania, kierowania i działania w organizacji przestępczej. W takiej organizacji widziano przede wszystkim jej zhierarchizowaną strukturę, jasno określoną rolę i relacje występujące między kierownictwem a wykonawcami. Stąd też w ostatnim czasie organy ścigania aktywizują zawodową dyskusję o trudnościach z subsumcją (procesem klasyfikacji prawnej – przyp. red.) zarzutów wobec określonych zachowań podmiotów, będących uczestnikami sieci przestępczych. Jednak mimo przyjęcia sieciowych rozwiązań wewnątrz or-

[10] P. Klerks, *The Network Paradigm Applied to Criminal Organisations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands*, Hague 1999, Eysink Smeets & Etman Autor dokonał oceny podejścia analitycznego sieciowego na podstawie doświadczeń holenderskich służb zajmujących się zwalczaniem przestępczości.

ganizacji przestępczej, nie traci ona samej idei powstania, którą jest działanie w celu wytwarzania zysków przestępczych (zachowanie celu). Stąd też mimo bardziej rozmytej i spłaszczonej struktury organizacyjnej, nadal można odnaleźć w niej te elementy, które były wyróżnione w klasycznym podejściu. Polega to na wyodrębnieniu osób, które stają się „ofiarami" w otoczeniu sieci i „odbiorcami zysków" w ramach sieci, z tych, którzy taką rolę im przypisują.

Jak już wspomniano na powszechnie występujące „usieciowienie społeczne" nałożyły się także podobne struktury kryminalne. Istotnym wyznacznikiem jest jednak to, jak spośród sieci społecznej wyróżnić sieć struktury kryminalnej i co uznać za jej zindywidualizowane (wyróżniające) cechy. Wbrew trudnościom zanalizowania tego rodzaju zachowań należy zauważyć, że w związku z rozszerzaniem się społeczeństwa informatycznego i przenoszeniem usług i obsługi obrotu towarowego i finansowego do obszaru teleinformatycznego, będzie można pozyskiwać coraz to nowe „ślady" kryminalnej działalności przestępców sieciowych.

Podstawowym problemem związanym z analizą sieci pozostaje sama jej konstrukcja. W przypadku sieci społecznych (do których zaliczono także sieci przestępcze), wskazuje się na następujące trudności:

- niekompletność – mimo staranności przeprowadzonej analizy, zawsze pozostają węzły i połączenia niewidoczne dla analityka,
- płynne granice – czyli trudności w określeniu, kogo należy uwzględnić w sieci,
- dynamika – sieci społeczne wciąż podlegają zmianom[11].

Nie ulega wątpliwości, że podobne problemy występują także przy typowaniu struktur przestępczych, w tym o budowie sieciowej. Pewnym rozwiązaniem doprecyzowującym elementy sieci jest możliwość zastosowania metody systemowej do działań rozpoznawczych[12]. Należy jednak pamiętać, że granica między systemem a jego otoczeniem jest granicą sztuczną[13]. Zewnętrzny obserwator może jedynie ocenić, co należy do systemu, a co pozostaje w jego otoczeniu. W rzeczywistości sieci przestępcze, działając równolegle do sieci społecznych „nieprzestępczych", stwarzają więcej problemów związanych z ustaleniem struktury niż grupy tradycyjne (hierarchiczne). Wykorzystywane przez grupy przestępcze możliwości technologiczne pozwalają na stanie się potencjalną ofiarą w sposób automatyczny, np. przez wejście na stronę internetową pozorującą legalne działanie. Podobnie można interpretować pozostawanie członkiem takiej sieci – osoba stawia się w roli potencjalnego sprawcy np. gdy przegląda strony internetowe o treści pedofilskiej. Dlatego też należałoby się zastanowić, czy zamiast poszukiwać całości struktury, nie należałoby odnajdywać w niej jedynie te istotne elementy, które stanowią o jej rdzeniu (bezpieczeństwie rdzenia), istotnych węzłach przejściowych (strategicznych) oraz o bezpośrednim wykonawstwie (relacja: członek sieci–wykorzystany element otoczenia). Rodzi się pytanie, jak dalece można uogólniać strukturę i jakie przyjąć kryteria, tak aby przy zachowanej tożsamości organizacyjnej nie pominąć węzłów istotnych z punktu widzenia typowania zachowań: zakładania, kierowania i wykonawstwa w sieci przestępczej. Wyniki analiz nawet nie w pełni wiarygodnych sieci mogą przy-

[11] A. Fronczak, P. Fronczak, *Świat sieci złożonych. Od fizyki do Internetu*., Warszawa 2009, Wydawnictwo Naukowe PWN, s. 227, wraz z powołaną literaturą.

[12] Zob. M. Mazur, *Pojęcie systemu i rygory jego stosowania,* „Postępy Cybernetyki" 1987, z. 2, s. 21–29, numer w całości poświęcony Marianowi Mazurowi.

[13] Z. Biniek, *Elementy teorii systemów modelowania i symulacji* [online], skrypt akademicki wydanie III internetowe, Wydawnictwo INFOPLAN, Szczecin 2002, s. 7–8, www.finus.com.pl [dostęp: 28 I 2014].

nieść wiele cennych informacji[14]. Pewnym rozwiązaniem jest wprowadzenie **uproszczonego modelu sieci**. Warto zaznaczyć, że na podstawie uproszczonego modelu sieci można prowadzić badania układu sieciowego znajdującego się w różnych sytuacjach.

Elementem dodatkowym typowania istotnych węzłów sieci pozostaje oderwanie się od oceny opartej na intuicji i doświadczeniu na rzecz matematycznych wzorów wyliczeń. Podstawą każdego z prezentowanych modeli sieciowych są wzory matematyczne pozwalające na ocenę relacji zachodzących w ramach badanej struktury. Nie można jednak interpretować sieci przestępczej jedynie jako technicznego i automatycznego wykonawstwa, to raczej wyrafinowane narzędzie użyte w procesie intelektualnym organizatora (elementu sprawczego) pozwalające na bardziej bezpieczne i optymalne osiąganie założonego celu działania. Sieci te, zwłaszcza terrorystyczne, są charakteryzowane w literaturze fachowej w kategorii nieredukowalnej złożoności i niejednoznaczności[15]**.** Nie ulega jednak wątpliwości, że w przypadku zarówno sieci przestępczych, jak i terrorystycznych, mamy do czynienia z klasyfikacją ich jako **rzeczywistych sieci złożonych**. Zastosowanie w analizie stałych wzorów jest trudne do zrealizowania, niemniej jednak nie niemożliwe w odniesieniu do oceny danego układu (lub jego części).

Dzięki analizie sieci przestępczych można uzyskać określone rodzaje informacji, odmienne od poszukiwanych w celu rozpoznania tradycyjnych organizacji przestępczych. Takie podejście pomoże w uzyskaniu odpowiedzi na podstawowe pytania:

- jaką rolę odgrywają organizatorzy sieci przestępczych i jak zapewnić ich ustalenie,
- jakie są mechanizmy wymiany ról odgrywanych w ramach sieci przestępczej,
- jakie węzły uznaje się za strategiczne, których usunięcie spowoduje osłabienie lub ustanie działalności sieci przestępczej,
- jakie cechy będzie można nadać poszczególnym węzłom na podstawie oceny ich relacji między sobą i z innymi węzłami sieci (podmiotami otoczenia sieci) – wprowadzenie skalowania siły węzłów[16],
- jaki jest rodzaj grupowania w sieci (budowania silnych węzłów), co stanowi o sposobie zarządzania siecią,
- w jaki sposób odbywa się przepływ informacji i finansów w sieci (ustalenie celów identyfikacyjnych poszczególnych węzłów),
- jakiego rodzaju odwzorowaniem zachowań elementów jest sama sieć,
- jak ustalić, w miarę możliwości, identyfikację całości organizacyjnej sieci[17] (przez wskazanie jej istotnych elementów, tj. takich, bez których sieć nie będzie mogła realizować wyznaczonego celu).

Specyfiką analizowania sieci organizacyjnych jest badanie relacji zachodzących między elementami. Analitycy zdobywają w ten sposób informacje o organizacji (o jej budowie) oraz roli, jaką odgrywają w niej poszczególne elementy strukturalne. Dlatego też istotnym elementem w sieci są węzły jako „łączenia" wchodzące w relacje z pozostałymi węzłami w sieci. Ocena każdego węzła jest oceną jego roli w sieci oraz jego stop-

[14] A. Fronczak, P. Fronczak; *Świat sieci złożonych*…, s. 227. Autorzy jako przykład takich analiz przywołują system COPLINK wykorzystywany w pracy wydziału policji w Tucson w Stanach Zjednoczonych.

[15] V. Fellman, R. Wright, *Modeling Terrorist Networks – Complex Systems at the Mid-Rang*, Proceedings of the Complexity, Ethics and Creativity Conference, London, s. 4.

[16] Na przykład przy zastosowaniu macierzy wpływów, zob. A. Piekarczyk, K. Zieniewicz, *Myślenie sieciowe w teorii i praktyce*, Warszawa 2010, Polskie Wydawnictwo Ekonomiczne, s. 60. Sposób działania został przedstawiony na podstawie metodyki zaproponowanej przez H. Ulricha i G.J.B. Probsta.

[17] K. Harężlak, M. Kozielski, *Metody analizy sieci kryminalnych*..., s. 36.

nia aktywności w osiąganiu celu przestępczego (zindywidualizowane wartościowanie węzłów spełniania się w sieci). Zmienność sieci w czasie będzie wymagała także oceny, w jakiej fazie działania sieć się znajduje (spoczynku czy aktywności), co będzie także wpływało na ocenę aktualnej struktury sieci.

Jako sieć należałoby potraktować zbiór wierzchołków połączonych krawędziami. Wierzchołkami mogą być: osoba, komputer bądź też numer telefonu. Inaczej mówiąc, wierzchołek to określony obiekt w konstrukcji sieci, a połączenia między wierzchołkami określają zachodzące między nimi relacje. Wierzchołkami sieci przestępczych będą poszczególni jej członkowie, użytkownicy sieci teleinformatycznych (jako uczestnicy „gry przestępczej"), rzeczy, którymi się posługują czy miejsca, w których planują działania przestępcze. Krawędzią jest uznanie organizacyjnej przynależności do sieci lub świadomy udział w „grze przestępczej", a także elementy rzeczowe, jakimi się te osoby posługują. W związku z tym, że relacje: osoba–rzecz niejednokrotnie nie są związane z popełnianiem przestępstw, analityk musi patrzeć na członka organizacji przestępczej o budowie sieciowej znacznie szerzej – także przez jego umiejscowienie w społeczeństwie. Samo uznanie, że jest się członkiem sieci, jest już możliwe przez bycie w tej sieci, wyrażając na przykład zgodę na przystąpienie do niej. Przy bardziej tradycyjnym podejściu do sieci jako jedynie spersonalizowanej organizacji przestępczej krawędzią będzie wymóg uznania przez organizatora sieci danej osoby za członka organizacji przestępczej (z wszystkimi dla niej konsekwencjami, np. dokonywaniem przestępstw jedynie w ramach organizacji, zgodnie z przyjętym wewnętrznym sposobem postępowania). Działanie członka w sieci przestępczej będzie się nakładało na aktywność tej osoby w sieci społecznej (obszarze niezwiązanym z popełnianiem przestępstw). Stąd też należy wyselekcjonować tego typu zachowania, aby można było ocenić „czysty" obraz aktywności przestępczej. W przypadku struktury sieciowej organizacji przestępczych możliwe jest występowanie węzłów o podwójnej roli – zarówno „ofiary", jak i „sprawcy".

Sieci są przedstawiane w postaci **grafów będących zbiorem węzłów (wierzchołków) i połączeń między nimi[18].** Każdej krawędzi będzie można przyporządkować jakąś wartość (wagę), co w ostateczności daje wersję grafu ważonego. Stopień wierzchołka to liczba bezpośrednich połączeń (krawędzi) danego węzła z innymi wierzchołkami w sieci. Określanie stopnia wierzchołka jest pomocne przy badaniach jego centralności w sieci oraz wskazuje, jak relacje z innymi węzłami sieci wpływają na jego umiejscowienie w całości sieci. Dodatkowo dzięki wiedzy na temat stopni poszczególnych wierzchołków w sieci będzie można uzyskać informacje na temat rozkładu stopni węzłów, co z kolei umożliwia określenie zróżnicowanej roli węzłów w sieci oraz mechanizmów występujących w sieci oraz nią kierujących.

