MACIEJ ALEKSANDER KĘDZIERSKI
ORCID: 0000-0003-3074-1355

DOI: 10.4467/20801335PBW.21.001.13558

Możliwość zastosowania inżynierii odwrotnej do zwalczania organizacji przestępczych typu sieciowego

Inżynieria odwrotna, określana także jako inżynieria wsteczna (ang. *reverse engineering*, RE), pozwala zrozumieć, jak „coś" (np. jakiś przedmiot) zostało wykonane – mimo dysponowania ograniczoną wiedzą na ten temat[1]. Próbuje zatem odpowiedzieć na pytanie, jak przebiegał proces tworzenia jakiegoś przedmiotu. Inżynieria odwrotna inaczej podchodzi do inżynierii niż inżynieria tradycyjna (postępowa). Ten drugi rodzaj inżynierii jest procesem przebiegającym od pomysłu, który jest generowany potrzebą stworzenia fizycznego produktu, do jego realizacji. Inżynieria odwrotna zaś – jak sama nazwa wskazuje – jest procesem przebiegającym od fizycznego produktu, którego wszystkie składowe są szczegółowo analizowane, a następnie rozwijane, do nowego fizycznego produktu w takiej samej bądź ulepszonej postaci[2]. Inżynieria odwrotna jest także dziedziną nauki zajmującą się wszelkimi metodami, które umożliwiają wprowadzenie realnego produktu do rzeczywistości wirtualnej. Nazwa „inżynieria odwrotna" pochodzi od kolejności wykonywania działań – najpierw jest obiekt rzeczywisty, a dopiero przy użyciu skanerów i zastosowaniu metod inżynierskich otrzymuje się obiekt wirtualny[3]. Inżynieria odwrotna znajduje zastosowanie głównie w „sztuce inżynierskiej", stąd też niekiedy jest nazywana „inżynierią rekonstrukcyjną". Zgodnie z definicją zaprezentowaną przez Elliota

---

1 K. Breeman, *How does reverse engineering relate to forensics and solving crimes?*, https://www.quora.com/How-does-reverse-engineering-relate-to-forensics-and-solving-crimes [dostęp: 14 IV 2020].

2 M. Szelewski, M. Wieczorowski, *Inżynieria odwrotna i metody dyskretyzacji obiektów fizycznych*, „Mechanik" 2015, nr 12, s. 183, http://www.mechanik.media.pl/pliki/do_pobrania/artykuly/22/40_183_188.pdf [dostęp: 15 IV 2020].

3 S. Kachel i in., *Zastosowanie inżynierii odwrotnej do procesu odtwarzania geometrii układu wlotowego silnika RD-33 w samolocie MIG 29*, „Prace Instytutu Lotnictwa" 2011, nr 213, s. 66 i nast., http://ilot.edu.pl/PIL/PIL_213.pdf [dostęp: 14 IV 2020].

Chikofsky'ego i Jamesa Crossa (…) *inżynieria odwrotna – to proces uzyskiwania wystarczającego zrozumienia na poziomie projektu o produkcie, który pomoże w jego utrzymaniu, ulepszeniu lub wymianie. To także jest część procesu utrzymania oprogramowania, która pomaga zrozumieć system wystarczająco do podjęcia decyzji w tej sprawie. W procesie tym nie jest wymagana zmiana systemu w jakikolwiek sposób*[4]. W przypadku inżynierii odwrotnej idea działania polega na zastosowaniu jej procesów w odniesieniu do obiektu materialnego, który jest kolejno mierzony, a następnie przekształcany w model. Otrzymany model może być przedmiotem dalszego badania i przekształcania w założonym celu.

Początkowo inżynieria odwrotna odnosiła się wyłącznie do analizy urządzenia technicznego (przedmiotu fizycznego). Obecnie jest ona stosowana w analizie programów komputerowych, np. w celu poznania, w jaki sposób dane oprogramowanie zostało użyte do popełnienia przestępstwa, wykrycia luk w projektowanym programie, ustalenia źródłowych kodów dostępu, wykrycia wirusowego (złośliwego) oprogramowania i jego analizy lub w celu odzyskania utraconych danych. Inżynieria odwrotna jest także wykorzystywana w analizie działań szpiegowskich dotyczących rozwiązań militarnych lub logistycznych przeciwnika. W tym przypadku szczególną rolę odgrywa zrozumienie badanego obiektu (systemu) i jego struktury. Omawiany rodzaj inżynierii jest więc procesem analizy mającym na celu zwiększenie ogólnego zrozumienia systemu – zarówno pod względem jego utrzymania, jak i umożliwienia jego dalszego rozwoju (doskonalenia)[5]. Inżynierię odwrotną wykorzystuje się zazwyczaj, aby uzyskać brakującą wiedzę bądź znaleźć pomysł na projektowanie, gdy takie informacje są niedostępne w chwili inicjacji zadania.

Proces RE jest podzielony na trzy fazy: przegląd, skanowanie podzespołów i ukierunkowane eksperymenty. W pierwszych dwóch fazach stosuje się metody statyczne (analiza statyczna), a w fazie końcowej – metody dynamiczne (analiza dynamiczna). Analiza statyczna sprawdza oprogramowanie, nie uruchamiając go i nie ryzykując uszkodzenia działającego programu. Za pomocą tej techniki eksperci mogą bezpiecznie dowiedzieć się więcej na temat kodowania takich programów, jak np. złośliwe oprogramowanie. Analiza dynamiczna polega na kontrolowanym uruchamianiu lub deasemblacji oprogramowania (tj. odtworzeniu kodu źródłowego z programu zapisanego w kodzie maszynowym[6]) w celu zrozumienia, w jaki sposób działa złośliwe oprogramowanie, przy jednoczesnym uniknięciu poważnego ryzyka dla rzeczywistych środowisk[7]. Dzięki oprogramowaniu komputerowemu jest możliwe nie tylko ustalenie i wykrycie

[4] E.J. Chikofsky, J.H. Cross II, *Reverse engineering and design recovery: a taxonomy*, „IEEE Software" 1990, nr 1, s. 13–17.

[5] E.J. Chikofsky, J.H. Cross II, *Encyclopedia of Software Engineering*, 2002, https://onlinelibrary.wiley.com/doi/abs/10.1002/0471028959.sof285 [dostęp: 15 IV 2020].

[6] *Słownik Języka Polskiego*, hasło: 'deasemblacja', https://sjp.pl/deasemblacja [dostęp: 15 IV 2020].

[7] B. Hendricks, *Reverse Engineering in Digital Forensics*, rozdział 4, lekcja 9, w: https://study.com/academy/lesson/reverse-engineering-in-digital-forensics.html [dostęp: 19 XII 2020].

powiązań sieciowych organizacji przestępczej, lecz także poznanie sposobów posługiwania się programem komputerowym przez organizację przestępczą jako instrumentem do popełniania czynów penalizowanych. Rezultat końcowy uzyskuje się w wyniku oceny relacji między elementami sieci a atrybutami cechującymi te elementy, np. na podstawie dających się zmierzyć cech (właściwości) wchodzących w skład atrybutów lub paramentów konstrukcji oprogramowania wykorzystywanych do realizacji wyznaczonego celu[8]. Taka ocena jest pomocna szczególnie wtedy, gdy organizacja przestępcza pozostająca w strukturze sieciowej dokonuje przestępstw, ataków terrorystycznych w cyberprzestrzeni albo używa specjalistycznego kodowanego oprogramowania, aby rozpowszechniać wiedzę terrorystyczną, werbować bojowników i utrzymywać kontakty ze swoimi zwolennikami. Warto zaznaczyć, że organizacje terrorystyczne również poszukują specjalistów z zakresu RE. Jest to konsekwencja chęci pójścia na skróty, braku odpowiednich środków na realizację celu i poszukiwania nowych sposobów przeprowadzania ataków terrorystycznych, np. z użyciem „brudnej broni jądrowej". Kod komputerowy napisany przez tzw. mocarstwa jądrowe może zostać przejęty (np. przez złośliwe oprogramowanie), poddany procesowi inżynierii odwrotnej, a następnie ponownie wykorzystany przez inne państwa lub podmioty niepaństwowe. Możliwe jest przyjęcie hipotetycznej sytuacji, w której grupa terrorystyczna kopiuje, a następnie poddaje procesowi RE niszczycielski wojskowy program komputerowy, utworzony na potrzeby ataku przeciw innym krajom, a następnie kieruje go na ustanowione przez siebie cele.

Powstaje więc pytanie, czy inżynierię odwrotną można zastosować nie tylko do odtwarzania, uzupełniania, udoskonalania rzeczy, oprogramowania i poszerzania wiedzy, lecz także do udoskonalenia przeprowadzonej procedury analitycznej, w której przedmiotem diagnozy jest organizacja typu sieciowego. A jeżeli jest to możliwe, to w jakim zakresie?

Wykorzystanie inżynierii odwrotnej jako obszar badawczy

Przestępczość jako zjawisko społeczne jest podporządkowana innym regułom niż działanie obiektów fizycznych. Mówi się o tzw. inżynierii społecznej (ang. *social engineering*), która odnosi się w zasadzie do socjologii (a w omawianym przypadku – mikrosocjologii) i jest związana ze stosowaniem wielu metod i technik służących osiągnięciu określonych celów, w tym manipulacji społeczeństwem (socjotechnika). Zbieżność nazwy nie oznacza jednak zbieżności pojęciowej. Natomiast sam proces działania (aktywizowania czynności) można uznać za proces inżynieryjny. Zjawiska, jakie zaszły w poprzednich latach, w tym postęp technologiczny, doprowadziły do nowego „umieszczenia" społeczeństwa w wirtualnej rzeczywistości, w której relacje społeczne

[8] Dotyczy dla przykładu: zestawu instrukcji, zaimplementowanych interfejsów i zintegrowanych danych, także utworzonych w sposób autorski, cechujący indywidualnego twórcę.

zostały ujęte ilościowo i wyrażone wzorami matematycznymi. Przeniesienie społeczeństwa do Internetu umożliwiło zastosowanie innego sposobu monitorowania zachowań jednostek – za pomocą technologii komunikacyjnych i zarządzania dystrybucją informacji. Jest to konsekwencja z jednej strony udostępniania ludziom urządzeń z różnymi niezbędnymi dla nich aplikacjami wywierającymi wpływ na ich aktywności, podejmowanie decyzji bądź planowanie działań w czasie, z drugiej zaś – umieszczania w przestrzeni publicznej przez ustawodawcę i organy władzy rozwiązań ułatwiających realizację spraw osobistych (e-bankowość, e-urząd, e-sądy) i połączenia użytkownika z tymi rozwiązaniami. Osoby korzystające z takich aplikacji zostawiają ślad w przestrzeni teleinformatycznej. Tak technologicznie (inżynieryjnie) stworzone społeczności są aktywne w matrycach zbudowanych na rozwiązaniach matematycznych, kreujących nową rzeczywistość, także tę sprzeczną z prawem. Nie byłoby możliwe zastosowanie inżynierii odwrotnej do badania zachowań struktur społecznych, gdyby nie wprowadzono do niej rozwiązań z zakresu sieci społecznych czy teorii grafów. Dzięki temu można było uporządkować zachowania jednostki i tworzone przez nią formy organizacyjne.

Działania jednostki są umieszczane na technologicznej matrycy, co umożliwia zarówno sterowanie procesami społecznymi, jak i ich kontrolowanie. Dzięki temu przy analizowaniu zjawisk społecznych można posłużyć się rozwiązaniami, które pod względem technologicznym powinny być raczej przypisane nie badaniom społecznym, a technicznym. Społeczeństwo (lub jego część) traktuje się wówczas jako układ złożony.

Systemy (układy) złożone mają pewne własności potwierdzone w praktyce, np. wrażliwość na początkowe warunki lub małe zakłócenia, mnogość interakcji między ich różnymi elementami. Wszystkich ich własności nie da się w prosty sposób przewidzieć po zbadaniu własności ich poszczególnych komponentów, ponieważ ciągle ewoluują i się rozwijają (dynamika)[9]. W celu określenia charakterystycznych cech układu będzie można zastosować następujące właściwości: miarę centralności wierzchołków[10] (charakteryzowaną przez: bliskość[11], stopień[12], promień, pośrednictwo[13],

[9] Zob. A. Fronczak, P. Fronczak, *Świat sieci złożonych: Od fizyki do Internetu*, Warszawa 2009; Z. Tarapata, *Czy sieci rządzą światem? Od Eulera do Barabasiego*, „Biuletyn Instytutu Systemów Informatycznych" 2012, nr 10, s. 37.

[10] Centralność jednostki (reprezentowanej przez węzeł w grafie) określa stopień zaangażowania jednostki w relacje z innymi jednostkami. Centralność może zostać wyrażona przez: stopień węzła, bliskość jednostki do innych jednostek, częstość występowania jednostki w charakterze pośrednika w procesie komunikacji między innymi jednostkami. Zob. P. Lula, *Analiza struktury serwisów WWW*, Uniwersytet Ekonomiczny w Krakowie, http://www.ae.krakow.pl/~lulap/WM_2009_04.pdf [dostęp: 11 II 2021].

[11] Zgodnie z tą miarą wierzchołek jest tym bardziej centralny, im jest bliżej wszystkich innych wierzchołków sieci.

[12] Stopień wierzchołka v w grafie G to liczba krawędzi dochodzących do tego wierzchołka.

[13] Pośrednictwem (ang. *betweenness*) węzła v nazywa się stosunek liczby najkrótszych ścieżek między dowolnymi dwoma węzłami przechodzących przez węzeł v do łącznej liczby wszystkich najkrótszych ścieżek.

współczynnik gronowania[14]) oraz stopień pośrednictwa elementów pośredniczących i peryferyjnych[15].

Pod pojęciem analiza sieci społecznej (ang. *social network analysis*, SNA), oznaczającym jedną z metod technicznych przedstawiających relacje między węzłami (wyznaczonymi elementami społeczności), należy rozumieć mapowanie i mierzenie relacji oraz przepływów między osobami, grupami, organizacjami, komputerami, adresami URL i innymi powiązanymi jednostkami informacji (wiedzy). Zmapowane relacje tworzą sieć, która pokazuje zależności lub przepływy między węzłami. Węzły w sieci to ludzie i grupy, podczas gdy połączenia (łącza) wskazujące na zależności lub przepływy między węzłami to krawędzie lub relacje. Analiza sieci społecznej zapewnia zarówno wizualną, jak i matematyczną ocenę relacji międzyludzkich[16].

Badania ukierunkowane na działania organizacyjne pozwoliły na stworzenie pojęć: analiza sieci organizacyjnych (ang. *organizational network analysis*, ONA), czyli zastosowanie SNA wobec organizacyjnych (sieciowych) form społecznych, oraz analiza sieci kryminalnych (przestępczych) (ang. *criminal network analysis*, CNA). Analiza sieci organizacyjnych to uporządkowany sposób wizualizacji przepływu przez organizację komunikacji, informacji i decyzji. Sieci organizacyjne składają się z węzłów i powiązań stanowiących podstawę do zrozumienia, w jaki sposób informacje przepływają w organizacji. Należy jednak pamiętać, że CNA to nie SNA. Za taką tezą stoi argument, że organizacje przestępcze z założenia działają w „niewidzialnej przestrzeni", kamuflują i zatajają swoją aktywność niezgodną z prawem, stawiają sobie inne cele i przyjmują taktykę działania odmienną od ustanowionych i akceptowanych norm państwowych i społecznych. Dlatego też trudno zakładać, że tego rodzaju struktury będą się uzewnętrzniać w sieciach społecznościowych. Można natomiast spotkać się z innymi działaniami tych struktur, które są widoczne w aktywności związanej z przygotowaniami do przestępstwa, legalizowaniem przestępczych aktywów lub ich inwestowaniem czy wręcz wynikają z popełnienia błędów polegających na zbytnim uzewnętrznianiu się ze swoim przestępczym statutem w sieci internetowej lub w świecie realnym. Te rodzaje działań wymagają prowadzenia rozpoznania również w otwartych źródłach informacji (sieć powierzchniowa), a przynajmniej w tzw. ukrytym Internecie czy czarnej sieci (ang. *Darknet*). Analiza sieci kryminalnych odnosi się do relacji

[14] Definiuje się go jako prawdopodobieństwo istnienia połączenia między parą węzłów, które mają przynajmniej jednego wspólnego sąsiada.

[15] Szczegółowo zob. Z. Tarapata, *Czy sieci rządzą światem?…* Podczas kształtowania się sieci społecznych dochodzi do efektu gronowania się (grupowania) ludzi o podobnych poglądach, zainteresowaniach, a także do uczestniczenia w naruszaniu prawa itp. Zob. także: M. Morzy, A. Ławrynowicz, *Wprowadzenie do analizy sieci społecznych*, Poznań 2010/2011, https://socnetwork.files.wordpress.com/2011/02/podstawowe-wc582ac59bciwoc59bci.pdf [dostęp: 16 IV 2020].

[16] Ł. Wawrzynek, *Analiza sieci społecznych w identyfikacji i wzmacnianiu potencjału innowacyjnego zespołów pracowniczych*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Research Papers of Wrocław University of Economics" 2017, nr 496, s. 183 i nast.

zachodzących w ramach nieformalnych, kryminalnych bądź terrorystycznych form organizacyjnych.

Rozwiązania przedstawione w artykule pozwalają przenieść relacje społeczne za pomocą wzorów matematycznych w obszar, który będzie można badać z wykorzystaniem RE. Metody stosowane w analizie sieci służą odtajnieniu i ujawnieniu ukrytych w niej danych oraz przedstawieniu ich jako wzorce ludzkich możliwości. Niezależnie od stosowanych określeń odnoszących się do organizacyjnych form popełniania przestępstw (zorganizowana przestępczość, organizacja terrorystyczna) występują różnice wewnątrzorganizacyjne, charakterystyczne dla danej organizacji, co wyróżnia ją spośród innych, podobnych form przestępczych. Dlatego też najpierw powinno się podjąć czynności zmierzające do oceny funkcjonowania takiej organizacji w sieci społecznej. Będzie można ocenić stopień integracji (stan zespolenia) oraz charakterystyczne zachowania przynależne jedynie tej organizacji (wewnętrzny kod organizacyjny) oraz wzajemne relacje organizacji z otoczeniem. Zastosowanie RE i analizy sieci społecznych powinno umożliwić zdobycie wiedzy o niewidocznych relacjach, a nie tylko o prostych, formalnie zdefiniowanych powiązaniach. Więzi nieformalne często w większym stopniu determinują i odzwierciedlają sposób pracy niż wyznaczone role i pozycje w strukturze formalnej (dane relacyjne i atrybuty)[17]. Wynikiem zastosowania RE i CNA powinno być nie tylko odtworzenie zachowań węzłów i samej organizacji jako sieci (jak w analizie kryminalistycznej[18]), lecz także „wytworzenie" tych relacji, które dotychczas były ukryte dla organów ścigania i dlatego nie zostały poddane czynnościom weryfikacyjnym czy sprawdzeniowym[19]. Odnosi się to zarówno do niewykrytych zachowań osób fizycznych, jak i zaszyfrowanych komunikatów (relacji) w sieci teleinformatycznej, korzystania z zamkniętych forów dyskusyjnych oraz ukrytego Internetu. Brak takiej wiedzy może spowodować przyjęcie niewłaściwej taktyki zwalczania przestępczości oraz niepoprawne wytypowanie sprawców, zleceniodawców i kierownictwa organizacji. Na przedmiot objęty analitycznym podejściem RE należałoby spojrzeć z dwóch stron. Pierwszej, w której przedmiotem jest organizacja przestępcza jako nieformalny twór przynależności i wspólnego działania kryminalnego (ujmowany w kategorii interpersonalnego związku przestępczego). Drugiej zaś, w której organizacja przestępcza jest określana jako podmiot organizacyjny (firma, sieć sprzedaży,

[17] Tamże, s. 189. Relacje (komunikacja, współdziałanie) wskazują na właściwą merytorycznie i rzeczywistą rolę danej jednostki w organizacji.

[18] W ramach badań kryminalistycznych poszczególnych przedmiotów, typowanych jako przedmioty (dowody) przestępstwa, również jest możliwe zastosowanie RE. Zob. T. Kurzynowski i in., *Proces inżynierii odwrotnej w zastosowaniach kryminalistycznych*, „Problemy Kryminalistyki" 2014, nr 285, s. 4–46.

[19] Działania uzupełniające mogą być konsekwencją przekazania dodatkowych informacji ze źródeł krajowych, zagranicznych jednostek policji czy służb, wykonania międzynarodowej analizy przez np. Interpol czy Europol, wykonania analizy informacji finansowej przez krajową Jednostkę Analityki Finansowej (GIIF) lub też na potrzeby dokonania ponownej analizy materiałów przez jednostkę prowadzącą daną sprawę.

instytucja finansowa) będący pod kontrolą grupy osób. W tym przypadku przedmiot organizacyjny staje się całościowo instrumentem do popełnienia określonego rodzaju przestępstwa (np. podmioty gospodarcze powołane w celu dokonania przestępstwa oszustwa na szeroką skalę – piramidy finansowe).

Próba oceny możliwości zastosowania inżynierii odwrotnej do badań nad sieciowymi strukturami przestępczymi

Wysoka technologizacja zachowań społecznych pozwala na rozważenie możliwości wprowadzenia RE w obszar zjawisk międzyludzkich (społecznych). Będzie można wówczas zbadać, dlaczego ktoś nie zachował się tak, jak powinien, lub też spowodować, aby ktoś zachował się tak, jak to zostało zaplanowane. Tego rodzaju elementy byłyby możliwe do wykorzystania na potrzeby taktyki zwalczania przestępstw, w tym do prowadzenia przez agenta swoistej gry z przeciwnikiem, np. w ramach operacji specjalnej jako czynności operacyjno-rozpoznawcze. Inżynieria odwrotna może być pomocna nie tylko przy wskazywaniu przyczyn niepowodzeń w procesach wykrywczych (np. z wykorzystaniem inżynierii postępowej), lecz także służyć poprawianiu efektów tych procesów przez wykrywanie ich możliwych wad (błędnej oceny poszczególnych relacji, węzłów i całości sieci).

Inżynieria odwrotna ma na celu przedstawienie schematu systemu, który pozwoli przewidzieć problemy, dokonać poprawek lub dowiedzieć się, co poszło nie tak w procesie budowania systemu lub narzędzia i gdzie popełniono błąd[20]. W przypadku oddziaływania na systemy inżynierię odwrotną można postrzegać technicznie przez pryzmat zastosowanych i modelowanych programów komputerowych (np. poszukując luk w oprogramowaniu, ustalając tzw. *zero-day*[21] stosowany w celu użycia złośliwego oprogramowania) lub przez usystematyzowane procesy przeciwdziałania popełnianiu przestępstw. Uporządkowanie procesów wykrywczych w ramach prowadzonych czynności operacyjnych i kryminalistycznych pozostaje więc istotne z punktu widzenia taktyki zwalczania przestępczości, która powinna uwzględniać podejście systemowe. Oznacza to również, że na nieuporządkowane działanie społeczne, w tym niezgodne z prawem, należy reagować w adekwatny sposób. Taktyka działań będących reakcją na zdarzenie przestępcze powinna zostać usystematyzowana, a przede wszystkim powinna znormalizować rzeczywistość, ale również powinna być odbierana jako działanie organu ścigania. Oznacza to możliwość przyjęcia określonego wzorca dla modelu postępowania, od którego odchylenia będą świadczyły o nieprawidłowościach. Ich ocena sytuacyjna będzie zmierzała do

[20] ABL Engineering, *What Are the Different Types of Reverse Engineering Tools?*, https://ablengineering.com.au/What-Are-the-Different-Types-of-Reverse-Engineering-Tools-~69 [dostęp: 19 XII 2020].

[21] Atak *zero-day* to atak, który wykorzystuje lukę *zero-day* w celu zainstalowania złośliwego oprogramowania.

ustalenia, czy odchylenie pozostaje w normie i nie narusza dobra chronionego prawem, czy też stanowi czyn karalny z punktu widzenia ustawodawcy. Takie postępowanie wynika z potrzeby wyodrębnienia z działań społecznych takich z nich, które – zgodnie z wolą ustawodawcy – są działaniami przestępczymi (stanowią więc specyficzne działania niezgodne z przyjętymi normami społecznymi) i nie mieszczą się w granicy postępowania dozwolonego prawem. Systemowe podejście do czynności mieszczących się w zakresie przeciwdziałania i zwalczania przestępczości ma ten walor, że w ramach RE jest możliwe przeanalizowanie zaistniałych procesów decyzyjnych, sprawdzenie ich zgodności z przyjętymi wzorcami oraz skorygowanie realizacji zadań.