Konstrukcje sieci przestępczych można określić jako: klasyczny graf losowy Erdosa-Renyiego, **graf losowy z ustalonym rozkładem stopni wierzchołków**, **sieć „małych światów"** (*small-world net-works* Wattsa i Strogatza) czy **sieć Barabasiego-Alberta**. W odniesieniu do analizy zachowań i przeciwdziałania funkcjonowaniu sieci przestępczych chodzi nie tyle o ustalanie nowych konfiguracji modelowych, ile o zbadanie, czy rozpoznawana struktura nie jest podobna po przedstawionych modeli, a w ostateczności, jak obrać właściwą taktykę postępowania przy modelowaniu usterek i przygotowywaniu ataków na tak przedstawione sieci (patrz: teoria perkolacji[19]). Róż-

[18] Innym sposobem prezentowania danych są macierze.

[19] Termin perkolacja (przeciekanie) został stworzony w 1957 r. przez matematyka J.M. Hammersleya. Pracował on nad przepływem płynu przez sieć kanałów, w której część kanałów może być przypadkowo za-

nica w poszczególnych sieciach przestępczych będzie wynikała z tego, czy inicjator[20] ich powstania będzie przewidywał utrzymanie klasycznej struktury sieci bez przyłączania dodatkowych węzłów, czy raczej będzie przewidywał rozwój sieci w czasie. W tym drugim przypadku przedmiotem oceny będzie sposób przyłączania i grupowania się nowych węzłów w stosunku do już istniejących. Dodatkowym obszarem będą relacje zachodzące w statycznej lub ewoluującej sieci przestępczej, dzięki którym będzie można ustalić: sposób przepływu informacji i towarów, zdolność do adaptacji i uczenia się sieci, występowanie luk organizacyjnych, słabych węzłów oraz węzłów strategicznych.

Informacja o topologii sieci ma szerokie zastosowanie w praktyce. Przedstawianie rzeczywistych kontaktów i znajomość liczby połączeń odchodzących od każdego węzła są w dzisiejszych czasach coraz bardziej cenione, chociażby ze względu na częstsze wykorzystanie zgromadzonej wiedzy podczas rozwiązywania problemów w ujęciu strategicznym i planistycznym[21]. W tym również prowadzenia walki z różnymi organizacyjnymi formami przestępczości.

Typowanie struktury sieciowej

Ważnym elementem przy ustalaniu struktury sieci jest badanie relacji zachodzących między jej węzłami. Relacje te można podzielić następująco:

- odwzajemnione – występują głównie w małej grupie o charakterze stabilnym, mogą także występować w czasie bezpośredniego przygotowania do dokonania przestępstwa. Skracają okres decyzyjny, pozostają charakterystyczne głównie dla relacji między kierownictwem a wykonawcami. Stwarzają jednak ryzyko ze względu na bliskość poszczególnych węzłów, co zwiększa możliwość identyfikacji elementów. Z tego powodu relacje mogą być krótkotrwałe, podlegające zagrożeniom zewnętrznym (np. działalności organów ścigania). Są one charakterystyczne dla struktury sieciowej organizacji skupionej wokół ustalonego kierownictwa (np. gangi). Decyzyjność jest odwzajemniona bezpośrednim wykonawstwem pozostałych członków organizacji. Naruszenie któregokolwiek z elementów powoduje osłabienie sieci lub ustanie jej działalności. Bliskość w sieci staje się miarą szybkości przepływu informacji, co jest ważne przy realizacji założonego celu[22];
- przychodzące – typowe dla kierownictwa wydającego dyspozycje. Charakteryzują się dużą częstotliwością wpływających informacji i małą częstotliwością informacji wychodzących. Podobnie jest z czasem reakcji: szybki wpływ informacji przy wydłużonym okresie zwrotnego przesłania informacji. Istotny pozostaje także dobór odbiorcy informacji uzyskanych od kierownictwa, co będzie się zawierało w potrzebie ustalenia klucza typowania takiego podmiotu w kon-

tkana, co powoduje że przeciekanie wody przez te kanały jest niemożliwe. W matematyce teoria perkolacji opisuje zachowanie się połączonych grup wierzchołków w grafie losowym. Ma ona jednak szersze zastosowanie, w tym do przygotowywania analiz w kierunku realizacji neutralizacji sieci przestępczych, nie do końca możliwych do całościowego rozpracowania.

[20] Sieć w stanie początkowym może być utworzona przez określonego (pojedynczego lub zbiorowego) organizatora, ale może także powstawać spontanicznie.

[21] R. Wdowiak, *Identyfikacja struktur sieci złożonych*, Politechnika Wrocławska Wydział Podstawowych Problemów Techniki, (praca inżynierska napisana pod kierunkiem dr R, Werona), s. 9 [online] http://www.ioz.pwr.wroc.pl/pracownicy/weron/prace/Wdowiak07.pdf [dostęp: 28 I 2014].

[22] W ramach prowadzonego rozpoznania organy ścigania, chcąc kontrolować działania przestępcze, powinny wprowadzić elementy dezinformacji lub opóźniania informacji w sieci.

tekście funkcjonowania sieci organizacyjnej. Tego typu relacje będą zachodziły w przypadku stabilnego kierownictwa, wielu wykonawców i typowania podmiotów do realizacji określonego zadania (przygotowania lub dokonania przestępstwa). Ponadto należy tu rozgraniczyć rodzaj popełnianego przestępstw, tzn. czy dane świadczą o tym, że jego popełnienie wymaga szybkości reakcji, czy raczej dłuższego przygotowania;

- wychodzące – charakteryzuje je ocena sytuacji i dobór odbiorcy, jeżeli przekazanie informacji następuje od kierownictwa do wykonawców. Badając je, można ustalić stopień zakonspirowania kierownictwa i typować sposób prowadzenia wewnętrznej łączności, co jest bardzo ważne w odniesieniu do sieci przestępczych. Niejednokrotnie jest to wewnętrznie utajona wymiana informacji uniemożliwiająca identyfikację kierownictwa. Możliwy tu będzie także brak bezpośrednich powiązań między typowanym kierownictwem a bezpośrednimi wykonawcami (duża odległość takich węzłów w sieci). Jednym z kierunków badań sieci jest określanie stosunku relacji przychodzących do relacji wychodzących od poszczególnych węzłów;
- powiązane – wymagają badania więcej niż jednych powiązań bądź też powiązań w różnych płaszczyznach. W tym przypadku można brać pod uwagę relacje wynikające z osobistych spotkań, kontaktów drogą elektroniczną, prowadzenia rozmów za pośrednictwem sieci teleinformatycznych, a także relacje wynikające z przepływu środków finansowych, odbioru towaru bądź też organizowania spotkań poprzez zidentyfikowanych pośredników[23].

Kolejnym zagadnieniem jest potrzeba kompleksowego wyodrębnienia sieci przestępczej z całości sieci społecznych występujących na danym obszarze lub w danej społeczności. Tym samym należałoby przyjąć, że zachowanie sieci przestępczych jest odmienne od zachowań sieci niemających charakteru struktur przestępczych (typu nieprzestępczego). Podstawowym wyróżnikiem obu tych kategorii będą: odmienność celów działania, odmienność stosowanych mechanizmów służących osiągnięciu tych celów, a także odmienność instrumentów, jakimi będą się posługiwały poszczególne elementy sieci (węzły). Wyodrębnienie sieci przestępczych z sieci społecznych, choć czasami niezwykle trudne do wykonania, będzie związane z poszukiwaniem krawędzi i wszystkich węzłów sieci przestępczych. Trudności przy wyodrębnieniu sieci przestępczych będzie sprawiała nieostrość samych krawędzi powodowana „wtapianiem się" i przenikaniem struktur przestępczych ze społecznymi, znajdującymi się w jej otoczeniu (np. stosowanych przy procederze prania pieniędzy). Zastosowanie tego rodzaju taktyki pozwala sieciom przestępczym na „rozmywanie się" i zapewnia im anonimowości w obszarze oddziaływania społecznego. Można jednak określić wyróżniki stanowiące o odmienności sieci przestępczych od innych sieci społecznych, które powinny posiadać przełożenie na samą strukturę, w tym jej obrazowe przedstawienie (tabela 1). Zaburzenie samego obrazu mogą wywoływać między innymi: zbieżność celów (osiąganie zysku przestępczego lub zysku finansowego z prowadzonej działalności gospodarczej) oraz nieprzestrzeganie bądź wręcz brak procedur w grupie przestępczej przy naruszaniu wewnętrznych przepisów proceduralnych w organizacjach sformalizowanych (typu urzędy).

[23] D. Batorski, *Sieci społeczne. Charakterystyka uwarunkowania i konsekwencje struktur relacji społecznych na przykładzie komunikacji internetowej* (prezentacja pracy doktorskiej), Warszawa 2004, Uniwersytet Warszawski, slajd nr 9.

Tabela 1. Porównanie założeń budowy sieci typu przestępczego z sieciami typu nieprzestępczego w strukturach sieci społecznych.

Sieć typu przestępczego	Sieć społeczna typu nieprzestępczego
Struktura zbudowana na przyjętym przez organizatora podziale niesformalizowanym lub na podstawie szerokiej anonimowości węzłów	Struktura sformalizowana, zbudowana na podstawie wewnętrznych przepisów, trybów postępowania i procedur, z wyznaczoną rolą w organizacji i zapewnieniem jasności tej roli dla zewnętrznego odbiorcy
Struktura elastyczna, szybko reagująca na zmiany sytuacji, w tym na zagrożenia	Struktura tradycyjna; jej zmiana następuje etapowo, po zatwierdzeniu przez decydentów i wprowadzeniu procedur postępowania obowiązujących w czasie
Podejmowanie działań „na skróty", dla optymalnego osiągnięcia założonego celu	Podejmowanie działań na podstawie ustalonych procedur postępowania
Anonimowość przywództwa organizacji	Oficjalne przywództwo, wyeksponowanie kierownictwa oraz jego zakresu uprawnień, szczególnie w przypadku styczności instytucja–obywatel
Nawet przy założeniu że ustanowiony zostaje jeden ośrodek decyzyjny, konstrukcja sieci „chroni" przywództwo, uniemożliwiając ustalenie centralnej jednostki w sieci	Przy sieci geocentrycznej łatwo jest ustalić centralną pozycję jednostki w sieci
Znajomość struktur wyłącznie na poziomie lokalnym, co ma zagwarantować bezpieczeństwo organizacji	Pełna znajomość struktur wewnętrznych z podziałem zadań dla poszczególnych komórek organizacyjnych i ich kierowników
Nieformalność decyzyjna przy jednoczesnym zapewnieniu bezpieczeństwa powiązań między węzłami znajdującymi się w dużych odległościach	Jasność procedur postępowania i odwoławczych; utrzymanie najczęściej hierarchiczności decyzyjnej; węzły pozostają widoczne przy analizie organizacyjnej (możliwość odwołania się od wydanej decyzji)
Różnice w odległości między węzłami sieci wynikają z rodzaju prowadzonej aktywności przestępczej i przyjętej taktyki działania przestępczego – często następuje zmiana odległości między węzłami	Różnice w odległości między węzłami wynikają z przyjętych procedur, terminów administracyjnych – utrzymywanie się stabilnej odległości przy zachowaniu ustalonych procedur postępowania