Zastosowanie metody inżynierii odwrotnej jest pomocne nie tylko w przeprowadzeniu audytu bezpieczeństwa, wykryciu oszustwa lub ukrywania się przestępców w sieci, lecz także wykryciu wykorzystania jej elementów, atrybutów lub struktury na potrzeby przestępcze. Umieszczenie forów społecznościowych, e-zakupów, e-usług (w tym finansowych). które są wykorzystywane również w celach przestępczych, w przestrzeni wirtualnej, pozwala na pozyskiwanie śladów działań przestępców i otrzymanie w ramach RE pełniejszego obrazu modelu przestępczego wykreowanego przez sprawcę (elementy sieci). Użycie instrumentów z przestrzeni wirtualnej pozwala też na budowanie schematu postępowania zarówno w fazie przygotowania, jak i dokonania przestępstwa.

Istotnymi elementami postępowania sprawców przestępstw jest ich kamuflowanie się, tajność, zacieranie przez nich śladów oraz wprowadzanie w błąd. Dlatego też organy ścigania podejmują wysiłki, aby odtworzyć przebieg zdarzenia przestępczego, wytypować konkretną osobę jako sprawcę czynu przestępczego oraz przypisać jej dokonanie tego czynu. Niestety, wielokrotnie ten obraz jest niepełny, zawiera luki w wiedzy o przebiegu zdarzenia, które nie ułatwiają wykazania związku przyczynowo-skutkowego między zdarzeniami lub pozwalają przypisać winę i popełnienie przestępstwa danej osobie jedynie w określonym stopniu. Inżynieria odwrotna daje organom ścigania dodatkowe możliwości uzupełnienia dotychczasowego obrazu przestępstwa przez rozbicie go na czynniki pierwsze i wykorzystanie metod oraz technik umożliwiających uzupełnienie luk i poszerzenie pola działania. Analizowanie przestępstwa oparte na modelowaniu inżynierskim może się odnosić między innymi do badania kryminalistycznego przedmiotów zabezpieczonych na miejscu zdarzenia (w tym otrzymania ich modelu w wersji 3D dzięki digitalizacji za pomocą skanera) lub też do przedmiotów uzyskanych w wyniku przeszukania miejsca, które zostało wytypowane jako to, w którym przebywał sprawca. Oznacza to możliwość technicznego odtworzenia brakującej części przedmiotu, istotnego ze względu na prawdopodobieństwo użycia go na miejscu zdarzenia przestępczego, wykonania całościowej ekspertyzy kryminalistycznej, a także przeprowadzenia analizy: od zdarzenia przestępczego do jego sprawcy.

Możliwość zastosowania metody RE do zwalczania organizacyjnych form przestępczych typu sieciowego (zorganizowane grupy przestępcze, organizacje terrorystyczne) jest sprawą otwartą. Inżynieria odwrotna to proces pomiarowy, zatem zmierzenie zjawisk społecznych będzie możliwe jedynie wtedy, gdy relacje społeczne

będzie można przełożyć na mierzalne modele. Im więcej obszarów społecznych będzie przedmiotem badań pomiarowych i im doskonalsze będą instrumenty badawcze, tym łatwiej będzie można przełożyć otrzymane wyniki na wzorce analityczne, które są skoncentrowane na badaniach zjawisk przestępczych[22]. Takie rozwiązania dają między innymi: teoria grafów, algebra macierzowa, statystyka, miarowanie mediów społecznościowych (ang. *social media*)[23], SNA, CNA, ale też RE, jeśli się założy istnienie racjonalnego konstruktora sieci, a w omawianym przypadku – założyciela zorganizowanej grupy przestępczej lub organizacji terrorystycznej. Stąd też RE można zastosować, gdy istnieje możliwość zmierzenia związku przestępczego (sieci przestępczej) lub czynności realizowanych przez podmiot organizacyjny (np. korzystania ze stron internetowych, mediów społecznościowych, SMS-ów, serwisu personalnego, e-maili, reklamy medialnej, sprzedaży w sklepie lub świadczenia usług) oraz gdy takie działania służyły do popełnienia przestępstwa. I w jednym, i w drugim przypadku organy ścigania mają możliwości pozyskania informacji, które będzie można przetworzyć na wyznaczniki. Te zaś będzie można zmierzyć (bilingi telefoniczne, dane z GPS samochodów, bramki poboru opłat drogowych, informacje pochodzące z obserwacji czy kontroli operacyjnej bądź analizy kryminalnej). Trudności powstają w momencie, gdy nie jest możliwe pozyskanie danych w celu poddania ich analizie. Dotyczy to drobnych przestępstw (np. oszustw), które nie są zgłaszane. Powody niezgłaszania są różne: zbyt drobne kwoty, unikanie utraty zaufania do przedsiębiorstwa, zatrzymywanie danych przez duże firmy i korporacje ze względu na chęć ograniczenia odpowiedzialności decydentów. W takich przypadkach roszczenia osób poszkodowanych są zaspokajanie z własnych funduszy firmy. W konsekwencji analityk otrzymuje niepełny obraz, a wręcz brakuje śladów istotnych przy typowaniu obszarów analitycznych. W takiej sytuacji będzie pomocne zastosowanie analizy predykcyjnej[24] lub inżynierii odwrotnej.

Kryminalistyka jako nauka wspierająca działania wykrywcze i służąca poznawaniu sposobów popełniania przestępstw wymaga gromadzenia dowodów, które następnie podlegają procesowi badawczemu (inżynieria kryminalistyczna). Aby właściwie zebrać

---

[22] Dla przykładu: modelowanie sieci bezskalowych (R. Albert, A.-L. Barabási), odkrywanie społeczności lokalnych, klik w sieciach społecznych (K. Faust, J. Scott, S. Wasserman), rozwijanie problemu hierarchii w sieciach (A.-L. Barabási, S.N. Dorogovtsev, E. Ravasz). Zob. szerzej: M. Kowalska-Musiał, *Strukturalna metodologia pomiaru sieci społecznych – rys historyczny i współczesne obszary zastosowań*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2013, nr 28, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ekon-element-000171350117 [dostęp: 15 II 2021].

[23] Zob. M. Lewandowski, *Pomiar mediów społecznościowych jako element zarządzania wiedzą i informacją w przedsiębiorstwach*, „Acta Universitatis Nicolai Copernici. Zarządzanie" 2018, nr 4, s. 117 i nast., https://apcz.umk.pl/czasopisma/index.php/AUNC_ZARZ/article/view/AUNC_ZARZ.2018.049/17178 [dostęp: 16 IV 2020].

[24] Analityka predykcyjna (ang. *predictive analytics*; wymiennie stosuje się też pojęcia *data mining* lub *data science*) to proces wydobywania informacji z istniejących zbiorów danych w celu określenia wzorów i przewidywania przyszłych zdarzeń i trendów. Za: https://algolytics.pl/analityka-predykcyjna-slownik-pojec/ [dostęp: 15 II 2021].

dowody, śledczy muszą zrozumieć zdarzenie, z którym mają do czynienia. Ponieważ nie wszystkie zdarzenia są typu *open source* lub dobrze udokumentowane, konieczne może być zastosowanie inżynierii odwrotnej, aby uzyskać dostęp do dowodów lub zrozumieć warunki użycia danego dowodu. Przykładowo tylko niektóre programy komputerowe są typu otwartego, czyli ich użytkownicy mogą zobaczyć, jak zostały napisane. Wiele programów tego nie umożliwia – ich użytkownicy nie mogą zobaczyć kodu, udostępnić go innym osobom ani zmodyfikować (są one stosowane do zamkniętych formatów danych, rozszerzeń kompatybilności i uzupełniania brakującej części kodu). W takich przypadkach ważne jest, aby zespół zajmujący się kryminalistyką cyfrową zdekonstruował to oprogramowanie i pracował nad nim krok po kroku. Poznanie elementów oprogramowania pomaga w szukaniu dowodów przestępstwa lub lepszym zrozumieniu znaczenia dowodów już odkrytych[25]. Inżynierowie mogą więc odegrać istotną rolę w dochodzeniu w sprawie o przestępstwo i służyć specjalistyczną wiedzą oraz umiejętnościami z zakresu inżynierii odwrotnej, które – jak już wspomniano – mogą zostać wykorzystane do opracowania technologii ułatwiających pozyskiwanie dokładniejszych informacji z zebranych dowodów.

O ile możliwe jest zastosowanie RE w technice kryminalistycznej, o tyle do oceny pozostaje, czy z tego typu rozwiązania można korzystać w analizie kryminalnej[26]. Czy istnieje możliwość zastosowania metody inżynierii odwrotnej w odniesieniu do zjawisk (np. funkcjonowania nieformalnych struktur organizacyjnych) lub do postępowania przestępczego, a nie tylko do regulacji czy konstrukcji technicznych opartych na ścisłych parametrach i wyliczeniach (podobnie jak ONA, ang. *organizational network analysis*, która jest sieciową analizą organizacji wykorzystywaną do oceny i zoptymalizowania relacji w ramach organizacji sieciowej). Ponadto na przedmiotową sprawę należałoby spojrzeć zarówno z punktu widzenia posiadania odpowiednich narzędzi do pozyskania i wyliczenia technicznych (metrycznych) parametrów danej organizacji przestępczej, jej sieci lub całości zjawiska, jak i postawionego celu ostatecznego. Tym celem może być zarówno neutralizacja organizacji przestępczej, jak i ocena skali zjawiska w granicach konkretnego kontynentu czy nawet świata, a także wskazanie trendów rozwojowych i ich kierunków. Zastosowanie RE pozwala na ustalenie, jak dany produkt działa, oraz na sprawdzenie, dlaczego dany mechanizm nie zadziałał, czyli dlaczego niektóre produkty zawodzą[27]. Oceniając brak wystarczającej wiedzy, należy określić luki między obecną rzeczywistością (stanem oceny funkcjonowania nieformalnej organizacji) a pożądaną przyszłością (wypełnieniem wiedzy o niej w celu określenia sił i środków do dokonania jej optymalnej neutralizacji). Podstawowym produktem wyjściowym

[25] B. Hendricks, *Reverse Engineering*…

[26] Zob. T. Kurzynowski i in., *Proces inżynierii odwrotnej*…, s. 42–46.

[27] Zob. oceny dokonane przez Colina Gagga, wykładowcę inżynierii sądowej na Open University w Milton Keynes w Anglii. C. Gagg, *Domestic product failures – Case studies*, „Engineering Failure Analysis" 2005, nr 5.

będzie w tym przypadku konstrukt[28] organizacji przestępczej, której „wytwórcą" pozostaje analityk lub inny funkcjonariusz organów ścigania dokonujący rozpoznania nie tylko konkretnych przestępstw, lecz także nieformalnej struktury mającej wpływ na rodzaj dokonywanych działań przestępczych, ich wykonawstwo oraz ich rezultat[29].

Źródłem wiedzy o samej organizacji, jej wewnętrznym zarządzaniu, podziale ról i przypisaniu przestępstw do konkretnych sprawców pozostają zarówno osoby fizyczne, jak i techniczne instrumenty analityczne i rejestracyjne będące w dyspozycji organów ścigania. Nie zawsze zasób pozyskanej wiedzy pozwoli na ustalenie, jak działa taka organizacja. Zwłaszcza gdy charakteryzuje się ona wysokim stopniem tajności, strukturą chroniącą przywódców, zleceniodawców oraz decydentów, a także gdy organy ścigania mają niepełną wiedzę na temat liczby przestępstw popełnionych przez tę organizację. Pomocne może być rozwiązanie w zakresie zarządzania zasobami ludzkimi (ang. *human resources*, HR) dla organizacji biznesowych, które zaproponowała firma ProSky. Według niej do oceny organizacji (w sensie struktury zarządczej) przyjęcie typowego schematu organizacyjnego typu „góra–dół" nie jest rozwiązaniem uniwersalnym, a próba zmuszenia firmy do przestrzegania tych standardów nie jest skuteczna. Zamiast tego zaproponowano podjęcie czynności od dołu organizacji i kontynuowanie działania „w górę", tworząc najpierw ścieżki dla każdego pracownika w organizacji. Po wprowadzeniu tych ścieżek schemat organizacyjny jest poddawany inżynierii wstecznej na podstawie potrzeb konkretnej firmy i prawdziwej struktury władzy[30].

Należy również odróżnić pojęcie i n ż y n i e r i a s ą d o w a (kryminalistyczna) od pojęcia i n ż y n i e r i a o d w r o t n a. Pojęcie „inżynieria sądowa" jest związane z prowadzonym postępowaniem i zastosowaniem metod kryminalistycznych, np. kryminalistyki cyfrowej (ang. *digital forensic*), i polega na przeprowadzeniu badań śladów pozostawionych w wyniku aktywności sprawcy (przypuszczenie, że ślady pozostawił sprawca) lub zaniechania przez niego dokonania przestępstwa. Tym samym materiał dowodowy pozostaje bez zmian i kolejno podlega różnego rodzaju badaniom w celu przyporządkowania śladu do określonego sprawcy bądź odtworzenia przebiegu zdarzenia przestępczego. Te czynności są realizowane na potrzeby postępowania prowadzonego przed prokuratorem lub sądem. „Inżynieria odwrotna", jako pojęcie znacznie szersze

---

[28] Pewna abstrakcyjna, logiczna całość złożona z danych elementów (przyp. red.).