Izolowanie węzłów mających największe kontakty – ochrona przywództwa sieci	Otwartość węzłów posiadających najwięcej kontaktów
Dążenie do ograniczania kontaktów w celu utrudnienia identyfikacji połączeń	Nakierowanie działań na otwartość relacji międzywęzłowych, przejrzystych dla odbiorcy
Występowanie połączeń, które przez dłuższy czas mogą pozostawać nieaktywne (w spoczynku)[a)]	Dążenie do optymalnego, aktywnego wykorzystania poszczególnych węzłów
Gęstość sieci skupionej wokół przywództwa decydenckiego; w przypadku usunięcia lub wymiany węzła decydenckiego, sieć jest narażona na likwidację (przy sieci typu hierarchicznego)	Gęstość sieci skupionej wokół przywództwa decydenckiego, w przypadku usunięcia lub wymiany węzła decydenckiego, sieć nie ustaje i utrzymuje swoją aktywność
Widoczny brak wyodrębnienia kierownictwa w sieci lub też sztuczne kreowanie kierownictwa w celu wprowadzenia w błąd	Wyraźne wyodrębnienie kierownictwa; jego status musi być jasny, zwłaszcza w strukturze samej organizacji oraz na styku instytucja–obywatel (widoczny zakres zadań kierownictwa)
Strategiczne i decyzyjne powiązania pozostają niezauważalne, utajnione, w rzeczywistości najbardziej aktywne stają się grupy o niskim poziomie zorganizowania (gangi) lub też sieci lokalne, nakierowane głównie na wykonawstwo; stanowią one jedynie przykrycie dla rzeczywistych, utajnionych powiązań przywództwa	Aktywność społeczna grupy osób powoduje powstanie wielu silnych powiązań widocznych po analizie zachowań, swoje zachowania grupa taka wręcz ujawnia i się z nimi utożsamia (przyjęcie zasady emanacji zachowań organizacyjnych)
Wysoka wartość wskaźnika oddalenia[b)] umożliwia zwiększenie możliwości kamuflażu rdzenia sieci przestępczej, a przez to powoduje zwiększenie jej bezpieczeństwa	Wysoka wartość wskaźnika oddalenia może oznaczać powstanie w zarządzaniu organizacją barier utrudniających przepływ informacji w takiej organizacji lub wiedzy wśród członków organizacji, może też wskazywać na niski stopień znajomości członków organizacji i zbytnie zhierarchizowanie jej struktury

[a)] Zob. A. Fronczak, P. Fronczak: *Świat sieci złożonych…*; A. Fronczak, J.A. Hołyst: *Sieci ewoluujące: od fizyki do Internetu* [online], Wykład z Sieci: 21 lutego 2007 Pracownia Dynamiki Nieliniowej Układów Złożonych, http://www.if.pw.edu.pl/~agatka/sieci/wyklad1.pdf [dostęp: 28 I 2014].

[b)] Zob. eksperyment „oddalenia sześciu kroków" Stanleya Miligrama.

Źródło: Opracowanie własne.

Przedstawione różnice wskazują na odmienność zachowań omawianych sieci. Istotnym elementem analizy sieci przestępczych jest ustalenie tych wierzchołków, które budują klastry (powiązanie systemowe mniejszych obiektów w jeden większy – przyp. red.). Są to osoby, które budują wokół siebie struktury przestępcze i przygotowują się do działań niezgodnych z prawem. Ważna będzie także analiza krawędzi (połączeń) sieci, przez którą będą się z sobą porozumiewać członkowie sieci przestępczej. Analiza zachowań między wierzchołkami pozwoli ocenić rytmikę przygotowań, ustalić, czy zachowania w określonych fazach przypominają przygotowania do przestępstwa, a także wskazać wykorzystywanie wierzchołków (urządzeń technicznych) służących utrzymywaniu łączności pomiędzy członkami sieci przestępczej. W sieciach przestępczych między typowanym kierownictwem (rdzeniem sieci) a wykonawcami (węzłami peryferyjnymi) unika się bezpośrednich połączeń, dąży się także do minimalizacji kontaktów między samymi węzłami przez dłuższy czas (są one skupione na organizowaniu przestępstw). Do podstawowych modeli sieciowych zaliczymy następujące struktury:

Sieć regularna

W sieci regularnej już z założenia będą znane informacje na temat zastosowanych w niej systematycznych rozwiązaniach. Niestety, tego rodzaju sieci są rzadkie i niewiele z nich posiada odwzorowanie w rzeczywistości (jest nią np. struktura kryształu). W klasycznej sieci zakłada się stałą liczbę wierzchołków, a tym samym w rzeczywistości w takiej sieci nie przewidywałoby się jej rozwoju. Sieć regularna nie ma w zasadzie odwzorowania w sieciach społecznych, tym samym trudno ją kwalifikować jako przykład dla sieci przestępczych. Sieć regularną charakteryzuje wysoki współczynnik gronowania (występowania zwartych grup połączeń w sieci) i długa tzw. średnia odległość pomiędzy węzłami (średnia droga połączeń). Stałe modus operandi sieci, łatwe do wykrycia i zdefiniowania, nie jest właściwe do konstruowania sieci przestępczych jako sieci regularnych. Ze względu na stałą ewolucję w sieciach przestępczych sieć regularna nie będzie odwzorowaniem ich funkcjonowania.

Sieć losowa

Model Erdosa-Renyiego to sieć losowa, gdzie liczba węzłów wynosi *N*, a prawdopodobieństwo połączenia między dwoma wierzchołkami wynosi *p*. Cechami charakterystycznymi sieci losowych jest krótka średnia droga połączeń między węzłami, co powoduje dość szybki przepływ informacji oraz niski współczynnik gronowania. W sieciach losowych każdy z węzłów odgrywa podobną rolę, ponieważ nie występuje zjawisko preferencyjnego przyłączenia, a więc przyłączenie kolejnego węzła jest równie prawdopodobne.

Prawdopodobieństwo przyłączenia kolejnego węzła w sieci losowej maleje wykładniczo dla wierzchołków o coraz wyższym stopniu. Ze względu na tę właściwość sieci centra (czyli węzły o znacznie większej niż przeciętna liczbie połączeń) nie mają prawa w niej istnieć[24]. Przy takich założeniach sieć losowa nie spełnia warunków (a zwłaszcza warunku bezpieczeństwa) przewidzianych przy zakładaniu sieci, której celem jest popełnianie przestępstw. Kształt sieci byłby za bardzo chaotyczny (głównie w obszarze wykonawczym), uniemożliwiający otrzymanie wymiernego wyniku przestępczego. Rodzaj takiej sieci w znacznej mierze nie spełniałby także potrzeb or-

[24] R. Wdowiak, *Identyfikacja struktur…,* s. 14.

ganizacyjnych dla sieci przestępczych ze względu na niemożliwość tworzenia centrów organizatorskich (np. dystrybucji narkotyków czy lokalnych miejsc organizacji ataku terrorystycznego).

Sieci rzeczywiste, do których zalicza się sieci przestępcze, posiadają jednak inne właściwości niż sieci regularne czy losowe, należą bowiem do sieci złożonych**.** Do ich cech charakterystycznych zalicza się: występowanie wysokiego współczynnika skupienia, występowanie efektu tzw. małego świata oraz rozkład stopni wierzchołków mający charakter potęgowy.

Sieć „małego świata"

Jest to model między sieciami klasycznymi (regularnymi) o ustalonej i stałej liczbie powiązań między sąsiadującymi wierzchołkami a sieciami połączeń przypadkowych. Jego twórcami są Duncan J. Watts i Steven H. Strogatz. Sieć „małego świata" miała łączyć w sobie pozytywne cechy sieci regularnej i losowej poprzez utrzymanie budowy sieci regularnej, w której losowo wybrane krawędzie są dodawane do już istniejących, z określonym prawdopodobieństwem *p.* Charakteryzuje je wysoki współczynnik gronowania (sieć regularna) oraz krótka średnia droga połączeń między węzłami (sieć losowa)[25].

Tym samym otrzymano konstrukcję, która charakteryzuje się szybkim przepływem informacji oraz wysokim współczynnikiem gronowania. Tego rodzaju rozwiązania będzie można prawdopodobnie zauważyć w sieciach przestępczych o charakterze rodzinnym (klanowym) lub zmowie znajomych, których celem jest otrzymanie zysku w wyniku przestępstwa (konstrukcja stosowana dla organizacji terrorystycznych). Niekoniecznie taki związek przestępczy będzie miał wyraźne cechy klasycznie pojmowanej zorganizowanej grupy przestępczej. Niewielkie grupy mogą być ocenione jako bardzo rozbudowane organizacje. Tego rodzaju sieci mogą być zbudowane na potrzeby niewielkiej grupy „założycielskiej" (klasycznej), na rzecz której pozostaje aktywnych wielu nieświadomych wykonawców, ustanowionych z określonym prawdopodobieństwem *p*, których działania powodują osiąganie zysków przestępczych.

M. Segeman jako przykład sieci „małego świata" podaje sieć terrorystyczną zbudowaną przez Fateha Kamela, która łączy muzułmanów zamieszkałych w Kanadzie (wspierających bośniacki dżihad), Mediolanie (wspierających logistycznie Islamski Instytut Kulturalny) oraz zdobywa środki finansowe ze sprzedaży kradzionych samochodów w Turcji i prowadzonych operacji w Jordanii. Sieć ta rozrastała się nie w procesie losowym, ale na zasadzie preferencyjnego połączenia. Prawdopodobieństwo, że z określonym węzłem zostanie powiązany jakiś nowy węzeł, jest tu wprost proporcjonalne do liczby już istniejących wiązań. Sieć rozrastając się, zgodnie z zasadą preferencyjnego przyłączania, ewoluuje w kierunku struktury „małego świata"[26], przypominającej sieć połączeń internetowych[27]. Pogląd prezentowany przez M. Segmana nie uwzględnia jednak tego, że model „małego świata" nie może jednak służyć obrazowaniu sieci z tzw. centrami, czyli nie bierze pod uwagę osób, które zawarły znacznie więcej znajomości od swoich kolegów (rozkład wiązań nie jest potęgowy)[28]. Taki charakter mają sieci bezskalowe.

[25] Tamże, s. 15.
[26] Zapis oryginalny.
[27] M. Segeman, *Sieci terroru,* Kraków 2008, Wydawnictwo Uniwersytetu Jagiellońskiego, s. 171–172.
[28] R. Wdowiak, *Identyfikacja struktur* ... s. 15.

Sieć bezskalowa – ewoluująca

Twórcami sieci bezskalowej są Albert-Laszlo Barabasi i Reka Albert, którzy badali strukturę sieciową stron WWW[29]. Charakteryzuje się ona stałym wzrostem, preferencyjnym (a nie losowym) dołączaniem kolejnych wierzchołków oraz potęgowym rozkładem stopni wierzchołków. W sieci o potęgowym rozkładzie stopni wierzchołków wiele węzłów ma tylko jedną krawędź, ale można też znaleźć węzły z ogromną liczbą krawędzi, tzw. huby.

Struktura połączeń w takiej sieci charakteryzuje się indywidualnością użytkowników, którzy sami decydują o korzystaniu z tej, a nie innej strony internetowej. Twórcy modelu ustalili, że potęgowy rozkład stopni wierzchołków w sieciach rzeczywistych jest konsekwencją wzrostu sieci i reguły preferencyjnego dołączania wierzchołków. Preferencja polega na tym, że prawdopodobieństwo utworzenia połączenia do jednego ze starszych węzłów przez nowy wierzchołek jest wprost proporcjonalne do stopnia tego węzła.

Model ten jako model sieci ewoluującej będzie mógł być zastosowany do analizy rozbudowujących się sieci przestępczych. Należy przyjąć, że „sieciowe narzędzia" przestępcze będą wykorzystywane do otrzymywania zysków przestępczych. Ta nieprzewidywalność będzie występować w ocenie odbiorców tego narzędzia, czyli np. osób chcących skorzystać z nielegalnego hazardu w Internecie. W takim zakresie organizacje przestępcze będą mogły wykorzystywać efekt autokatalityczny, czyli samonapędzającego się procesu społecznego. W wyniku dotychczasowych badań sieci bezskalowych stwierdzono, że węzły mające wiele czynnych połączeń są bardziej atrakcyjne, i tym samym przyciągają kolejne węzły.

Dalsze prace podjęte w celu zrozumienia zjawisk zachodzących w sieciach bezskalowych prowadzone przez Bianconiego i Barabasiego wykazały, że zdolność do przyciągania nowych węzłów jest zależna nie tylko od stopnia węzła, lecz także od parametru *fitness*, dzięki któremu nowy węzeł o dużych zdolnościach generowania relacji może w szybkim tempie zwiększać swój stopień i zdystansować starsze węzły[30]. Organizacje przestępcze działające w sieci teleinformatycznej będą oferowały swoje nielegalne produkty, opierając się na strategii wykorzystania znanych węzłów oraz na stałym uatrakcyjnianiu oferty wobec potencjalnego użytkownika (zapewniając większą satysfakcję z korzystania z nielegalnego produktu i większe bezpieczeństwo, a także atrakcyjność wizualną), przy jednoczesnej możliwości wprowadzania gracza w błąd w celu pozyskiwania nowych graczy, po spełnieniu warunków przystąpienia określonych przez inicjatora sieci.

Ta nieprzypadkowa przewidywalność sieci jest prawdopodobna, tak aby mogła zaistnieć w rzeczywistości przy kształtowaniu się organizacji przestępczej typu sieciowego, zwłaszcza gdy organizacja przestępcza typu sieciowego działa przez kierowanie nielegalnej oferty do członków społeczeństwa (usługi oparte na prostytucji, sprzedaż narkotyków, przeglądanie stron pornograficznych itp.). Przy konsolidacji organizacji przestępczych mniejsze sieci przestępcze będą raczej dołączały do większych organizacyjnie sieci kryminalnych, a nie poszukiwały innych rozwiązań (jest to możliwe nie tylko na skutek własnych działań słabszych grup, ale z powodu zdominowania mniejszych sieci przez większe przy użyciu nielegalnych metod). Dalsze badania nad ewolucją sieci bez-

[29] Skomplikowany system obliczania typowania poszczególnych węzłów w sieci bezskalowej został przedstawiony w opracowaniu A. Fronczak, P. Fronczak, *Świat sieci złożonych*..., s. 253–254.

[30] J.M. Zając, K. Rakocy, A. Nowak, *Nierówności w sieci. Zróżnicowanie pozycji węzłów na przykładzie sieci linków między blogami,* w: *Układy złożone w naukach społecznych,* A. Nowak, W. Borkowski, K. Winkowska-Nowak (red.), Warszawa 2009, Wydawnictwo Naukowe PWN, s. 216.

skalowych pozwolą także lepiej zrozumieć dobór personalny w sieciach przestępczych i taktykę prowadzenia tego rodzaju działań w przestrzeni teleinformatycznej, zwłaszcza pod kątem czynników przeważających przy doborze i przyjmowaniu do struktury sieci takich, a nie innych kolejnych węzłów.

Należy jednak podkreślić, że sieci przestępcze zmieniane na różnym poziomie przez organizatorów nie są w rzeczywistości pełnym odwzorowaniem powyższych modeli, a pozostają jedynie podobne do nich, przeplatając się jednocześnie z indywidualnym kreowaniem ich przez organizatorów. Dobór modeli będzie zależał przede wszystkim od tego, czy organizator będzie się starał stworzyć personalny mechanizm realizacji utajnionych zadań w szerokiej skali geograficznej i wykonawczej (nie wiąże go potrzeba bezpośredniego wykonywania kierownictwa i kontroli), czy raczej posłuży się niewielką, rzeczywistą siecią personalną, uruchamiając techniczny mechanizm nieograniczonych (teoretycznie) możliwości popełniania przestępstw w przestrzeni teleinformatycznej. Tym samym do kreowania takich zachowań pomocne będzie zarówno zastosowanie modelu „małych światów", jak i modelu bezskalowego. Ponadto uwzględniając inwencję twórczą organizatora sieci, nawet ze względów bezpieczeństwa nie będzie się on kierował budowaniem sieci na wzór uznanych modeli matematycznych.

Istotą posłużenia się modelami matematycznymi sieci (również *mix-network*, czyli ich kombinacją) przez organy ścigania będzie takie dokonanie oceny sieci rzeczywistej, aby osiągnąć cel. W przypadku sieci przestępczych będzie to ustalenie niezbędnych czynników, które pozwolą organom ścigania na przeprowadzenie skutecznego ataku, w którego wyniku zostanie dokonana destrukcja funkcjonowania sieci. Ograniczeniem działania inicjatora będą założenia do funkcjonowania obszaru, w którym ma się odbywać aktywność przestępcza (np. pomysł przestępczy ulokowany w obszarze Internetu będzie musiał pozostawać zgodny z założeniami matematycznymi budowy tego środowiska komunikowania się, pozyskiwania i poszukiwania informacji).

Badanie sieci bezskalowych będzie można zastosować przy analizie obszaru teleinformatycznego wykorzystywanego przez członków sieci przestępczych jako sposobu komunikowania się. Badaniem takim byłyby objęte strony WWW, blogi, Skype'y oraz fora społecznościowe służące do organizacji sieci i przygotowywania przestępstw.

Kolejnym zagadnieniem jest ustalenie istoty funkcjonowania sieci przestępczej. Uzyskanie jej przybliżonej struktury niekoniecznie da odpowiedź na pytanie, jak ona działa, gdzie znajdują się ważne z punktu widzenia przesyłu informacji węzły, jaki jest sposób zadaniowania poszczególnych wierzchołków oraz jaki jest sposób koordynowania realizacji tych zadań. W podjętych badaniach Guillaume i Latapy próbują odpowiedzieć na pytanie, co wpływa na to, że wiele sieci ma takie, a nie inne cechy. Zwracają oni uwagę na to, że pewne własności elementów sieci (cechy) mogą decydować o jej strukturze. Sugerują także, że istnieje pewna, ukryta lub nie, dwudzielna struktura, w której istnieją dwa zbiory: zbiór elementów sieci i zbiór ich własności[31]. Taka ocena jest zrozumiała z punktu widzenia taktyki organizacji przestępczych, która była stosowana jeszcze w strukturze hierarchicznej. Polegała ona na tym, że oprócz „widocznych" członków w organizacji funkcjonowali członkowie „ukryci", których można było scharakteryzować jako kierujących, a jednocześnie wykorzystujących mechanizmy kamuflażu (np. używanie rzadkiego dialektu, posługiwanie się sfałszowanymi dokumentami, stosowanie kryptografii, nawiązywanie od-

[31] K. Rybarczyk-Krzywdzińska, *Losowe grafy przecięć. Modelowanie sieci i ich analiza* (praca doktorska), Poznań 2009, Uniwersytet Adama Mickiewicza, s. 20.

powiednich relacji z innymi węzłami w celu zapewnienia bezpieczeństwa własnego i sieci). Do rozwiązań taktycznych można zaliczyć: występowanie jako tzw. cichy wspólnik, podawanie się za inną osobę, odbywanie kary za innego członka grupy przestępczej, dysponowanie wypranymi, „legalnymi" środkami finansowymi, wprowadzanie w błąd organów ścigania, manipulowanie organami ścigania przy pomocy „świadków koronnych" oraz podwójna tożsamość.

Przedstawione powyżej modele mogą posłużyć organom ścigania do:

- przeszukiwania globalnych sieci społecznych w celu ustalenia funkcjonowania sieci przypominających swoim działaniem sieci przestępcze (jako wyróżnione z całości),
- przeszukiwania globalnie działających sieci terrorystycznych w celu wyodrębnienia sieci lokalnych,
- projektowania taktyki przeciwdziałania popełnianiu przestępstw przez ustalanie wewnętrznej budowy zdefiniowanych sieci przestępczych oraz ocenę ich organizacyjnego funkcjonowania w porównaniu do znanych teoretycznych modeli sieci,
- dokonywania oceny modeli skonkretyzowanych sieci przestępczych, aby wyszukać „strategiczne węzły" (jako słabe punkty w sieci) do przygotowania na nie ataku,
- oceny skali i zakresu występowania węzłów wchodzących w skład rdzenia sieci przestępczej.

Ogólna analiza struktury sieci przestępczych

Działalność grup przestępczych ma na celu przede wszystkim stworzenie jak największego dystansu między czterema punktami: terenem faktycznego operowania, miejscem dowodzenia, z którego płyną polecenia, miejscem ujawnienia korzyści (zwłaszcza finansowych) oraz miejscem legalizacji korzyści (prania pieniędzy)[32]. Mówiąc o miejscu, niekoniecznie należy je kojarzyć z odległościami, które są znacznie skracane lub też nie mają znaczenia w aktywności organizacji przestępczych. Oprócz przyjmowania określonej struktury organizacyjnej (spontanicznej) sieci przestępcze są budowane także na podstawie dynamiki geograficznej łatwości popełniania przestępstw, mniejszej odpowiedzialności karnej czy podatności na korupcję organów ścigania. Dotyczy to tak sieci kryminalnych, jak i sieci terrorystycznych. Przykładem może być przyjęcie czynnika geograficznego, który umożliwia wytypowanie kolejnych członków z obszaru Maghrebu, północno-wschodniej Afryki, Azji Środkowej czy spośród diaspory muzułmańskiej w Europie na potrzeby organizacji terrorystycznych. Jeżeli chodzi o grupy zorganizowane, podział ten jest związany między innymi z „ekonomią przestępczości". W tym zakresie wyróżnia się m.in. obszary: pozyskiwania narkotyków (Azja, Ameryka Południowa), ich zyskownej dystrybucji (Europa) oraz prania nielegalnych środków (raje podatkowe)[33]. Ten rodzaj

[32] M. Płachta, *Zwalczanie przestępczości zorganizowanej na arenie międzynarodowej*, „Biuletyn" 1999, nr 3/4, Centrum Europejskie Uniwersytetu Warszawskiego, s. 34. Zob. W. Kurowski, *Wpływ globalizacji na działalność organizacji przestępczych i ich zwalczanie*, praca magisterska napisana w Katedrze Prawa Karnego i Kryminologii, pod kierunkiem naukowym prof. zw. dr. hab. Emila Pływaczewskiego, Białystok 2004, s. 44

[33] W przypadku posługiwania się analizą opartą na ryzyku rozpoznawania procederu prania pieniędzy czy finansowania terroryzmu, stosowane są kryteria: geograficzne, behawioralne, przedmiotowe oraz ekonomiczne (art. 10a *Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, Dz.U z 2010 Nr 46, poz. 276, z późn. zm.).

konstrukcji sieci nie jest przypadkowy (losowy), jest natomiast związany z możliwością tworzenia lokalnych centrów zdolnych do określonych ogólnie przyjętych działań kierunkowych, naznaczonych cechą kierownictwa (zakłada się tu racjonalne postępowanie organizatora i określenie roli węzłów na potrzeby ustalonych celów organizacyjnych). Przy czym nie jest to proceder organizowany odgórnie i pod bezpośrednią kontrolą.

Na zbudowanie współczesnych sieci przestępczych będą miały wpływ następujące czynniki:

- cel do osiągnięcia – jest to związane ze wskazaniem, do czego ma być pomocne tworzenie sieci, czy jest to jedynie ad hoc luźne związanie się poszczególnych węzłów np. dla wykazania słabości organów ścigania bądź przedstawienia protestu bez skutków ubocznych, czy jest to zachowanie, którego celem jest dokonanie destabilizacji struktur władzy bądź społecznych, czy chodzi o osiągnięcie zysków finansowych. Cel będzie kojarzony raczej z przestępstwami, niż z kształtowaniem struktury przestępczej organizacji,
- trwałość w czasie – odnosi się do zachowania założeń intelektualnych budowy sieci, czy jest to zachowanie pojedyncze krótkotrwałe, czy raczej ustalone, i w założeniu mające trwać dłużej w czasie, działanie niezgodne z prawem,
- typowanie węzłów – powinno się kojarzyć z ustaleniem schematu przestępczego działania, przyjęciem założenia, jakiego rodzaju przestępstwa mają być dokonywane bądź też z utworzeniem swoistego rusztowania dla całego mechanizmu przestępczego. W tym ostatnim przypadku oznacza to, że jedynie niektórzy (czyli organizatorzy) znają całość mechanizmu i kierunek wytwarzania środków, pozostali zaś to bezwiedni uczestnicy lub ofiary przyjętych rozwiązań przestępnych. Ważne będzie dokonanie oceny, jaki schemat stosują węzły sieci przy pozyskiwaniu kolejnych węzłów. Typowanie elementów struktury hierarchicznej będzie odmienne niż węzłów w strukturze sieciowej. Na dobór węzłów będzie wpływała potrzeba zachowania struktury w czasie. Ponadto organizator będzie musiał dbać o zapewnienie bezpieczeństwa w sieci (zapewnienie odporności na ataki) przy zachowaniu znacznych odległości między poszczególnymi węzłami,
- określenie użytych metod działania – niektóre z planowanych metod pozostają charakterystyczne dla określonego postępowania, np. dystrybucja narkotyków może odbywać się przez osoby fizyczne (dealerów) oraz anonimowo przez sieci Tor i sprzedaż za pośrednictwem sieci teleinformatycznych z wykorzystaniem firm kurierskich. Ponadto niezbędne jest prowadzenie rozpoznania pod względem zastosowanych metod kamuflażu, zdolności dezorganizacji działań organów ścigania itp.