[29] W rzeczywistości w działaniach operacyjnych służb realizuje się zadanie polegające na sporządzeniu równoległej rekonstrukcji organizacji przestępczej, która jest rozpoznawana lub rozpracowywana. Taka rekonstrukcja może dotyczyć zarówno jej nazwy, przywódców, zakresu działania, utrzymywania kontaktów z otoczeniem, używanych środków łączności, jak i przypisania poszczególnych przestępstw członkom tej organizacji jako sprawcom. Niestety, tego rodzaju czynności analityczne są konsekwencją pozyskiwania informacji od innych funkcjonariuszy (np. na podstawie błędnych informacji od osobowego źródła, niewłaściwego zakwalifikowania meldunku informacyjnego, braku doświadczenia w czynnościach zawodowych) albo w związku z działaniami na danych świadomie obarczonych błędami, np. w celu ukrycia rzeczywistego przywództwa organizacji lub pośrednich decydentów w sieci.

[30] D. Chen, *Reverse-engineering the Org Chart*, ProSky, 19 XII 2020 r., https://talkingtalent.prosky.co/articles/reverse-engineering-the-org-chart [dostęp: 21 XII 2020].

niż pojęcie „inżynieria kryminalistyczna", jest metodą badawczą, która może, ale nie musi, służyć celom postępowania przygotowawczego. Nie jest ona zatem ograniczona ramami zarówno postępowania karnego (w tym metodyki postępowania biegłych w trakcie prowadzonej ekspertyzy), jak i skonkretyzowanej oceny w danej sprawie, chyba że zostanie w tym celu wykorzystana. Nie oznacza to jednak, że w zakresie zastosowania RE występuje pełna dowolność. Po pierwsze, zastosowanie RE przez odpowiednie organy musi odbywać się w granicach prawa. Dotyczy to zarówno ram postępowania, jak i określonego celu, który ma być osiągnięty. Po drugie, inżynieria odwrotna jest związana ze skonstruowanym już urządzeniem, opracowaniem technicznym jego funkcjonowania bądź z faktami, które już wystąpiły i zostały poddane badaniu. Inżynieria kryminalistyczna polega zazwyczaj na: odzyskiwaniu niepowiązanych obiektów systemu plików (np. usuniętych plików) czy odzyskiwaniu przez pamięć podręczną historii przeglądania i jest zwykle wykorzystywana, aby wyegzekwować prawo. Natomiast RE polega na określeniu, według jakich zasad działa produkt. W tym celu przegląda się pliki binarne (lub pliki wykonywalne), a następnie wskazuje wzorce, dekompilacje[31] plików binarnych wykonywalnych, służące określeniu intencji kodu czy przeglądaniu skrzynek. Celem jest ustalenie nominalnego zachowania w odniesieniu do danych[32]. Inżynieria odwrotna analizuje kod lub plik binarny pliku (systemu) i pokazuje, w jaki sposób jest on skonstruowany i jak działa. Zwykle RE jest stosowana do celów interoperacyjności[33]. Podsumowując, inżynieria kryminalistyczna wskazuje na to, kto i jak czegoś dokonał, a inżynieria odwrotna – jak to działa. Dlatego też inżynieria odwrotna odnosi się raczej do instrumentu, jaki został użyty, niż do tego, kto go używał.

Inżynieria odwrotna ma także swoje zastosowanie w działaniach antyterrorystycznych i antykryzysowych, a zwłaszcza w ocenie praktyki analizy wywiadowczej i prawidłowości reagowania na zagrożenie. Informacje, które się wykorzystuje, to przede wszystkim „twarde dane", np. data wjazdu do kraju, identyfikacja osób zajmujących się obsługą i komórkami logistycznymi (zapleczem terrorystycznym zapewniającym bezpieczeństwo przed dokonaniem zamachu), zarządzanie komunikacją i informacją, identyfikacja podmiotów, które dostarczyły fałszywe dokumenty tożsamości, identyfikacja kierownictwa i najważniejszego członka grupy terrorystycznej, używanej poczty elektronicznej, ustalenie liczby rekrutowanych młodych ludzi, szczegółów dotyczących przyszłych ataków. Te dane powinny być przydatne do rozpracowania sieci terrorystycznej, metod jej finansowania i zakłócenia tego procederu, identyfikacji sieci, a w konsekwencji – do aresztowania członka komórki logistycznej oraz doprowadzenia do uniknięcia zrealizowania zamachu. Traktując RE jako (…) *proces pozyskiwania informacji o fizycznym produkcie oraz*

[31] Odtworzenie postaci źródłowej programu na podstawie jego kodu wynikowego (przyp. red.).

[32] Chodzi tu o ustalenie wartości wielkości fizycznych charakterystycznych dla jakiegoś urządzenia, maszyny itp.

[33] Forum dyskusyjne, odpowiedź udzielona Pranitowi Kothariemu na pytanie: *What is difference between Digital Forensic and Reverse Engineering?*, https://stackoverflow.com/questions/18289773/what-is-difference-between-digital-forensic-and-reverse-engineering [dostęp: 14 IV 2020].

ich analizowania i przetwarzania w celu opracowania technicznych danych i wytworzenia nowego produktu w takiej samej bądź ulepszonej postaci[34], można zauważyć, że pozostaje ona mocniej związana z kryminalistyką badającą obiekty fizyczne niż z zachodzącymi zjawiskami przestępczymi. Wynika to prawdopodobnie ze zadecydowanie łatwiejszego włączenia konstrukcji fizycznego przedmiotu w określony schemat podlegający następnie badaniu (szczególnie przez zebranie wielu danych technicznych, które można zmierzyć, o właściwościach oraz konstrukcji przedmiotu), ale też z posiadania odpowiednich narzędzi i dokonania precyzyjnego zmierzenia badanych obiektów[35]. Dlatego też ważne jest zabezpieczanie przez organy ścigania urządzeń wykorzystywanych np. przez terrorystów do wzajemnego komunikowania się, pozyskiwania z zewnątrz środków finansowych na działalność, koordynowania zaplecza logistycznego czy przygotowania i organizacji zamachu terrorystycznego. Zwłaszcza gdy dane urządzenie zostaje przerobione na potrzeby terrorystyczne lub od początku jest świadomie wykonane w tym celu.

Inżynieria odwrotna pozwala na szczegółowe rozpracowanie schematu funkcjonowania istniejącego urządzenia albo skonstruowanie nowego, które jednocześnie stanie się mechanizmem wewnętrznego rozpoznania aktywności terrorystycznej (np. przez zamianę urządzenia na takie samo, ale kontrolowane przez organy ścigania w ramach zastosowania techniki operacyjnej). Może to ułatwić zgromadzenie śladów potrzebnych do badań kryminalistycznych lub wykorzystanych później jako materiał dowodowy w prowadzonym postępowaniu karnym bądź jako przedmiot badań biegłego. Wydaje się więc, że istnieje możliwość wykorzystania RE zarówno w taktyce śledczej (jako określony i zastosowany w danej sprawie plan działania organu ścigania, decydujący o wyborze konkretnych, najlepszych i najodpowiedniejszych środków technicznych), jak i w analizie taktyki przestępczej, czyli sposobu popełnienia przestępstwa przez sprawcę (sposoby, metody i środki przestępczego działania). Ten drugi obszar odnosi się bardziej do podejmowania działań w zakresie czynności operacyjno-rozpoznawczych. Poddany analizie „przedmiot–model" może być niekompletny, gdyż nie będzie można wprowadzić do niego np. danych o stanach emocjonalnych sprawcy, a także nie będzie możliwe pozyskanie pełnej wiedzy o przygotowaniu do popełnienia przestępstwa. Jednak szeroki wachlarz zarówno instrumentów śledczych, jak i przedmiotów lub programów używanych przez sprawcę powinien pozwolić na zbudowanie modelu na tyle kompletnego, że będzie go można odtworzyć na poziomie RE (podobnie jak przy odtworzeniu mechanizmu bez możliwości wglądu w jego rysunek konstrukcyjny i instrukcję obsługi). Przy wykonywaniu określonych czynności wykrywczych jest możliwe zaistnienie elementów indywidualnych zachowań osób realizujących te czynności, co może skutkować subiektywnym charakterem działań podejmowanych wobec przestępców. Jest to sytuacja podobna do

[34] M. Szelewski, M. Wieczorowski, *Inżynieria odwrotna i metody dyskretyzacji obiektów fizycznych*, I Krajowa Konferencja Naukowa „Szybkie prototypowanie. Modelowanie-Wytwarzanie-Pomiary", Rzeszów–Pstrągowa, 16–18 września 2015 r., „Mechanik" 2015, nr 12, s. 183.

[35] Należy wziąć pod uwagę także wysoki poziom wykorzystywanych metod konspirowania działań, posługiwanie się fałszywymi tożsamościami, stosowanie kodu, szyfracji lub szczególnego dialektu podczas porozumiewania się ze sobą osób należących do sieci.

tej, gdy przy odtwarzaniu określonego przedmiotu brakuje jakiegoś jego elementu i musi on zostać wykonany ręcznie ze względu na brak innych możliwości działania.Tym samym istnieje duże prawdopodobieństwo wykonania go w sposób niedoskonały. Pomocna staje się wówczas digitalizacja działania i jego automatyzacja, którą zapewnia RE.

Analogicznie jest w przypadku prowadzenia czynności wykrywczych. Przy ich realizacji może bowiem dojść do podjęcia działań rutynowych lub błędnych, a w ich konsekwencji – do przedwczesnego zamknięcia sprawy i wyjaśnienia jej w sposób niepełny. Dlatego też retrospekcyjne odwzorowanie zachowań indywidualnych lub organizacyjnych z zastosowaniem RE powinno dać asumpt do weryfikacji zrealizowanych działań, szczególnie gdy dotychczasowe czynności zakończyły się niepowodzeniem (np. nieobecność osoby w miejscu planowanego zatrzymania, niewłaściwe ustalenie zdeponowania środków w instytucji finansowej, nieprawidłowe wytypowanie miejsca i czasu dokonania przestępstwa). Do złego wytypowania może dojść, gdy istotna część procesu wykrywczego zostanie zrealizowana na podstawie modelu technicznego (analitycznego, programistycznego, predykcyjnego) w połączeniu z oceną zachowań i propozycją rozwiązań. Inżynieria odwrotna pozwala na obiektywne, oparte na informacjach o zaistniałych faktach połączonych z przestępcą, odtworzenie i ustalenie zachowania sprawcy przestępstwa w warunkach jemu przynależnych i z wytypowanym dla niego sposobem postępowania i analizy sytuacyjnej. Może być przydatna w różnych sytuacjach, także tych, w których zakłada się powtarzalność działania przestępcy (np. stosowanie przez niego takiej samej taktyki podczas napadu na kantory, okradania bankomatów czy mieszkań), wobec seryjnych morderców czy przy analizowaniu niewykrytych spraw (tzw. Archiwum X). Można ją ponadto zastosować w odniesieniu do zachowań przestępczych i taktyki zwalczania przestępczości. Warto się także zastanowić, czy można skorzystać z RE w przypadku procesów decyzyjnych i zdarzeń będących następstwem przyczynowo-skutkowym oraz reguł postępowania lub niezorganizowanego (spontanicznego) działania. Wydaje się, że jest ona dopuszczalna i stanowi „wsteczne" śledztwo, czyli daje możliwość rozebrania na elementy cząstkowe działań bardziej skomplikowanych, podlegających ocenie. Im w działaniach sprawcy przestępstwa jest mniej precyzji i obowiązujących reguł, a więcej przypadkowości, tym mniejsza możliwość zastosowania RE. Nie oznacza to jednak, że jeśli w wyniku analizy odwrotnej zostanie stwierdzony przypadek związany nie tyle z nieprzestrzeganiem reguł (których może nawet nie być), ile z przypadkowością, to przedmiotowe zdarzenie nie może być odpowiednio ocenione. Trzeba sprawdzić, czy reguła postępowania pozwalała na dowolność, czy też ten obszar stanowił nieuregulowaną lukę, której konsekwencji nie przewidziano, np. luki nie wykrył projektant (programista), a zrobiła to osoba postronna, którą był sprawca nieprawidłowości[36].