Złożone sieci przestępcze mają odmienne od społecznych, pod względem konstrukcyjnym, systemy budowania relacji między poszczególnymi węzłami. Ta odmienność jest przyjmowana jako wynik dokonywania wyboru między sprzecznymi z sobą celami, tj. efektywnością i szybkością działania a potrzebą zachowania bezpieczeństwa, np. ukrycia struktury przed organami ścigania

Różnicy w występowaniu odmiennych sieci przestępczych można doszukiwać się w więzach narzuconych na funkcjonowanie sieci przestępczych. Tym, co niewątpliwie wymusza takie, a nie inne formowanie się struktur (przykładowo gangu i sieci dealerów narkotykowych), jest konieczność wyboru między dwoma sprzecznymi z sobą celami, tak samo, jak w przypadku sieci przestępczych i sieci społecznych, efektywnością i szybkością działania a potrzebą pozostania w ukryciu. Im częściej grupa podej-

muje różnego typu akcje, tym lepszy powinien być w niej przepływ informacji, nawet kosztem możliwej dekonspiracji. Gwiaździsta struktura gangu umożliwia błyskawiczną komunikację pomiędzy jego członkami, usprawniając koordynację działań[34]. Bardziej skomplikowane sieci przestępcze chroniące swoich rzeczywistych przywódców (trzon sieci) będą się zachowywały podobnie jak elementy nielosowe w sieci, które będzie charakteryzowało indywidualne zachowanie i poszukiwanie relacji z podobnymi sobie (kolejnymi członkami przywództwa własnej lub innych sieci). Obserwacja związków zachodzących pomiędzy takimi osobami pozwoli na ocenę, czy i z kim zachodzą relacje kierownicze oraz jakie to daje wyniki dla funkcjonowania sieci jako całości (obserwacja aktywności poszczególnych węzłów lub klastrów).

Mimo różnic występujących między sieciami przestępczymi a sieciami społecznymi, do analizy tych pierwszych wykorzystuje się metodę badawczą określoną jako analiza sieci społecznych (*Social Network Analysis* – SNA). Główną zaletą SNA jest możliwość odtwarzania, wizualizacji i oceny złożonych, wielopoziomowych relacji społecznych, biorąc pod uwagę zarówno bezpośrednie, jak i pośrednie kontakty między podmiotami[35].

W strukturze hierarchicznej występuje najwyższy stopień centralizacji i gęstości (definicja gęstości dalej – przyp. red.) skupionej w głównej mierze wokół osoby lidera. Występujący w sieci członkowie, wobec których ustalono najwyższy poziom centralizacji, mogą odgrywać różną rolę. Przy bardziej hierarchicznej strukturze rola ta będzie decydowała o kierowaniu całością organizacji. W innym przypadku widoczne to będzie przy spłaszczonej, poziomej strukturze organizacyjnej, wówczas taka osoba będzie prawdopodobnie odpowiedzialna za działanie przestępcze (poziom wykonawstwa) jedynie w lokalnym zakresie (będzie odgrywała rolę „huby" w strukturze sieci złożonej, bezskalowej). W ten sposób można wykazać jej aktywność w przygotowaniu przestępstw, ale nie w kierowaniu zorganizowaną grupą lub związkiem. W przypadku przyjęcia modelu hierarchicznego lub sieciowego, opartego na potrzebie stałego kontrolowania wykonawstwa z punktu widzenia organizatora, działanie takie może być zgubne. Pozostawia ono zbyt wiele „śladów", głównie „śladów" relacjacyjnych (wynikających z relacji) umożliwiających identyfikację rdzenia organizacji. Tym samym bardziej bezpieczne stają się układy sieciowe zapewniające kontrolę działania wykonawców w sposób bezpieczny, przez nieangażowanie się bezpośrednio w nadzór nad popełnianiem przestępstw. Sieć taka może być bezpieczna ze względu na odległość między wierzchołkami decyzyjnym a wykonawczymi oraz niewielką liczbę połączeń między nimi. Kamuflażem może być także znaczna liczba relacji zarówno istotnych z punktu widzenia organizacji przestępstwa, jak i innych, nieistotnych, także z elementami otoczenia sieci. Pozwala to na zaciemnienie oceny znaczenia poszczególnych węzłów podczas analizy prowadzonych relacji.

Współczesne organizacje terrorystyczne działają prawdopodobnie jako samozsynchronizowanie sił rozproszonych (ang. *self-synchronisation of dispersed forces*[36]*).* Tego rodzaju sieci mają rozproszoną konstrukcję, duże odległości między węzłami, nieliczne relacje (słabe połączenia z innymi węzłami), co zapewnia zachowanie bezpie-

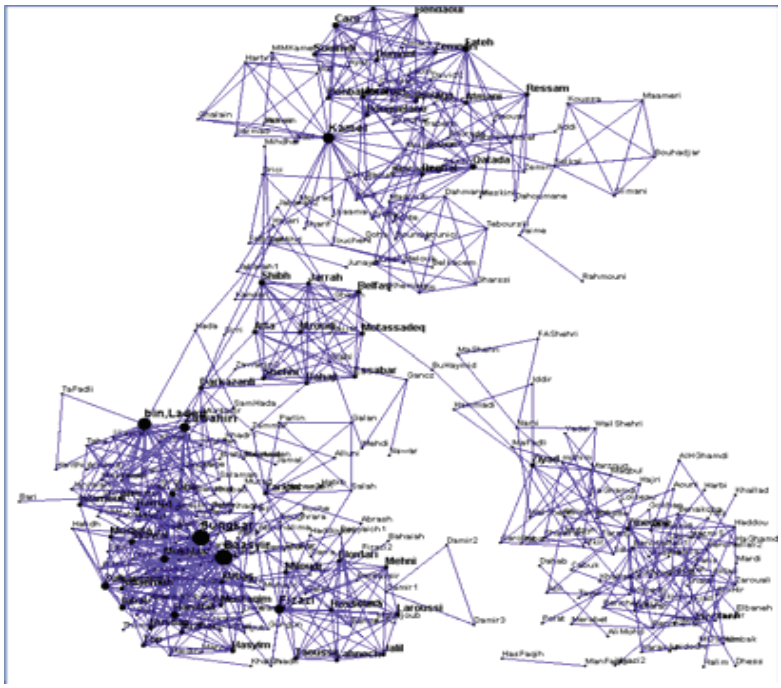
[34] A. Fronczak, P. Fronczak, *Świat sieci złożonych*…, s. 228–229.

[35] Zob. P. Stępka, K. Subda, *Wykorzystanie analizy sieci społecznych (SNA) do budowy organizacji opartej na wiedzy* [online], http://www.e-mentor.edu.pl/artykul/index/numer/28/id/618 [dostęp: 28 I 2014].

[36] Pojęcie zaczerpnięte z terminologii wojskowej. Nad *self-synchronisation* (NCW) pracował A. Cebrowski z US Navy. NCW wykorzystuje teorię złożoności, wspólnych zachowań, osiągnięć technologicznych i samoorganizacji. Zob. D. Penzar, A. Srbljinović, *About modelling...,* s. 31.

czeństwa, ale nie sprzyja operatywności sieci. Ponadto należy zauważyć, że taka konstrukcja nie wymaga stałego kierowania. Jest to możliwe dzięki wcześniejszemu uczestniczeniu w szkoleniach, wzajemnym poznawaniu się, nabieraniu zaufania i tworzeniu związków towarzyskich wykorzystywanych później do celów terrorystycznych. Istotna jest też wspólna świadomość sytuacji, która ułatwia organizowanie sił i ich synchronizację. Na dalszym etapie rozrost sieci będzie się odbywał o już istniejące węzły, które w wyniku relacji z innymi węzłami oraz z otoczeniem uzyskały silną pozycję. Punkty te będą źródłem dalszego rozbudowywania peryferyjnych obszarów sieci. Osiągnięcie takiego poziomu świadomości będzie możliwe wtedy, gdy sieć będzie się składała z członków uprzednio kompleksowo przeszkolonych w zakresie: walki zbrojnej, konstrukcji ładunków wybuchowych, logistycznego organizowania zamachów terrorystycznych, kamuflażu czy pozyskiwania środków na działalność. Wprowadzenie do sieci amatorów (bojowników) znacznie ogranicza samozsynchronizowanie sił w sieci i zwiększa ryzyko zagrożenia bezpieczeństwa uczestników sieci przestępczej.

Zastosowanie samozsynchronizowania sił w sieci jest możliwe ze względu na ponadnarodowy charakter zarówno przestępczości zorganizowanej w celu osiągnięcia korzyści finansowych, jak i przestępczości terrorystycznej (cele ideologiczne lub polityczne). W ich działaniach brakuje ujęcia lokalnego (np. narodowego), a wiodącym założeniem jest przyjęcie priorytetów zbieżnych lub tożsamych dla tych organizacji. Impuls do lokalnego działania w taktyce sieciowej (złożonej) aktywności nie musi być tajny. Równie dobrze może być przekazany przez ogólnodostępne media (wypowiedź uznanego przywódcy, np. nagrane wcześniej przemówienie Bin Ladena, wyemitowane w telewizji Al Jazeera). Samozsynchronizowanie sił jest jednak łatwiejsze do sprawdzenia w przypadku sieci terrorystycznych, luźno powiązanych z mocnym zaangażowaniem ideowym (patrz rysunek), niż w przypadku organizacji przestępczych, które jednak kierują się dużym autonomizmem celów lokalnych.



Rysunek. Powiązania sieciowe występujące w ramach organizacji terrorystycznej Al-Kaida.

Źródło: Ch.C. Yang, N. Liu, M. Sageman, *Analyzing the Terrorist Social Networks with Visualization Tools*, s. 5, http://www.artisresearch.com/articles/Sageman_Analyzing_the_Terrorist.pdf [dostęp: 28 I 2014].

Analiza sieci nie rozwiązuje wszystkich problemów, stąd też organy ścigania od samego początku muszą zwracać uwagę na to, jak umiejętnie zbierać informacje na temat stosowanych mechanizmów przestępczych bądź też jak typować sprawców. Sama analiza sieci powinna być elementem wsparcia o charakterze ocennym i wskazywać to, co nie jest widoczne podczas standardowego rozpoznania. Takie założenie należałoby przyjąć głównie przy sprawach dotyczących popełniania przestępstw związanych z rozprowadzaniem narkotyków bądź znacznej liczby podmiotów popełniających przestępstwa mniejszej wagi, dzięki którym przestępcy osiągają znaczne zyski (wyłudzania środków w Internecie, hazard elektroniczny itp.). Wiele możliwości kamuflowania rzeczywistego sprawcy oraz realnego kierownictwa sieci przestępczej daje też samo środowisko teleinformatyczne. Związane jest to między innymi z podszywaniem się pod adresy IP poszczególnych osób niezwiązanych i niemających powiązań przestępczych lub też wskazanych jako rzekomi przestępcy (np. osoby uprzednio karane), tak aby odwieść organy ścigania od rzeczywistego sprawcy i potencjalnego zagrożenia (metoda *world driving*)[37]. Wynika to także z techniki zbierania dowodów w sieciach teleinformatycznych na cele postępowania przed organami ścigania. Tak więc typowanie rzeczywistych węzłów

[37] Zob. I. Kacprzak, G. Zawadka: *Bezsilni wobec hakera*, „Rzeczpospolita" z 2 lipca 2013 r.

i krawędzi przy tak zaawansowanych technologiach staje się coraz bardziej trudne, a wręcz czasami niemożliwe.