Inżynierię odwrotną stosuje się wobec tych zdarzeń, które można w jakiś sposób opisać cyfrowo. Dlatego też dane analogowe należy zamienić w postać cyfrową,

[36] Za nieprawidłowość nie należy przyjmować naruszenia, gdyż nie było co naruszać, a osiągnięcie nieprawidłowego stanu przez wykorzystanie luki.

co umożliwia umieszczenie ich w pamięci komputera. Nie można jednak twierdzić, że jedynie te dane, które będzie można skwantyfikować, mogą zostać wykorzystane w inżynierii odwrotnej. Z pewnością takie dane przysłużą się sprawnemu przeprowadzeniu postępowania. Takie procesy, jak zachowania przestępcze lub taktyka sprawców przestępstw, niekoniecznie rządzą się regułami matematycznymi i są bardziej skomplikowane, niż przewidywano. Zarówno te czynniki, jak i powtórna analiza zdarzenia rozłożonego na poszczególne elementy powinny być przyczynkiem do zbudowania nowego modelu przeciwdziałania, bardziej odpornego na aktywność przestępców i zwiększającego obiektywizm analityka kryminalnego.

Metody RE można wykorzystać do:

- oceny funkcjonalności, skuteczności oraz sposobów posługiwania się urządzeniami fizycznymi (programami) wykorzystywanymi w celach przestępczych (środki łączności, gry komputerowe, konsole, urządzenia zdalne itp.);
- prowadzenia gry operacyjnej przy wykorzystaniu urządzeń będących w dyspozycji przestępców (np. w Darknecie);
- pozyskania wiedzy z autorskich programów lub z modyfikacji programów dedykowanych wyłącznie działaniom grupy przestępczej (demontaż binarny);
- przeprowadzenia analizy niekompletnego materiału dowodowego, zwłaszcza dotyczącego wykorzystania złożonych narzędzi przestępstwa (np. oprogramowania);
- wykorzystania rynkowych instrumentów dysponowania aktywami, którymi posługują się przestępcy zgodnie z przyjętym celem kryminalnym;
- badania, kontrolowania i nadzorowania naruszeń w zakresie procedur księgowych (bilansowych) dotyczących pozyskiwania aktywów, prania pieniędzy oraz finansowania terroryzmu, zwłaszcza procedur realizowanych przy wsparciu ze strony profesjonalnych programów księgowych;
- udoskonalania stosowanych badań kryminalistycznych (w tym przy użyciu metod statystycznych);
- badania naruszeń procedur *compliance* w celu wykorzystania podmiotów gospodarczych do działań przestępczych (chodzi o zgodność działalności z normami, zaleceniami lub stosownymi praktykami);
- budowania systemów monitoringu społeczności internetowych;
- zwiększenia skuteczności analiz kryminalnych dotyczących funkcjonowania sieciowych organizacji przestępczych i terrorystycznych;
- ponownego przeanalizowania elementów w ramach prowadzenia przez organy ścigania różnych baz danych na potrzeby skuteczniejszego kojarzenia faktów pomocnych w typowaniu sprawców przestępstw;
- udoskonalenia prowadzenia taktyki śledczej, w tym w obszarze cyberprzestrzeni;
- odzyskania utraconych dowodów w sprawie lub zlokalizowania ich w miejscach dotychczas nietypowanych;
- walidacji oceny wytypowania rzeczywistego przywództwa i ważnych (pośrednich) węzłów w sieci przestępczej;
- weryfikacji wartości diagnostycznej.

Etapy procesu inżynierii odwrotnej wykorzystanej w analizie sieci przestępczych

Pierwszym etapem RE jest pozyskanie danych i analiza informacji, w tym uzyskanie modelu produktu (którym w tym przypadku jest obiekt – Podmiot A) do dalszej analizy, zawierającego również identyfikację krytycznych elementów tego produktu (dyskretyzacja[37]). W wyniku digitalizacji dane o charakterze analogowym zostają przekształcone w dane cyfrowe, które będzie można dalej przetwarzać przy wykorzystaniu programów komputerowych. Kolejne etapy RE to: opracowanie i weryfikacja oraz odzyskanie projektu utrzymanego i pochodzącego z fazy wdrażania i fazy projektowania. Proces wymaga zdefiniowania nowych oraz zmodyfikowania już istniejących wymagań dla produktu docelowego (przeprojektowanie).

Pierwszy etap jest decydujący dla przebiegu pozostałych faz, w których analitycy skupiają się na przetworzeniu pozyskanych danych, odpowiednio do wyznaczonego celu. Uzyskanie danych, gdy opracowuje się przedmiot fizyczny, nie powinno być trudne. Inaczej jest w przypadku zdarzeń, które nie są podporządkowane regułom technicznym (w takiej sytuacji należałoby mieć na uwadze potrzebę zastosowania indywidualnej metody postępowania, adekwatnej do zaistniałego problemu). W ramach procesu RE jest możliwe wystąpienie tzw. nacjonalizacji, czyli przejęcia cudzego produktu w celu uzyskania produktu krajowego (na własne potrzeby) z jednoczesnym pominięciem procedur patentowych i zastrzeżeń co do ochrony własności intelektualnej twórców urządzenia[38]. Z tego względu część działań może być podejmowana niezgodnie z prawem. W niektórych przypadkach osoby realizujące zadania inżynierii odwrotnej powinny być chronione kontratypami[39]. Może między innymi zaistnieć sytuacja, że analizowane urządzenie zostało stworzone przez wytwórcę działającego niezgodnie z przepisami prawa. Ponadto nowy produkt, mimo szerokiego odwzorowania (bez uzyskania autoryzacji), będzie miał po przetworzeniu wysoki poziom autonomizacji.

---

[37] Dyskretyzacja – pojęcie dotyczące procesu transformowania modeli i równań funkcji ciągłych na ich dyskretne odpowiedniki. Jest to zwykle pierwszy krok w procesie przygotowywania tych modeli (i równań) do ewaluacji numerycznej i implementacji na komputerach cyfrowych, za: Wikipedia, https://pl.wikipedia.org/wiki/Dyskretyzacja_(matematyka) [dostęp: 5 II 2021] – przyp. red.

[38] Nie będzie to wchodziło w grę, gdy „twórcą" projektu, urządzenia, programu będzie osoba współpracująca z organizacją przestępczą, członek tej organizacji, mający pełną świadomość przydatności opracowanych rozwiązań technicznych w realizacji celu przestępczego.

[39] W ustawodawstwie amerykańskim: zgodnie z sekcją 103 (f) ustawy *Digital Millennium Copyright Act* [17 USC § 1201 (f)] osoba będąca w posiadaniu programu może przeprowadzić proces inżynierii wstecznej i obejść jego ochronę, jeśli jest to konieczne do osiągnięcia „interoperacyjności". Istnieje ograniczone wyłączenie, które pozwala na dzielenie się zdobytą w ten sposób wiedzą i wykorzystywanie jej do celów interoperacyjności. Zob. hasło: inżynieria odwrotna, https://pl.qaz.wiki/wiki/Reverse_engineering#Source_code [dostęp: 15 II 2021]. W Unii Europejskiej obowiązuje: *Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych* (Dz. Urz. UE L 111 z 5 V 2009 r.), s. 16, https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A32009L0024 [dostęp: 15 II 2021].

We wszystkich tych przypadkach czynności podejmowane w ramach RE powinny być uznane za prawnie dopuszczalne.

Wykorzystanie RE wobec form organizacyjnych przestępczości można rozważyć pod kątem rozpoznania szczegółów kodu działania przestępców. Oznacza to możliwość ustalenia poszczególnych elementów, etapów i sposobów zarządzania w organizacji, które się przekładają na przygotowanie i dokonywanie konkretnych przestępstw oraz na zbudowanie zaplecza logistyczno-finansowego dla struktur organizacyjnych. Jest to część wiedzy, której organy ścigania nie będą mogły zdobyć w wyniku takich działań operacyjnych, jak: współpraca z osobowymi źródłami informacji, stosowanie techniki operacyjnej czy pozyskanie wiedzy z operacji specjalnej. Dzięki temu będzie można rozpoznać kod występujący zarówno na poziomie operacyjnym (wykonawczym), jak i na poziomie zarządzania strategicznego. Kod działania przestępców to głównie wiedza, którą dysponuje niewielka liczba osób, przede wszystkim ścisłe kierownictwo organizacji przestępczej.

Zastosowanie procesu inżynierii odwrotnej ma na celu: rozpracowanie oprogramowania, poradzenie sobie ze złożonością zadania, wygenerowanie alternatywnych rozwiązań, odzyskanie utraconych informacji, wykrycie skutków ubocznych działania oraz synteza na wyższym poziomie abstrakcji. Są to ogólne cele, które można uzupełnić tymi, które bezpośrednio wiążą się z przeciwdziałaniem przestępczości. Zalicza się do nich:

- poznanie oprogramowania opracowanego i stosowanego przez przestępców;
- poznanie sposobów wykorzystania powszechnie dostępnego oprogramowania do popełniania przestępstwa;
- zdobycie wiedzy o wewnętrznym oprogramowaniu używanym w instytucji wykorzystanej do dokonania przestępstwa;
- zdobycie wiedzy na temat szczegółów konstrukcyjnych urządzeń służących do dokonania przestępstwa;
- zdobycie wiedzy na temat konfiguracji wielu instrumentów finansowych, biznesowych i prawnych przygotowanych przez przestępców do wygenerowania zysku przestępczego, zalegalizowania środków finansowych czy zapewnienia wsparcia finansowego organizacjom terrorystycznym;
- uzyskanie produktu umożliwiającego śledzenie (monitorowanie) przedsięwzięć przestępczych bez wiedzy zainteresowanych;
- przeprowadzenie testu oprogramowania (algorytmu) przyjętego jako „bramka" lub „czerwona flaga" dla instytucji w celu zabezpieczenia jej klientów przed przestępstwem, szczególnie gdy takiego zabezpieczenia nie było;
- uniemożliwienie wykorzystania produktu do popełnienia przestępstwa.

Do czynników, które mogą oddziaływać na replikację (odwzorowanie) produktu, można zaliczyć m.in.:

- posiadanie oryginalnego obiektu stanowiącego przedmiot badań inżynieryjnych – ważne jest poznanie konstrukcji, mechanizmu działania oraz rodzaju materiału, z jakiego został on wykonany. Jest to istotne przede wszystkim

ze względu na potrzebę jak najdokładniejszego odwzorowania danych, których przedmiotowy produkt jest nośnikiem;
- tolerancja – zaakceptowanie odchyleń w dokonanych pomiarach;
- dokładność – potrzeba zapewnienia jak najbardziej precyzyjnego dokonania pomiarów, tak aby spełnić założony cel nowego produktu (dotyczy to zarówno całościowego odzwierciedlenia istniejącego przedmiotu, jak i uzyskania zmodyfikowanej konstrukcji);
- podejście pomiarowe – potrzeba dobrania odpowiedniego urządzenia pomiarowego, aby właściwie zidentyfikować dane produktu;
- cel – czyli główne założenie zastosowania RE, a także sprawdzenie, do czego ostatecznie posłuży zastosowanie inżynierii odwrotnej (np. uzyskanie odpowiedzi na pytania, jak ten produkt działa i co poszło nie tak lub co mogło pójść źle w jego działaniu)[40].

Podczas stosowania procesu RE trzeba zwrócić uwagę na następujące zasady, a także pojawiające się problemy:
- nie należy mylić hipotez z wnioskami. Inżynieria odwrotna pozwala na otrzymanie hipotezy, dlatego też trzeba dokładnie zrozumieć aplikację, zanim będzie można wyciągnąć jednoznaczne wnioski;
- należy się spodziewać wielu interpretacji, ponieważ nie ma tu jednej odpowiedzi, jak w inżynierii postępowej (tradycyjnej). Alternatywne interpretacje struktury i informacji zaczerpniętych z baz danych mogą przełożyć się na otrzymanie różnych modeli;
- nie należy zniechęcać się wynikami przybliżonymi. Trzeba dążyć do wydobycia z baz danych jak największej liczby informacji (co najmniej 80 proc.). Można użyć typowych technik inżynierii postępowej (takich jak przeprowadzanie wywiadów z użytkownikami mającymi wiedzę na ten temat), aby uzyskać pozostałe 20 proc. Wiele osób uważa ten brak doskonałości za niewygodny, ponieważ jest to zmiana paradygmatu w stosunku do inżynierii postępowej;
- należy spodziewać się uzyskania nietypowych konstrukcji. Projektanci baz danych, a także eksperci, używają czasami nietypowych konstrukcji. W niektórych przypadkach nie ma możliwości stworzenia kompletnego, dokładnego modelu bazy danych, ponieważ taki model nigdy nie istniał;
- należy utrzymać spójny styl. Bazy danych są zwykle projektowane przy użyciu spójnej strategii, w tym spójnej realizacji dobrych praktyk projektowych. Dzięki temu powinno się wywnioskować podstawową strategię[41].

[40] Zob. M. Knicker, *What Are The Types of Reverse Engineering and Why Does it Matter?*, Q-Puls Labs, Dimensional Measurement Blog, 8 XI 2012 r., https://www.qpluslabs.com/blog/what-are-the-types-of-reverse-engineering-and-why-does-it-matter/ [dostęp: 15 IV 2020].

[41] M.R. Blaha, *Reverse Engineering for Product Assessment*, informIT, 13 X 2001 r., https://www.informit.com/articles/article.aspx?p=23692&seqNum=6 [dostęp: 18 XII 2020]. Zob. także: tenże, *A Manager's Guide to Database Technology. Building and Purchasing Better Applications*, wyd. 1, [bmw] 2000.

Inżynieria odwrotna może znaleźć zastosowanie w odniesieniu zarówno do dziedziny programowania, jak i do opracowanych procedur postępowania w zakresie monitoringu i przeciwdziałania przestępczości, z uwzględnieniem m.in. transakcji finansowych, procedur rozpracowania grup przestępczych, taktyki działania organów ścigania i badań kryminalistycznych. Jako przykład można podać zagadnienia związane z procesem decyzyjnym przywódców organizacji, księgowością śledczą, wewnętrznymi procedurami instytucji obowiązanych dotyczącymi przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu, procedurami *compliance* i przeciwdziałaniem oszustwom oraz nieprawidłowościom na szkodę instytucji finansowych. Podczas stosowania metody RE niezbędne jest rozdzielnie zdarzeń (transakcji) na podstawowe części oraz wywnioskowanie na podstawie przyjętego modelu postępowania, jakie elementy nie zadziałały, zadziałały nieskutecznie lub zadziałały w celu innym niż założony w projekcie (czyli np. posłużyły dokonaniu przestępstwa). Jest to zarazem proces zmierzający do uzyskania „kodu decyzyjnego".

Stworzony model jest stosowany przede wszystkim w instytucjach komercyjnych w celu wypracowywania zysków (podobnie jak w organizacji przestępczej). Przy realizacji wyznaczonego zadania mogą być wykorzystywane także inne modele, które stanowią wsparcie lub spełniają funkcję kontrolną czy rozliczeniową (mogą one być wprowadzane niezależnie od przyjętego modelu). Dla przykładu, model sposobu sprzedaży produktu będzie wsparty modelem rozliczeniowym, pomocnym – zgodnie z zasadami księgowania i przyjętego planu kont – przy rozliczeniu produktu między kontrahentami. Dzięki temu będzie możliwe wygenerowanie informacji, jak dany produkt jest przyjmowany przez klientów lub wykorzystywany w sposób niezaplanowany w strategii sprzedaży. W przypadku modelu przestępczego cel dotyczący dysponowania środkami będzie inaczej konstruowany i będzie uzależniony od głównego celu organizacyjnego. Stąd też istnieje możliwość zidentyfikowania innego zarządzania aktywami niż to, które jest charakterystyczne dla modelu inwestycyjnego „prawego klienta". Aby prawidłowo i efektywnie wykorzystać inżynierię odwrotną, już na wstępie projektowania określonych rozwiązań w instytucjach, które będą chciały zaakceptować te rozwiązania i wdrożyć je do swojej strategii sprzedażowej, niezbędne będzie przyjęcie ścisłej i precyzyjnej reguły (schematu) postępowania z danym produktem. Będzie to np. umieszczenie w nim „czerwonych flag", które będą świadczyć o jego wykorzystywaniu niezgodnym ze strategią produktu lub z prawem. Produkt powinien zostać zaopatrzony w szczegółową instrukcję postępowania z nim, co pozwoli – w ramach działań wstecznych – na uzyskanie modelu porównawczego wobec rozpatrywanego, ocenianego przypadku.

Przy korzystaniu z RE należałoby rozpatrzyć przynajmniej dwa tryby postępowania. Pierwszy odnosiłby się do oceny reguł postępowania z produktem i klientem występujących w danej instytucji. Drugi zaś do skonfrontowania konkretnej sytuacji z trybem „ostrzegawczym", uplasowanym w obszarze bezpieczeństwa instytucji (uzyskanym np. na podstawie przeprowadzonej analizy ryzyka). Im reguły postępowania są bardziej szczegółowe i doprecyzowane, tym skuteczniej będzie można zwrotnie ocenić

produkt w odniesieniu do oddziałujących na niego czynników i torów zgodnościowych tego postępowania (w tym objętych elementami zasad *compliance*). Zastosowanie RE w dziedzinie finansów wiąże się z potrzebą oceny zakresu i sposobu wykorzystania instrumentów finansowych (najczęściej publicznie dostępnych) w kontekście nielegalnego pozyskania aktywów, legalizowania środków pochodzących z czynów zabronionych, dystrybucji i redystrybucji aktywów w ramach sieci przestępczej oraz monitorowania „zachowań finansowych" jako zwiastunów ataków terrorystycznych.

Przedstawiona propozycja zastosowania RE odnosi się do spraw związanych z zasileniem aktywami finansowymi organizacji przestępczej (terrorystycznej). Prowadzono również badania, które dotyczyły ścisłego procesu decyzyjnego w ramach samej organizacji[42]. Za pomocą metody analizy decyzji (ang. *applied decision analysis,* ADA) zbadano procesy decyzyjne przywódców takich organizacji, jak: Al-Kaida, Hamas i Hezbollah. Identyfikacja sposobów podejmowania przez nich decyzji pozwoliła na przyjęcie taktyki najbardziej adekwatnej do stawianego celu zadania (różnej fazy aktywności) i skutecznej w przeciwdziałaniu terroryzmowi. W badaniu wykorzystano wiele modeli decyzyjnych (np. eliminację według aspektów[43], leksykograficznego[44], poliheurystycznego[45] lub maksymalizacji użyteczności[46]).

Wykorzystanie procesu RE w badaniu taktyki przestępczej będzie polegać na prześledzeniu aktywności sprawcy, tj. tego, w jaki sposób rozwiązywał dane problemy (sytuacje) na określonym etapie postępowania przestępczego. Inżynieria odwrotna znajdzie zastosowanie przede wszystkim w przypadku wielowymiarowego i wieloinstrumentalnego postępowania sprawczego, a nie działań prostych, łatwo rozpoznawalnych. Chodzi o rozbudowane formy przestępczości, które same w sobie są czynem sprawczym o dużej złożoności, jak np. przestępstwa finansowo-gospodarcze, proceder prania pieniędzy czy państwowy sponsoring działań terrorystycznych.

---

[42] Zob. szerzej: J.T. Chatagnier, A. Mintz, Y. Samban, *The Decision Calculus of Terrorist Leaders*, „Perspectives on Terrorism" 2012, nr 4–5, s. 125 i nast., https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2012/issue-4/the-decision-calculus-of-terrorist-leaders-j.tyson-chatagnier-alex-mintz-and-yair-samban.pdf [dostęp: 20 XII 2020].

[43] Model związany ze sposobem podejmowania decyzji. Polega on na tym, że wybiera się jakąś cechę-aspekt (która jest akceptowana lub nie) i dokonuje się przeglądu dostępnych opcji, eliminując te, które nie spełniają tego wymagania. Zob. T. Tyszka, *Analiza decyzyjna i psychologia decyzji*, Warszawa 1986; J. Kozielecki, *Psychologiczna teoria decyzji*, Warszawa 1977.

[44] Reguła leksykograficzna – wybierany jest wariant, który pod względem najważniejszej cechy jest najlepszy. Jeśli między wariantami zachodzi równość, porównuje się następne pod względem hierarchii cechy. Zob. M. Wójcik, *Proces podejmowania decyzji w przedsiębiorstwie*, wyd. 1, 2009, s. 16, e-book.

[45] Zob. T. Pawluszko, *Poliheurystyczna teoria podejmowania decyzji w analizie bezpieczeństwa*, „Colloquium Pedagogika – Nauki o Polityce i Administracji" 2020, nr 1, https://colloquium.amw.gdynia.pl/index.php/colloquium/article/view/164/157 [dostęp: 15 II 2021].

[46] Zob. B. Polanowska-Sygulska, *Użyteczność a maksymalizacja bogactwa: Filozoficzne zakorzenienie poglądów Chicagowskiej szkoły law & economics*, „Archiwum Filozofii Prawa i Filozofii Społecznej" 2011, nr 1, s. 5–14; O. Kapliński, *Drzewa decyzyjne i użyteczność decyzji*, http://sipb.sggw.pl/Monografia_2015/Strony%20odRekomendowane_metody-11.pdf [dostęp: 15 II 2021].

Będzie można ją wykorzystać zwłaszcza w rozpracowywaniu zorganizowanych grup przestępczych oraz ugrupowań (organizacji) terrorystycznych. Dzięki RE będzie można uzyskać wieloźródłowy i wielodecyzyjny obraz zarządzania w celu wygenerowania informacji o przygotowaniu i dokonaniu przestępstwa. Ocenie mogą być poddane: treść decyzji, szybkość jej wydania i realizacji, personalny dobór wykonawców jej treści, personalny dobór adresatów (gradacja dostępu do skali informacji). Inną kategorią spraw badanych w ramach RE będą te przestępstwa, przy których popełnianiu wykorzystuje się elektroniczne platformy atakowanych podmiotów, np. przestępstwa giełdowe, przestępstwa w bankowości elektronicznej lub dotyczące kryptowalut. Zadaniem do zrealizowania będzie rozbicie na czynniki pierwsze procesu decyzyjnego opartego na doborze sprawców oraz osób kontrolujących przebieg przestępstwa, umiejscowieniu działania w zakresie geograficznym i wirtualnym, a także podjęcie – na określonym etapie – decyzji o skorzystaniu ze współpracy z innym podmiotem przestępczym bądź wykorzystaniu firmy zarejestrowanej w strefie *offshore* (tzw. rajach podatkowych – dop. red.) itp.

W modelu odtworzeniowym należy założyć racjonalność (a nie chaos) w postępowaniu sprawcy. Zadaniem inżyniera-kryminalistyka, chcącego skorzystać z metody RE, jest zdobycie wiedzy o takim przebiegu zdarzeń, które spowodowało zmianę planowanej taktyki przestępczej i podjęcie decyzji np. o nierealizowaniu w ustalonym czasie określonych przedsięwzięć lub o posłużeniu się innymi instrumentami w realizacji przestępstwa[47]. Łatwo będzie tym samym wykryć słabe punkty w procesie decyzyjnym sprawcy oraz prześledzić planowanie alternatywnych rozwiązań, które zapewniają większą skuteczność i bezpieczeństwo (tajność) działania przestępczego. Zastosowanie RE umożliwi odtworzenie kolejności zdarzeń – od ich docelowego efektu (popełnienia przestępstwa) do początku, tj. jego zaaranżowania. Badanie można będzie wykonać niezależnie od prowadzonych czynności dochodzeniowo-śledczych i na potrzeby czynności procesowych.

Dla wspomnianej metody ADA macierz decyzyjna[48] składa się z zestawu alternatyw, wymiarów (lub kryteriów) wyboru spośród tych alternatyw oraz oceny implikacji każdego wymiaru dla każdej alternatywy. Wagi (lub poziomy ważności) mogą

[47] Zmiana może zajść na skutek informacji uzyskanej od organów ścigania, w tym od uznanych źródeł informacji, bądź na skutek działań neutralizacyjnych podjętych przez służby niezależnie w innej sprawie czy też pod wpływem warunków niezależnych, np. odwołania lotu samolotem, wprowadzenia blokady granicy, klęski żywiołowej

[48] Macierz decyzyjna (ang. *decision matrix analysis*, DMA) to lista wartości w wierszach i kolumnach, która umożliwia analitykowi systematyczne identyfikowanie, analizowanie i ocenianie wydajności relacji między zestawami wartości i informacji. Analiza matryc decyzyjnych jest najprostszą formą analizy decyzji wielu kryteriów (ang. *multiple-criteria decision analysis*, MCDA), znanej również jako pomoc decyzyjna o wielu kryteriach lub zarządzanie decyzjami o wielu kryteriach (ang. *multiple-criteria decision making*, MCDM). Zaawansowana MCDA może obejmować wysoce złożone modelowanie różnych potencjalnych scenariuszy przy użyciu zaawansowanej matematyki, https://steemit.com/polish/@techiwebicodi/pl-podejmowanie-decyzji-przez-wazenie-roznych-czynnikow-decision-matrix-analysis-i-przyklad-wykorzystania [dostęp: 15 II 2021].

być przypisane do każdego wymiaru. Zestaw alternatyw obejmuje prawdopodobne kierunki działań decydenta (np. lidera organizacji terrorystycznej), z uwzględnieniem rozwiązań w razie wystąpienia ewentualnych problemów decyzyjnych[49]. Dzięki analizie inżynieryjnej będzie można ocenić stopnień zaawansowania organizacyjnego grupy przestępczej (rodzaj zorganizowania struktury) oraz jej uplasowanie w ramach zewnętrznych relacji z typowanymi obiektami spoza organizacji. Ostatecznym celem RE będzie pozyskanie umiejętności w zakresie szybszego i skuteczniejszego neutralizowania organizacyjnych form przestępczości, a także zastosowanie „głębokiej" analizy samej organizacji w kontekście przywództwa, relacji między członkami czy procesu decyzyjnego.