Jednym z ważnych, wstępnych, elementów oceny sieci jest wykazanie jej gęstości. Przez g ę s t o ś ć sieci rozumie się stosunek liczby istniejących związków w sieci do liczby wszystkich potencjalnych związków w sieci. Jest ona miarą kompletności sieci. Tym samym przez gęstość w sieci można ustalić, czy analizowana sieć pozostaje kompletna, czy też należałoby wiedzę o niej uzupełnić, zwłaszcza o informację, czy potencjalne powiązania w sieci nie wskazują na inne zachodzące w niej relacje.

Kolejnym aspektem jest w y t r z y m a ł o ś ć s i e c i, która jest związana z odpornością sieci zarówno na bodźce zewnętrzne, jak i tkwiące wewnątrz organizacji. W tym zakresie należałoby poruszyć trzy podstawowe zagadnienia:

- typowanie (celowe) węzłów sieci,
- losowe wybieranie węzłów sieci,
- odporność na nieprzewidywalny atak na węzły sieci.

Odnosząc się do pierwszego punktu, należałoby wskazać na to, że typowanie poszczególnych węzłów w sieci pozostaje głównie w gestii organizatora. Jego zdolności ocenne pozwalają na takie zaplanowanie struktury personalnej, aby była ona odporna na bodźce. Stąd też w poszczególnych organizacjach zaobserwowano: skomplikowane metody i wieloetapowość przyjmowania w poczet członków organizacji osób, które powinny wykazać się popełnieniem poważnych przestępstw, stosowanie wzajemnej kontroli, stałe sprawdzanie lojalności, typowanie przywództwa z kręgu najbliższych osób, znanych od lat i o których wiedza jest najszersza. Pozwala to na wyeliminowanie członka, który mógłby być w przyszłości wytypowany na świadka koronnego przez organy ścigania (taki sposób postępowania charakteryzuje tradycyjne struktury przestępcze). Ponadto wybór węzłów będzie związany z przyjęciem założeń, w jakim celu sieć przestępcza powstaje, a więc i w jakiej kategorii przestępstw organizacja będzie działała – przestępstwa kryminalne z użyciem siły fizycznej będą wymagały posiadania innych predyspozycji niż popełnienie przestępstw wyłudzenia środków z kont elektronicznych klientów e-banków (w tym drugim przypadku silnymi węzłami sieci będą osoby charakteryzujące się umiejętnościami hakerskimi, planowania gier strategicznych itp.). Dobór może odbywać się także anonimowo przez sprawdzenie przydatności do zakładanych celów organizacyjnych lub też przez godzenie się, narażając się na karalność, na odegranie roli w przygotowaniu przestępstwa i jego dokonaniu.

Organy ścigania zbierają informacje o różnym poziomie prawdopodobieństwa. Nie można wykluczyć także takiej sytuacji, że informacje uzyskiwane od przedstawicieli świata przestępczego są zmanipulowane. W takim przypadku służby będą miały niezgodny z rzeczywistością (błędny) lub niepełny obraz. Mając na względzie konieczność neutralizacji zagrożeń, niezbędne jest odpowiednie przygotowanie taktyki realizacji działań. Analizy pomagają zweryfikować otrzymany obraz, a także losowo, choć z większym prawdopodobieństwem, umożliwiają wytypowanie tych podmiotów, których wyeliminowanie spowoduje w ostateczności znaczne ograniczenie lub też całkowite ustanie aktywności struktury przestępczej.

Przypadkowe typowanie węzłów będzie się wiązać z potrzebami organizacyjnymi, rozszerzeniem zakresu działalności lub działaniem na większym niż dotychczas terenie. Ten sposób taktyki przestępczej będzie szczególnie związany z testem czasowym sieci. Możliwe są tu dwa rozwiązania. Pierwsze będzie polegało na przejęciu innej struktury w ramach już działającej organizacji, w celu poszerzenia terytorium, innego ukierunkowania, wzmocnienia organizacyjnego. W drugim rozwiązaniu rzeczywiście sieć będzie

wytypowana losowo (np. ze względu na terytorium czy rodzaj dotychczas prowadzonej działalności przestępczej), ale przed ustaleniem więzów z już istniejącą siecią zostanie zweryfikowana personalnie (zmiana przywództwa), organizacyjnie (zmiana struktury działania) lub merytorycznie (ocena wykonania narzuconego zdania).

Odporność na nieprzewidziany atak na węzły sieci może się wiązać z przygotowaniem struktury na to, że zawsze może nastąpić zdarzenie losowe, które spowoduje straty w samej sieci. W dotychczasowej ocenie struktury sieciowej z założenia przyjmuje się, że zastosowanie takiego rozwiązania przy odchodzeniu od struktury zhierarchizowanej jest elementem wprowadzenia większego bezpieczeństwa w organizacji. Atak na poszczególne węzły w sieci nie spowoduje naruszenia całości konstrukcji. Jak stwierdzają A. Fronczak i P. Fronczak w grupach przestępczych, w których czas nie odgrywa takiej roli, szybkość komunikacji nie jest priorytetem. Przygotowania do akcji trwają tygodniami, niekiedy nawet miesiącami. Priorytetem jest tajność organizacji. Mówiąc językiem sieci złożonych, średnia droga między węzłami jest długa. Rozbicie takiej struktury jest zatem utrudnione. W odróżnieniu od gangu, gdzie aresztowanie centralnego węzła niszczy całkowicie spójność sieci, w sieciach dealerów narkotykowych usunięcie jednego węzła dysponującego informacją jedynie w swoim lokalnym otoczeniu nie prowadzi do rozbicia całej grupy[38]. Takie rozwiązanie wiąże się także z budowaniem struktury na węzłach znających jedynie lokalne powiązania i przekazujących informacje jedynie w tym zakresie, nie zaś na węzłach strategicznych posiadających wiedzę o całości czy dużej części obszaru funkcjonowania organizacji. Dlatego też ten rodzaj struktury sieciowej wymaga wprowadzenia dodatkowych „ukrytych" mechanizmów porozumiewania się na odległość między węzłami, bez potrzeby narażania organizacji na dekonspirację[39]. Trudności w typowaniu rodzajów sieci i jej zachowań są związane z tym, że sieci złożone ewoluują i zmieniają się, zwiększając lub zmniejszając aktywność poszczególnych węzłów bądź klastrów. Stąd też niezbędne jest zapewnienie stałego monitorowania sieci poprzez pozyskiwanie informacji o jej funkcjonowaniu. Dodatkowo projektowanie ataku na sieć powinno być poprzedzone odwzorowaniem graficznym samej sieci opartej na gromadzonych informacjach oraz ocenie zachodzących wewnątrz sieci relacji, szczególnie z jakim rodzajem sieci organy ścigania mają do czynienia i gdzie w takiej sieci muszą wytypować newralgiczne węzły. Wskazanie takich węzłów pozwala na wskazanie podmiotów ataku. Będzie się to odbywało na podstawie zachodzących wewnątrz sieci relacji: międzyosobowych, utrzymywanych za pomocą środków rzeczowych, miejsc organizowania się itp. Z punktu widzenia optymalizacji ataku ważne jest ustalenie węzłów pośredników i rdzenia organizacji, co pozwala na założenie, że w wyniku ataku sieć zostanie skutecznie zdestabilizowana lub przestanie funkcjonować. Stąd też w organizacji przestępczej mogą zaistnieć zarówno powiązania, które z punktu widzenia pożądanej własności sieci umożliwiają posiadanie krótkich ścieżek (gdzie założeniem jest osiągniecie szybkiego wyniku, np. zysku przestępczego, zniszczenia dowodu popełnienia przestępstwa, uprzedzeniu o działaniach organów ścigania), jak i wprowadzenie długich ścieżek (w przypadku przygotowania skomplikowanego organizacyjnie przestępstwa, ustanowienia bezpiecznych relacji między węzłami peryferyjnymi a centralnymi).

Analiza poszczególnych modeli sieci złożonych (tabela 2) dostarcza tylko częściowej wiedzy na temat struktury sieci przestępczych. Organizator sieci, tworząc ją, w za-

[38] A. Fronczak, P. Fronczak, *Świat sieci złożonych*…, s. 229.

[39] Długość ścieżki w sieci określa, przez ile wierzchołków należy przejść, aby dojść od jednego wierzchołka do dowolnego innego.

sadzie nie kieruje się wzorami matematycznymi, a intuicją i osobistymi zdolnościami organizatorskimi. Z punktu widzenia uzyskania wiedzy o mechanizmach funkcjonowania takich sieci, typowania rzeczywistego przywództwa czy typowania „słabych punktów" w mechanizmach służących popełnianiu przestępstw w obszarze teleinformatycznym, pomocne jest posłużenie się wiedzą na temat funkcjonowania świata sieci złożonych. Mogą zachodzić podobieństwa funkcjonowania poszczególnych podmiotów przestępczych, np. w grupach hierarchicznych minimum decyzji kierowniczych powoduje maksimum realizacji wykonawczych, optymalizacja zysków (finansowych) maksymalizuje się w kierownictwie grupy, podejmowanie realizacji w organizacji skupionej wokoło lidera (decydenta) i szybkiej realizacji celu organizacyjnego czy rozproszenie wykonawstwa, wprowadzenie spłaszczonej szerszej decyzyjności w zakresie wykonawstwa przy jednoczesnym ukrywaniu rzeczywistego rdzenia organizacyjnego.

Tabela 2. Porównanie założeń struktury sieci typu przestępczego o budowie hierarchicznej z organizacją typu sieciowego.

Organizacje przestępcze typu klasycznego	Organizacje przestępcze typu sieciowego
Hierarchiczna, wieloszczeblowa struktura organizacyjna (centralizacja)	Struktura pozioma (fragmentacja)
Podział pracy i ról pomiędzy członkami organizacji	Wymienna rola poszczególnych elementów wykonawczych (niestabilność ról), te same osoby pełnią wiele różnych funkcji
Rywalizacja o zajęcie pozycji w strukturze organizacyjnej	Synergia działania, zbędność konkurencji i rywalizacji o pozycję w organizacji
System pozyskiwania i awansowania członków uwzględniający ich umiejętności i kompetencje przynoszące określone korzyści dla organizacji	Rekrutacja oparta głównie na powiązaniach rodzinnych, etnicznych, wcześniejszych znajomościach lub przystąpienia do sieci z określonym prawdopodobieństwem
Wewnętrzne działanie oparte na sformalizowanych i tajnych zasadach	Brak określonych zasad działania, zmienna w czasie elastyczność postępowania
Struktura wrażliwa na ataki	Elastyczna struktura odporna na ataki
Działanie w decyzyjnej strukturze hierarchicznej podporządkowanej wewnętrznym regułom	Decyzyjność jest realizowana na niskim poziomie wykonawczym, niezależnie lub pośrednio zależnie od ukrytych czynników decydenckich
Formalna komunikacja	Komunikacja bezpośrednia (niesformalizowana)[a)]

Homogeniczna	Większa rozpiętość przestrzenna[b)] i związana z tym możliwość większej kooperacji przestępczej w środowisku lokalnym na różnych niezależnych obszarach
Kumulacja inicjatyw przestępczych na danym obszarze	Globalne oferowanie usług przestępczych

[a)] A. Giménez-Salinas Framis, *Illegal networks or criminal organizations: Power, roles and facilitators in four cocaine trafficking structures*, Madrid 2011, Instituto de Ciencias Forenses y de la Seguridad Universidad Autónoma, s. 3–4.

[b)] D. Batorski, *Sieci społeczne. Charakterystyka uwarunkowania …*, slajd nr 16.

Źródło: Opracowanie własne.