Przed zastosowaniem RE pomocne będzie rozpatrzenie analizowanej sprawy w kategoriach porządkujących. Na czynniki porządkujące prowadzone działania operacyjnie bądź równolegle do nich prowadzone postępowanie procesowe będą miały wpływ:

- prowadzenie czynności operacyjno-rozpoznawczych zgodnie z przyjętymi regulaminami i wewnętrznymi instrukcjami uprawnionych służb;
- wprowadzenie systemu pozyskiwania i kategoryzacji informacji (wartości informacji), które będą inicjacyjne wobec dalszych czynności służbowych[50];
- wprowadzenie od samego początku sprawy w reżim (w schemat) analizy kryminalnej prowadzonej zgodnie z określonymi (znanymi) silnikami analitycznymi;
- zastosowanie, również wobec informacji pozyskanych spoza służb, reguł i schematów przynależnych strukturze schematów analitycznych, przetwarzaniu i analizie, przy czym należałoby założyć potrzebę kompatybilności własnych systemów bazodanowych i analitycznych służb z bazami danych podmiotów zewnętrznych (również z wbudowanym elementem predykcyjnym);
- pozyskanie informacji o funkcjonalności działania całościowych i lokalnych matryc przeznaczonych dla społeczności internetowych;
- rozważanie wprowadzenia zindywidualizowanego programu analitycznego ze znanym silnikiem analitycznym na potrzeby danej sprawy;

---

[49] J.T. Chatagnier, A. Mintz, Y. Samban, *The Decision Calculus of Terrorist Leaders*…, s. 128.

[50] Zob. dla przykładu: *Decyzja nr 338 Komendanta Głównego Policji z dnia 12 października 2016 r. w sprawie Systemu Informacji Operacyjnych*, Dz. Urz. KGP z 2016 r. poz. 65, https://isp.policja.pl/isp/aktualnosci/prawo/9626,Decyzja-nr-338-Komendanta-Glownego-Policji-z-dnia-12-pazdziernika-2016-r.html [dostęp: 16 IV 2020]. Meldunek informacyjny sporządza się w każdym przypadku uzyskania przez policjantów informacji przydatnych do „(…) zapobiegania, rozpoznawania, ujawniania i wykrywania przestępstw, ustalania metod ich popełniania oraz wykrywania i zatrzymywania sprawców, w tym także: 1) informacji o zdarzeniach, miejscach, pojazdach, dokumentach oraz osobach fizycznych i innych podmiotach nie będących osobami fizycznymi; 2) informacji o telekomunikacyjnych urządzeniach końcowych wykorzystywanych do przekazu informacji, z wyłączeniem danych pozyskanych w trybie określonym w art. 20c ustawy o Policji; 3) informacji o rachunkach w bankach lub innych instytucjach finansowych oraz o czynnościach bankowych, z ograniczeń dostępu do tych danych wynikających w art. 20 ust. 3 i 4 ustawy o Policji".

– klasyfikacja przez ustawodawcę w przepisach karnych schematu zachowania sprawcy, które jest penalizowane jako przestępstwo;
– realizowanie zadań pozaschematycznych w przyjętym modelu systemowym, który z założenia funkcjonalnego powinien współistnieć z ogólnymi systemami i mieć na celu porządkowanie oraz kategoryzację danych (szczególnie odnosi się to do – w miarę możliwości – całościowego i spójnego wprowadzenia modelu matematycznego sieci zbudowanej z rozpoznawanych elementów, co jest niezbędne do rekonstrukcji interakcji między elementami).

Atutem ułatwiającym rozwiązywanie zagadnień w ramach analizy prowadzonej na podstawie metod RE jest bazowanie na sieciowym schemacie (m.in. graficznym) przyjętym dla danej organizacji przestępczej lub terrorystycznej, ale też dla każdego skomplikowanego taktycznego działania przestępczego[51]. Taki schemat może być kreowany zarówno w ramach analizy kryminalnej, jak i innych rozwiązań wynikających z teorii grafów czy SNA. Ważne jest, aby przez cały czas prowadzenia sprawy utrzymywać wyznaczone schematy postępowania, nazewnictwo, metodykę pracy operacyjnej bądź śledczej, zarówno na potrzeby opisania węzłów sieci (atrybutyzacji), jak i identyfikacji relacji zachodzących między węzłami. W ten sposób sieci organizacyjne można klasyfikować na podstawie rodzaju zaangażowanych podmiotów i interakcji zachodzących między nimi. Korzystanie z takiego schematu umożliwi wnioskowanie o każdym jego elemencie, a ich ocena będzie wynikiem relacji istniejących między danym elementem a innymi elementami zakwalifikowanymi do sieci bądź elementami z bliskiego otoczenia sieci, np. występowanie stanu recesji (w działaniach sieci) lub zaktywizowanie kryminalne, zmiana przywództwa czy pobudzenie aktywności pod wypływem czynników spoza organizacji. Ponadto taki schemat pozwoli na umiejętne nazwanie atrybutów sieci i przypisanie ich do jej węzłów. Dzięki temu ocena sieci oraz schemat (katalog) zachowań przestępczych zostaną wzbogacone o wnioskowanie przeprowadzone w przeszłości, ale uzupełnione o informacje nieznane w tamtym momencie.

Ta swoista retrospekcja oprócz uzupełnienia modelu przestępstwa (organizacji) pozwala na przeanalizowanie reakcji członków grupy przestępczej oraz podział zdarzeń na planowane bądź przypadkowe. Umożliwia to rozpoznanie taktyki przestępstwa przyjętej przez sprawców oraz stosowanych przez nich metod kamuflażu. Jednocześnie można ocenić, czy reakcja organów ścigania na przestępstwo była adekwatna do zagrożenia (przeprowadzona we właściwym czasie, miejscu i w stosunku do odpowiednich osób – przy założeniu całościowej lub częściowej neutralizacji organizacji przestępczej

[51] Patrz przykładowo: program iBase zintegrowany z Analyst's Notebook. iBase zapewnia prosty mechanizm importu umożliwiający pobieranie danych z wielu źródeł, takich jak: pliki tekstowe, źródła danych zgodne z OLE lub pliki XML (schemat MS Rowset), i konwertuje je na encje (bazy danych – dop. red.) oraz łącza, zapewniając jednolity standard informacji. Crime Workbench (CWB) pozwala na tworzenie, zarządzanie i wykorzystywanie tekstowych baz danych, które mają zastosowanie w procesie analizy kryminalnej. Przydatny w sprawach wielowątkowych obejmujących duży obszar terytorialny ze złożoną strukturą organizacji przestępczych oraz dużą ilością informacji, http://www.acsys.com.pl/index_en.php?action=iBase [dostęp: 15 IV 2020].

bądź zapobieżeniu zamachowi terrorystycznemu). W podejściu sieciowym niektóre atrybuty elementów (węzłów) są możliwe do zmierzenia (zmienne losowe) i można je przeanalizować za pomocą narzędzi statystycznych. Pomocne tu będą zarówno teoria informacji, jak i sklasyfikowanie i skwantyfikowanie relacji, niezbędne przy rozpoznaniu całej działalności sprawców (węzłów sieci). Ten drugi aspekt będzie się wiązał z rodzajem popełnianych przestępstw, taktyką popełniania przestępstw przyjętą przez sprawców (w tym *modus operandi*), podejmowanymi decyzjami, np. co do narzędzi wykonawczych, schematów zabezpieczeń logistycznych działań przestępczych oraz ciągłości organizacyjnej.

W badaniach metodami stosowanymi w ramach procesu RE inne założenia należy przyjąć dla przestępczości kryminalnej, a inne dla przestępczości finansowej (ale też dla działań hybrydowych dotyczących obydwu tych sfer). Wiąże się to przede wszystkim z tym, że dotyczy to innego przedmiotu przestępstwa i odmiennej konstrukcji prawnej penalizującej zaistniałe zdarzenia. Ocena, w której analitycy posługują się wyłącznie danymi, jakimi dysponowały organy ścigania przez dokonaniem neutralizacji grupy przestępczej, jak i tymi danymi, które w wyniku zastosowania inżynierii odwrotnej wzbogacają wiedzę o sposobie przestępczego funkcjonowania, umożliwia poznanie aktywności przestępczej. Oznacza to, że ten retrospektywny model postępowania może poszerzyć i „ulepszyć" wiedzę o rozpatrywanym układzie. W konsekwencji obraz działań przestępczych będzie uzupełniony i zwiększy zakres kontrdziałań służb, w tym wykorzystania komputerów kognitywnych (tj. poznawczych, ang. *cognitive computing*, CC).

Przy pozyskiwaniu sygnałów aktywności sprawców będzie również pomocne posługiwanie się przez nich urządzeniami mobilnymi. W kryminalistyce zbieranie i analiza danych pochodzących z telefonów komórkowych obejmuje m.in. pobieranie informacji z tych telefonów, a następnie ich zidentyfikowanie i przeanalizowanie, czy uzyskane dowody są istotne dla trwającego dochodzenia. Dzięki monitorowaniu i odzyskiwaniu danych z urządzeń mobilnych jest możliwe mapowanie zachowań (co do czasu) i ich geolokalizacja. Dokonuje się tego przez odczyty aplikacji zainstalowanych przez sprawcę w telefonach komórkowych, GPS czy korzystanie z informacji zawartych w sieci Internet (korzystanie z e-zakupów, e-płatności, e-usług publicznych czy gier). Mimo preferowania całościowego podejścia do organizacji przestępczej przy przeprowadzaniu diagnozy jej funkcjonowania oraz czynności podejmowanych wobec niej przez organy ścigania, w ramach inżynierii odwrotnej można realizować zadanie przez posiłkowanie się podejściem cząstkowym do poszczególnych obszarów związanych z ocenianą (duplikowaną) organizacją[52].

Podejście całościowe wiąże się z działaniem systemowym i potraktowaniem przedmiotu badawczego jako całości. Natomiast cząstkowe obszary badawcze mogą się

[52] W takim przypadku odtworzona sieć komunikacyjna będzie świadczyła o atrybutach węzłów w sieci. Będzie to jeden z elementów branych pod uwagę przy typowaniu krawędzi sieci i istotnych, z punku widzenia wykrycia przywództwa i sprawców przestępstw, relacji zachodzących między poszczególnymi członkami organizacji uznanymi za węzły sieci.

odnosić do: wewnętrznego zarządzania organizacją, ustanawiania relacji z podmiotami zewnętrznymi (np. innymi organizacjami) czy zarządzania finansami i zapleczem logistycznym organizacji[53]. Dla inżynierii odwrotnej podejście całościowe należy uznać za cel ostateczny. Dzięki badaniom cząstkowym można połączyć impulsy (symptomy) skutkujące konkretnymi sytuacjami (faktami) wiążącymi się z poszczególnymi członkami organizacji, a co za tym idzie – zbadać wpływ tych sytuacji na całą organizację.

W ramach inżynierii odwrotnej można skorzystać również z informacji o danej sprawie uzyskanych ze źródeł cyfrowych. Są nimi m.in. sygnały (informacje) zdobyte dzięki „wyzewnętrznieniu się" członków organizacji terrorystycznych. Dotyczy to takich obszarów, jak: propaganda, wojna psychologiczna, rekrutacja, zbieranie funduszy, eksploracja danych, zbieranie informacji o atakach komputerowych, dystrybucja oprogramowania, kupowanie fałszywych dokumentów (tożsamości), działalność szkoleniowa. Oznacza to, że w przypadku prowadzenia sprawy o wyższym stopniu skomplikowania, ale bez zastosowania analizy kryminalnej, będzie możliwe przedstawienie schematu działania grupy przestępczej w formie wizualizacji wirtualnej, co zapewnia jego większą przejrzystość, dostępność, zwiększa obszar analizy i wnioskowania o dalszych działaniach operacyjnych lub procesowych. Proces RE ma na celu nie tylko weryfikację istniejącego obiektu[54], lecz także stworzenie takiego jego duplikatu, który będzie stanowić poszerzoną wersję modelu wyjściowego lub też jego udoskonalenie. Nowa wersja stanie się zaś obiektem wyjściowym dla podjęcia czynności wykonawczych skutkujących neutralizacją obiektu wyjściowego lub modelem służącym w przyszłości do nauki (wsparcie procesu decyzyjnego).