Organizacja przestępcza tworzy strukturę sieciową w celu własnej ochrony. Staje się dzięki temu mniej widoczna dla organów ścigania. Struktura sieciowa pozwala też na lepsze zabezpieczenie organizatora i głównego kierującego (tzw. trzonu organizacji) oraz ukrycie zależności wewnętrznych. Niejednokrotnie ze względu na jednakową ocenę roli poszczególnych węzłów i krawędzi trudno jest wytypować kierownictwo w rozumieniu zhierarchizowanej organizacji przestępczej (badając sieć, pozornie wydaje się, że jest to słabiej zorganizowany podmiot przestępczy). Jest to jednak ocena wątpliwa, ponieważ należy zauważyć, że niskie „zorganizowanie" na poziomie wykonawstwa pozwala na szybsze i bardziej elastyczne działanie i zwiększa odporność na ataki – bez znacznej straty dla całości sieci. Dotychczasowe analizy funkcjonowania sieci pomagają typować rzeczywiste przywództwo oraz te węzły, które pozostają newralgiczne dla funkcjonowania sieci. Innymi właściwościami sieci, które można wykorzystać przy planowaniu ataku, jest bliskość, która jest miarą zasięgu danego węzła. Stanowi ona o czasie, jaki jest potrzebny do przemierzenia odległości między dwoma węzłami. Bliskość jest związana z przydatnością rozchodzenia się informacji w sieci. Ponadto na uwagę zasługuje także ważność węzła w sieci, co jest związane z określaniem, które węzły są powiązane z najważniejszymi węzłami[40].

Elementem wyróżniającym poszczególne sieci przestępcze (np. organizacje przestępcze od grup terrorystycznych) jest czas realizacji zadania wpływający na zapewnienie bezpieczeństwa organizacji. W przypadku grup zorganizowanych, których głównym celem jest zdobycie środków finansowych, działanie jest ograniczone czasowo i wymaga szybkiej reakcji, nawet niekiedy kosztem bezpieczeństwa sieci. W przypadku zaś organizacji terrorystycznych, gdzie motywem działania jest ideologia, okres działania jest znacznie dłuższy, a węzły oczekują na odpowiedni moment do działania – tym samym priorytetem takiego rodzaju sieci staje się jej bezpieczeństwo[41]. Sieci kryminalne wy-

[40] Zob. M. Morzy, A. Ławrynowicz, *Wprowadzenia do analizy sieci społecznych*, prezentacja, slajd nr 22, [online] http://www.cs.put.poznan.pl/mmorzy/tsiss/9_Wprowadzenie_do_SNA.pdf [dostęp: 28 I 2014].

[41] Zob. C. Morselli, C. Giguére, K. Petit, *The efficiency/security trade-off in criminal networks*, „Social Networks" 2007, nr 29, s. 143–153, Sieci, które są ograniczone czasowo w stosunku do zadania, muszą sobie to zrekompensować przez utrzymywanie bardziej efektywnego systemu komunikacji w rdzeniu w celu zmniejszenia prawdopodobieństwa wykrycia. Sieci, w których działanie może być opóźnione przez dłuższy czas (dłuższy czas na realizację zadania), mają mniejszą wydajność w centrum, ale są w stanie działać w bardziej bezpiecznych warunkach. Sieci przestępcze mające wysoki poziom odległości pomiędzy uczestnikami

magają stałego zasilania finansowego i zapewniania zysków poszczególnym członkom, co powoduje, że sieć musi być wydajna. Wydajność zaś wyzwala potrzebę skracania dystansu czasowego do działania, a tym samym wzrasta ryzyko zagrożenia bezpieczeństwa sieci. Stąd też można wywnioskować, że w przypadku współdziałania organizacji kryminalnych z terrorystycznymi wrażliwym obszarem pozostają punkty styczne, gdzie bardziej zakamuflowana grupa terrorystyczna musi brać pod uwagę większą otwartość zorganizowanej grupy przestępczej.

Różna ocena funkcjonowania sieci przestępczych i nieprzestępczych sieci społecznych, a także różnice zachodzące między celami działania grup zorganizowanych a organizacji terrorystycznych pozawalają na wysunięcie wniosków, że na styku tych sieci można mieć do czynienia z tzw. bramkami czy portalami, co może w konsekwencji być uznane za najważniejsze przy całościowym rozpoznawaniu sieci przestępczych. Te węzły styczne (między światem kryminalnym a legalnym), występujące na krawędzi peryferyjnej sieci, mogą się okazać kluczem do zdobycia informacji o strukturze i relacjach zachodzących w sieci przestępczej będącej przedmiotem analizy[42].

Bezpieczeństwo sieci jest związane między innymi z ryzykiem zależnym od częstości akcji wymaganej do funkcjonowania samej organizacji. To ryzyko wzrasta szybciej w organizacjach typu kryminalnego niż w organizacjach terrorystycznych. W organizacjach typu kryminalnego do wzrostu ryzyka może dochodzić wtedy, gdy działają one na zasadzie częstego popełniania drobnych przestępstw oraz gdy jedynie na skutek popełniania przestępstw zdobywa się środki finansowe dla organizacji. Każda aktywność w sieci powoduje pozostawienie „śladów" umożliwiających jej identyfikację strukturalną i ocenę ważności poszczególnych węzłów w sieci. Stąd też „pęd za kryminalnym zyskiem" w sieciach przestępczości zorganizowanej pozostawia znacznie więcej „śladów" niż działania grup terrorystycznych. Ponadto rodzaj popełnianych przestępstw wyzwala ryzyko wykrycia. Wiąże się to również z tym, że np. w przypadku przemytu znacznej ilości narkotyków (przestępstwo pojedyncze), wyzwala ono dalszą potrzebę popełnienia wielu innych przestępstw związanych ze sprzedażą tych narkotyków (przestępstwa wielokrotne). Przestępstwo terrorystyczne zaś to przestępstwo pojedyncze (skonkretyzowany atak terrorystyczny na wyznaczony wcześniej cel). Wynika to także z tego, że dla członków sieci przestępczych ich działalność jest jedynym źródłem dochodu, nawet mimo braku zapewnienia całkowitego bezpieczeństwa. Również niektóre organizacje terrorystyczne popełniają różnego rodzaju przestępstwa kryminalne, narkotykowe czy ekonomiczne, które są źródłem finansowania zamachów. Obszar działania sieci jako całości może być dzięki temu zidentyfikowany jeszcze przed dokonaniem samego zamachu terrorystycznego. W sieciach terrorystycznych, których sponsorem są poszczególne osoby (mocodawcy) lub finansowanie odbywa się za pośrednictwem operacji specjalnych służb wywiadowczych, poziom kamuflowania jest większy, ponieważ na tajności sieci zależy zarówno inicjatorowi, jak i organizacji wykonawczej. Także popełnianie określonych przestępstw (np. rozprowadzanie narkotyków bądź wykonanie zabójstwa na zlecenie) będzie umożliwiało identyfikację sieci. Przyjęty przez sieć charakter i rodzaj popełniania przestępstw narzuca potrzebę takiej, a nie innej konstrukcji sieci. W rzeczywistości podstawowym założeniem jej funkcjonowania będzie ochrona rdzenia sieci (mała liczba

(dłuższy czas realizacji zadania) są bardziej rozproszone niż siatki przestępcze o niskim poziomie odległości (krótszy czas do zadania).

[42] Zob. P. Williams, *Transnational criminal networks*, s. 19 [online] http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch3.pdf [dostęp: 28 I 2014].

powiązań i widocznej aktywności w sieci). Obszary peryferyjne zaś będą się charakteryzować aktywnością dobrze usieciowionych węzłów. Między nimi będą występowały „bufory" chroniące dostępu do rdzenia sieci[43].

Do sposobów obrony sieci przed atakami można zaliczyć:

- występowanie wielu obszarów peryferyjnych w sieci niepołączonych bezpośrednio z jej rdzeniem,
- ochrona rdzenia przez dokonywanie podziałów klastrowych,
- wydłużanie odległości w sieci pomiędzy decydentem a wykonawcą,
- stosowanie paralelnych sposobów komunikowania się przywództwa z kanałami przekazu informacji związanymi z wykonawstwem,
- łączenie węzłów sieci przestępczych z nieprzestępczymi sieciami społecznymi w celu rozmycia struktury[44],
- utrzymywanie elastyczności struktury poprzez zamianę roli poszczególnych węzłów w sieci (brak możliwości zdefiniowania roli węzła w sieci).

Sieci posiadające szybki czas reakcji pozostają bardziej skupione (odległość między poszczególnymi węzłami jest krótka), co powoduje, że atak na poszczególny klaster może zakończyć się jego zniszczeniem, a nawet zniszczeniem całości układu sieciowego[45]. Natomiast sieci, które ze względu na bezpieczeństwo zwiększają odległości między węzłami, pozostają bardziej rozproszone, a tym samym trudniejsze do zneutralizowania. Taka sieć jest bardziej bezpieczna, mimo zniszczenia poszczególnych jej klastrów. Twierdzenie, że sprawność przekazu informacji zależy tylko od odległości pomiędzy nadawcą a odbiorcą, nie jest jednak słuszne. Istotną rolę w takim przekazie odgrywają w ę z ł y p o ś r e d n i c z ą c e. Miarą ich ważności jest pośrednictwo (pojmowane jako wpływ węzła na odporność sieci na uszkodzenia)[46]. Oznacza to, że aby spowodować skuteczne zakłócenie funkcjonowania sieci, powinno się uszkodzić te węzły, których pośrednictwo jest największe. Tak więc niekoniecznie skuteczny będzie atak na te węzły, które są „hubami", a właściwszy i bardziej skuteczny będzie atak na taki węzeł pośredni, bez którego nie będą mogły funkcjonować poszczególne segmenty sieci (klastry). Pośrednictwo pozwala na wytypowanie tych węzłów w sieci, które są najbardziej pożądanymi z punktu widzenia utrzymywania komunikacji między elementami sieci. W konsekwencji atak na najbardziej usieciowione węzły może doprowadzić do przerwania (uszkodzenia) sieci.

Istotnym elementem bezpieczeństwa sieci jest także przyjęcie sposobu jej budowy, a w konsekwencji sposobu funkcjonowania. Obserwacja i analiza działania poszczególnych sieci pozwala na stwierdzenie, że jednym ze sposobów ochrony sieci jest plasowanie najbardziej narażonych elementów sieci w obszarach peryferyjnych (obwodowych), przy zapewnieniu bezpieczeństwa rdzenia sieci, od którego jest uzależnione utrzymanie się sieci w czasie. Innym sposobem zapewnienia bezpieczeństwa jest dzielenie sieci na segmenty, co pozwala na izolowanie poszczególnych elementów od pozostałych[47]. Człony peryferyjne sieci przestępczych będą

[43] Tamże, s. 12–16.

[44] Na przykład łączenie się sieci przestępczych z sieciami finansowymi w celu wyprania środków zdobytych w przestępczy sposób oraz stałego pomnażania kolejnych środków na podstawie rynku towarowo -pieniężnego. Takim sposobem łączenia obu sieci jest na przykład wymuszenie przez grupę przestępczą „sztucznego" zatrudnienia jej członka na etacie u zastraszanego przedsiębiorcy.

[45] Zob. V. Krebs, *Mapping networks of terrorist cells*, „Connections" 2001, nr 24 (3), s. 43–52.

[46] A. Fronczak, P. Fronczak; *Świat sieci złożonych*…, s. 42–43.

[47] Zob. W. E. Baker, R. R. Faulkner, *The social organization of conspiracy: illegal networks in the heavy electrical equipment industry*, „American Sociological Review" 1993, nr 58, s. 837–860.

mogły być analizowane jako działające na zasadzie kliki[48].

W działaniach analitycznych odnoszących się do funkcjonowania sieci można zauważyć także pewne niedogodności. Związane są one z tym, że badana jest głównie aktywność podmiotu w sieci, zarówno w relacji z inną osobą, jak i z przedmiotem (miejscem). Stąd też trudno oceniać relację podmiotu, który nie wykazuje aktywności. Do takich elementów zalicza się: „uśpionych" agentów, nieaktywne telefony oraz osoby, o których organy ścigania nie mają wiedzy z powodu braku możliwości uzyskania o nich informacji.

W ramach sieci poruszana jest także kwestia tzw. kluczowych graczy, zwłaszcza pod kątem stwierdzenia, czy wyeliminowanie takiego gracza nie spowoduje zmniejszenia się spójności sieci (jej spoistości). Z ich oceną łączy się także analiza relacji, jakie zachodzą między takim podmiotem a innymi węzłami sieci (sposób przekazu informacji, weryfikacja zwrotna, oddziaływanie na inne węzły). Typowanie tych osób w sieci może być w praktyce wykorzystane w prowadzonej grze pomiędzy nim a funkcjonariuszem działającym w ramach operacji specjalnej, której celem będzie ujawnienie zachowań sieci przestępczej. Ponadto powstaje pytanie, kto będzie tym kluczowym graczem, czy osoba wchodząca w skład rdzenia, czy też węzeł spajający dwa obszary współdziałające, ale ze względu na odległość funkcjonujące osobno. Przy takiej organizacji sieci wystąpi możliwość anonimowego przenikania funkcjonariuszy działających pod przykryciem do struktury sieciowej. Ich fizyczny byt nie będzie niezbędnym warunkiem wniknięcia w strukturę. Bardziej będą się liczyły posiadanie umiejętności wykrycia mechanizmów rządzących strukturą i możliwości prowadzenia manipulacji węzłami sieci. Poszczególni gracze będą oceniani pod kątem relacji kształtowanych przez nich w sieci i co w ich wyniku zaistniało. W rzeczywiści liderzy sieci będą mieli prawdopodobnie realny wpływ na powstające kontakty między węzłami oraz to, że decyzyjność będzie się utrzymywała w czasie[49]. W drugiej grupie będzie można umieścić węzły ważne ze względu na pośrednictwo (*betweenness*) między poszczególnymi grupami (szczebel pośredni) w obrębie sieci oraz mające realny wpływ na wykonawstwo (przy czym niekoniecznie będą to węzły najbardziej usieciowione)[50]. Wysoki poziom węzłów pośredniczących w grafie sieci przestępczej wskazuje, że struktura jest rozbudowana i złożona z wielu grup wewnątrz organizacji mających wysoki poziom niezależności. Typowanie i badanie *betweenness* jest możliwe dzięki posiadaniu wiedzy na temat przepływów informacji w sieci.

Węzły skupione (najbardziej usieciowione) wokół danego węzła (szczebel koordynacji bezpośredniego wykonawstwa) będą ostatnim poziomem eliminacji. Przy ataku na takie węzły może dojść do zniszczenia klastra, można jednak nie uzyskać rezultatu skutecznego zmniejszenia spójności całości sieci. Jeżeli dany węzeł o wysokim stopniu usieciowienia znajduje się nie na poziomie peryferyjnego wykonawstwa, a zbliża się do rdzenia lub się w nim znajduje, to należałoby domniemywać, że sieć bardziej przypomina organizację hierarchiczną, a decydowanie nie zostało scedowane na niższy

[48] Kliką w grafie określa się zbiór wierzchołków, którego każda para jest połączona krawędzią; *n* – kliką określa się taką grupę lokalną, do której należą wierzchołki, których odległość od każdego innego wierzchołka nie jest większa niż *n*.

[49] Zob. C. Borgatti P. Stephen, *Identifying sets of key players in a social network,* „Computational & Mathematical Organization Theory" 2006, nr 12 (1), s. 21–34.

[50] Mogą to być członkowie sieci przestępczej decyzyjni w zakresie nadzorowania przygotowania przestępstwa, ale nie są oni uprawnieni do podziału zysków finansowych uzyskanych z popełnionego w ramach organizacji przestępstwa.

szczebel lub nie zastosowano sieciocentrycznego sposobu działania. Tym samym kierowanie organizacją przestępczą skupia się w rdzeniu sieci.

Inną propozycją oceny połączeń w sieci przestępczej jest przyjęcie zależności między sposobem prowadzonych relacji w fazie przygotowania przestępstwa a fazą dystrybucji „owoców" tego przestępstwa, czyli podziału zysków finansowych. Wydaje się, że powinno tu nastąpić odwrócenie proporcjonalności polegające na tym, że przy małym bezpośrednim zaangażowaniu niektóre węzły sieci otrzymują największy proporcjonalnie zysk z przestępstwa. Obraz takiego postępowania może być rozmyty, w przypadku gdy podczas współdziałania różnych sieci dokonuje się barterowa wymiana towarów, środków lub informacji. Stąd też powstaje potrzeba oceny i konfrontacji uzyskanych danych, a tym samym oceny wagi węzłów na poziomie „przygotowania przestępstwa", a w dalszym etapie – tych samych węzłów na poziomie dystrybucji informacji czy przy „podziale zysków i ich inwestowania" (np. opierając się na analizie częstotliwości decydowania o wykorzystaniu zdobytych środków).

Rolę poszczególnych węzłów w sieci będzie można ocenić z dwóch poziomów. Pierwszy dotyczy określenia relacji zachodzących z podmiotami zewnętrznymi, drugi jest oceną aktywności węzła w samej organizacji. Niejednokrotnie węzeł w organizacji jest tak dobierany, aby spełniał w niej określoną rolę (posiadał wymaganą w sieci wagę czy cechę). Inaczej będą oceniane węzły pośredniczące (utrzymanie spójności sieci, bezpieczeństwa rdzenia, prawidłowego przepływu komunikatów). Odmiennie będą natomiast oceniane węzły bezpośrednio realizujące zadanie organizacji przestępstwa. Ich aktywność będzie głównie widoczna na peryferiach sieci, a relacje będą podporządkowane zdobywaniu zysków. Wytwarzanie zysków nie będzie wymagało dokonywania fizycznej ingerencji w niekryminalne sieci społeczne. W przypadku sieci przestępczych będących sieciami złożonymi pozycja danego węzła nie jest stała (dynamizm sieci), tym samym trudno jest oceniać jego rolę w organizacji jako całości. Węzły w sieci można też lokalizować według pozycji zajmowanych przez nie w stosunku do innego węzła (mikropozycja) bądź w stosunku do całego systemu (makropozycja)[51]. W przypadku organizacji przestępczych działających w sieciach teleinformatycznych niekoniecznie muszą one być budowane jako wieloosobowe. Stosowane mechanizmy przestępcze oparte na rozprzestrzenianiu się w sieciach teleinformatycznych powodują to, że potencjalne ofiary (usługobiorcy ofert przestępczych, np. gier hazardowych) sami bez aktywności węzłów organizacji sieciowej przystępują do relacji, w których wyniku organizacje przestępcze uzyskują znaczne zyski finansowe. Skuteczność działania takiego mechanizmu nie powoduje potrzeby budowania struktur wieloosobowych. Podobne rozwiązania można zaobserwować przy tworzeniu firm słupów czy rachunków bankowych, niekoniecznie wymagających istnienia konkretnych podmiotów dla fikcyjnych przepływów finansowych, a funkcjonujących wyłącznie na podstawie rejestracji na stronach e-banków. Wystarczy urealnić ich istnienie w obszarze przepływów teleinformatycznych (np. przez uprzednie zarejestrowanie w Internecie aktywności związanej z działalnością gospodarczą, służącą uwiarygodnieniu przedsiębiorcy). W konsekwencji tego rodzaju mechanizmy mogą być wykorzystywane do prania pieniędzy, wyłudzeń towarów w sklepach (aukcjach) internetowych, wyłudzeń podatkowych bądź stosowania kreatywnej księgowości.

[51] E. Stańczyk-Hugiet, J. Gorgól, *Elementy sieci międzyorganizacyjnych – aspekty organizacyjno-zarządcze*, w: *Sieci międzyorganizacyjne. Współczesne wyzwanie dla teorii i praktyki zarządzania*, J. Niemczyk, E. Stańczyk-Hugiet, B. Jasiński (red.), Warszawa 2012, C.H. Beck, s. 22.

Na zakończenie należy także zasygnalizować potrzebę zmian o charakterze legislacyjnym. Nowe struktury sieciowe wymuszają zastanowienie się nad potrzebą zmiany penalizacji zachowań organizacyjnych podejmowanych w celu popełniania przestępstw. W. Kurowski wskazuje, że dotychczasowe uregulowane zawarte w art. 258 Kodeksu karnego nie są adekwatne do tzw. przestępstwa partnerskiego[52]. To nowe podejście powinno zapewnić zarówno karanie zachowań tradycyjnych, odnoszących się do zhierarchizowanych struktur zakładanych w celu popełniania przestępstw, jak i posiadać wymiar znacznie szerszy, umożliwiający karanie nowatorskich zachowań występujących typowo w sieciach przestępczych, które czerpią organizacyjne wzorce z modeli charakterystycznych np. dla obrotu finansowego i gospodarczego.

Abstrakt

Stale zmieniająca się struktura organizacyjna grup działających w obszarze przestępczości zorganizowanej oraz terroryzmu wynika z potrzeby doskonalenia kamuflażu i przyjmowania bardziej elastycznych rozwiązań, które uniemożliwiają ich rozpracowanie przez organy ścigania. Dlatego też coraz liczniej organizacje przestępcze, budując swoje struktury, przyjmują model o charakterze sieciowym. Tym samym przed organami ścigania stają nowe, coraz trudniejsze wyzwania związane z oceną zachowań organizacyjnych, typowaniem rzeczywistego przywództwa i identyfikacją kanałów informacyjnych. Naprzeciw tym wyzwaniom wychodzą rozwiązania stosowane między innymi w naukach ścisłych (fizyce), które zostały także przetransponowane na nauki społeczne (socjofizyka). Pomocne są między innymi badania zależności (relacji) i zachowań, jakie zachodzą między poszczególnymi węzłami w sieciach złożonych.

Podążając za negatywną ewolucją zjawisk społecznych, organy ścigania powinny podjąć badania kryminalistyczne nad oceną funkcjonowania sieciowych struktur organizacyjnych. Dotyczy to nie tylko samych modeli strukturalnych, lecz także kreowania przestępstw popełnianych w przestrzeni cybernetycznej, przy wykorzystaniu mechanizmów przekazu informacji, jakie stwarzają nowoczesne komunikatory. Prowadzone w wielu krajach badania dotyczą przede wszystkim analizy zachowań organizacyjnych w skomplikowanych wewnętrznie i obszarowo strukturach przestępczych. Dzięki badaniom organy ścigania będą mogły otrzymać obiektywny obraz odwzorowujący zachowania nielegalnych organizacji, ale przede wszystkim będą mogły przyjąć najwłaściwszą taktykę przeciwdziałania ich działalności. Uzyskane w wyniku przeprowadzonych analiz wnioski mogą pozwolić w przyszłości także na dokonanie rewizji aktualnie uznawanych rozwiązań o charakterze penalnym.

Abstract

The constantly changing organisational structure of groups operating in the field of organised crime and terrorism results from their need to improve camouflage and adopt

[52] Przestępstwo partnerskie to nowa ekonomia popełniania przestępstw, na zasadzie demokracji, w której wszyscy pełnią kluczowe funkcje. Cechuje się wykorzystaniem inteligencji, pomysłowości i umiejętności rozproszonych i luźno powiązanych z sobą jednostek, wykorzystując do tego powiązania sieciowe, tworzące organizacje o ukrytej strukturze horyzontalnej, w: W. Kurowski, *Globalna gospodarka usług…,* s. 32.

more flexible solutions to prevent law enforcement authorities from their dismantling. Therefore, an increasing number of crime groups, while building their structures, adopt the model of a network. Thus, law enforcement authorities face new, more and more difficult challenges relating to the assessment of organisational behaviour, identification of the actual leadership and information channels. Solutions applied, inter alia, in science (physics) and social sciences (sociophysics) make it possible to tackle these challenges. Studies of dependencies (relations) and behaviour occuring between the individual nodes in complex networks have proven to be useful.

Due to the aggravation of social probelms, law enforcement authorities should undertake forensic examination in order to assess the functioning of the network organisational structures. It concerns not only those very structural models but also emerging crimes commited in cyberspace, by means of mechanisms for communication of information, created through the modern communicators. Studies conducted in several countries concern mainly analysis of organisational behaviour in internally complex and complicated in terms of their field criminal structures. Thanks to the studies, law enforcement authorities will be able to gain an unbiased picture reflecting behaviour of illegal groups; but above all they will be able to use the most appropriate tactics in countering their activity. Conclusions that will be obtained as a result of the conducted analyses may enable to review the currently recognized penal solutions in the future.