Podstawowe działanie RE wobec organizacyjnej formy przestępczej przeprowadzone z wykorzystaniem programów komputerowych przebiega w następujących etapach:

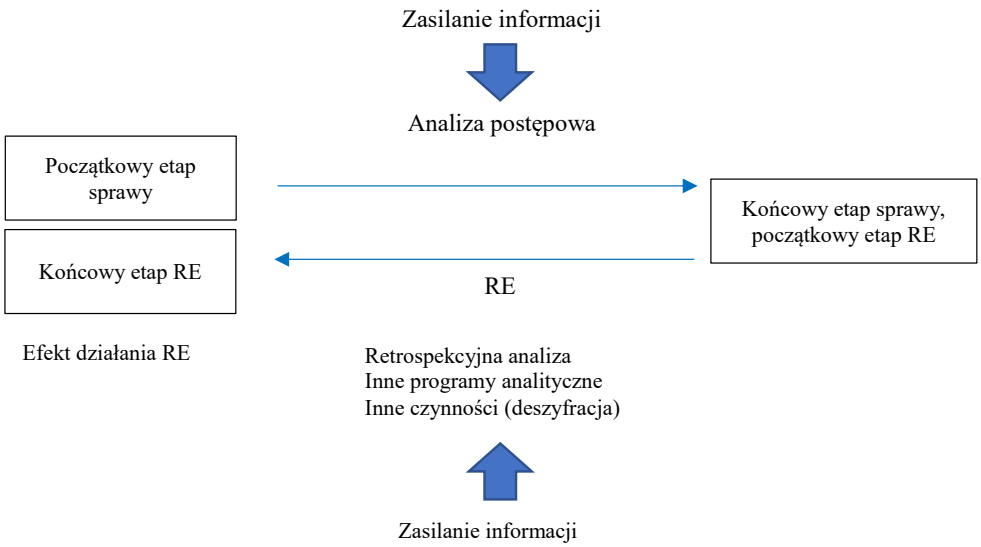
- za materiał wyjściowy należałoby uznać efekt analityczny (konstrukcja sieciowa rozpoznawanego obiektu) uzyskany w wyniku zastosowania określonego oprogramowania analitycznego oraz dostępne dane zgromadzone w celu poznania konstrukcji sieciowej rozpracowywanego obiektu;
- zebranie jak największej liczby informacji (śladów sieciowych) o aktywności analizowanej organizacyjnej formy przestępczej na temat zdarzeń (koncentracji w sprawie), które będzie można poddać pomiarom (społeczności sieci wprowadziły wiele różnych systemów pomiarowych do zbierania i prezentowania informacji o właściwościach sieci, np. protokoły, techniki, narzędzia, nakładki, ramy, archiwa);

[53] Zob. P. Klimas, *Podejście sieciowe w logistyce*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 249, s. 36 i nast.; W. Czakon, *Sieci w zarządzaniu strategicznym*, Warszawa 2012.

[54] Wprowadzone pojęcie o b i e k t odnoszące się do podmiotu zawiera w sobie zarówno analizę osób fizycznych, prawnych, relacji, jak i procesów decyzyjnych, stylu myślenia, psychologii. Jest to zabieg upraszczający, świadomie zastosowany na potrzeby dalszych rozważań.

- poszukanie luk, np. przyczynowo-skutkowych, komunikacyjnych czy logistycznych, w dotychczas podjętych czynnościach, m.in. w:
  - wykonaniu retrospekcyjnej analizy danych w sprawie przez przeprowadzenie działań inżynierii odwrotnej wobec uzyskanego efektu analitycznego, będącego konsekwencją wykorzystania programu analizy dostępnego organom ścigania,
  - prowadzeniu analizy danych w sprawie na podstawie dostępnych komercyjnych programów analitycznych przez przeprowadzenie działań inżynierii odwrotnej w stosunku do uzyskanego efektu analitycznego;
  - ustaleniu, czy zdefiniowana konstrukcja sieciowa uwzględnia także dane pochodzące z ukrytych obszarów komunikacyjnych (zaszyfrowanych wiadomości, informacji z sieci Tor czy Darknet), co może ostatecznie mieć wpływ na uzyskanie niepełnego efektu analitycznego;
- ustalenie zaszyfrowanych danych i dokonanie ponownej analizy konstrukcji sieci;
- weryfikacja i walidacja posiadanych danych (np. czy nie doszło do błędu w wyniku przetwarzania danych) przez organy ścigania w konkretnej sprawie oraz pozyskanie dodatkowych informacji (uzupełnienie działań odwrotnych).

W rezultacie tych czynności powinien powstać nowy obraz analizowanej struktury sieci, co zostało przedstawione na schemacie 1.



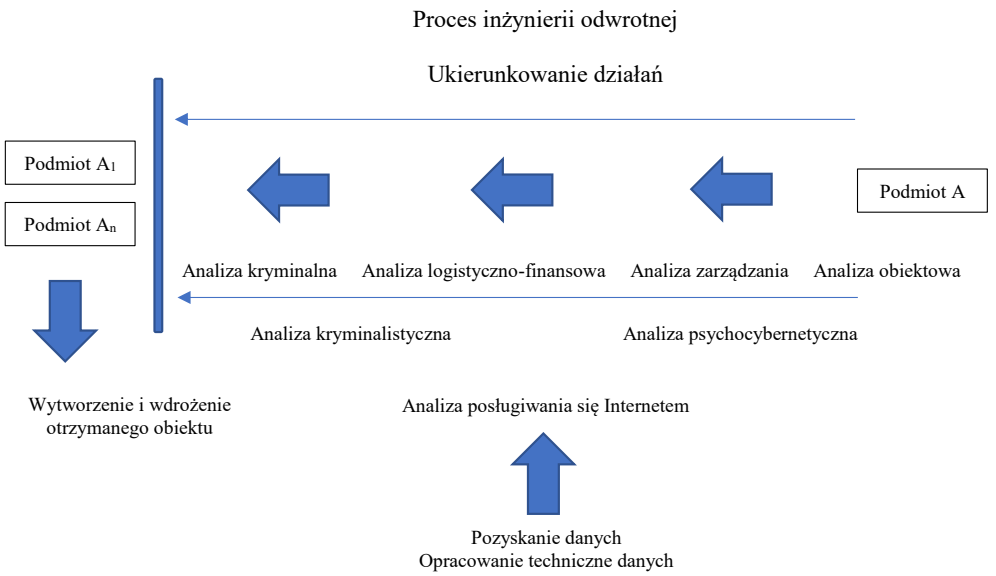
Schemat 1. Przebieg analizy przeprowadzonej z wykorzystaniem procesu inżynierii odwrotnej.

Źródło: Opracowanie własne.

Korelacja inżynierii postępowej (tradycyjnej) z inżynierią odwrotną w rozpoznawaniu struktur sieciowych

W inżynierii odwrotnej zakłada się docelowo, że uzyskany nowy model wyjściowy umożliwi skuteczniejszą reakcję organów ścigania (zarówno na poziomie śledczym, jak i operacyjnym). Rozpatrywanym obiektem może być zarówno organizacja przestępcza jako całość, jak i jej najmniej rozpoznana część, która nie została poddana badaniu ze względu na niewystarczającą liczbę informacji o samych węzłach oraz relacjach z innymi węzłami i otoczeniem. Wynikiem inżynierii postępowej jest ustalenie i zbadanie danego przedmiotu jako noszącego wartość dowodową. Stąd też jego stan odnosi się do określonego zdarzenia, czasu przeszłego oraz śladów pozyskanych w wyniku jego zbadania i przeprowadzonej analizy. W konsekwencji zarówno w fazie przedsądowej, jak i sądowej można przypisać winę sprawcy, któremu dany przedmiot (podmiot) będzie można sprawczo przyporządkować. Oznacza to zamknięcie pewnego procesu dowodowego dotyczącego określonego okresu aktywności przestępczej. Analiza RE nie poprzestaje na tym etapie. Jest to związane z dynamiką działań przestępczych, np. z „odrodzeniem się" działalności przestępczej pod innym kierownictwem, na innym obszarze geograficznym czy w innych rodzajowo obszarach, w których dotychczas grupa nie była przestępczo aktywna (np. w przestępczości narkotykowej, finansowej, kryminalnej). W przypadku inżynierii postępowej czynniki ocenne dla przedmiotu (grupy) będą charakteryzowały statyczny obraz jego działalności na dany czas. W przypadku RE będą to czynniki umożliwiające dynamiczną ocenę aktywności przestępczej w czasie i pozwalające na jej stały monitoring. Materiałem wyjściowym mogą być statyczne parametry wykorzystane w inżynierii postępowej, ale analityk będzie musiał na dalszych etapach zastosować metody dynamiczne, aby uzyskać cel postawiony na początku procesu RE. W konsekwencji powinien powstać aktualny i aktywny w czasie obraz dynamiki działań opracowywanego podmiotu. Przed rozpoczęciem analizy RE należy ocenić, z jakim rodzajem obszaru analitycznego analityk miałby do czynienia w przypadku prowadzenia czynności w ramach inżynierii postępowej. Prawdopodobnie realizowane czynności będą się skupiały na przygotowaniu materiału, który – jako włączony do postępowania – będzie materiałem dowodowym. Może, ale nie musi to ograniczać zastosowania określonej metody w ramach procesu RE. Dla przykładu, taką metodę w ramach tego procesu będzie można zastosować przy badaniu „niekompletnego" przedmiotu przestępstwa. Inżynieria odwrotna umożliwia ponowne zastanowienie się nad sprawą w zakresie wyszukania luk w procesie wykrywczym, rekapitulacji struktury sieciowej rozpracowywanej organizacji, zidentyfikowania rzeczywistego przywództwa itp., zwłaszcza gdy struktura przestępcza wymaga dłuższego czasu do jej rozpoznania. Dotyczy to różnych aktywności w Internecie, m.in. kontaktów z osobami spoza sieci przestępczej (np. przez czaty komunikacyjne Telegram i Signal czy w sieci Darknet), pozyskiwania technologii w celu jej konwersji na potrzeby przestępcze (po dokonaniu ponownego skonfigurowania i wykorzystania kodu, dodając tym samym

niepowtarzalną funkcjonalność i (lub) kontrolę danych)[55], wzrostu działań w obszarze logistycznym (zakup: broni, fałszywych kart, tożsamości, złośliwego oprogramowania czy pozyskiwanie środków finansowych), zmiany dotychczasowego systemu komunikacji, kamuflowania przywództwa i procesów decyzyjnych w sieci, deszyfracji danych, badania dialogu informacyjnego prowadzonego przez media zależne od organizacji terrorystycznych, nielegalnego wytwarzania elementów broni (w tym zakazanej proliferacją). Na schemacie 2 przedstawiono zastosowanie metod RE w rozpracowywaniu przestępczości zorganizowanej.



Schemat 2. Proces inżynierii odwrotnej zastosowany w odniesieniu do obiektu Podmiot A (do organizacji przestępczej).

Źródło: Opracowanie własne.

Zgodnie z powyższym schematem obiekt Przedmiot A (określany jako „Podmiot A") był wynikiem odwzorowania cyfrowego istniejącego w rzeczywistości. Podstawowym modelem analizowanym (mierzonym i przekształcanym) w procesie inżynierii odwrotnej jest Podmiot A (jako docelowy dla inżynierii postępowej i początkowy dla inżynierii odwrotnej). Inżynieria postępowa dotyczyła obszaru przestępstw dokonywanych wyłącznie lub w znacznej części w obszarze internetowym. W przypadku inżynierii odwrotnej będzie prowadzona analiza sieci komputerowej. Sieć zazwyczaj

[55] K. Podiņš, K. Geers, *Aladdin's Lamp: The Theft and Re-weaponization of Malicious Code*, w: *10th International Conference on Cyber Conflict CyCon X: Maximising Effects*, T. Minárik, R. Jakschis, L. Lindström (red.), Tallinn 2018, NATO CCD COE Publications, https://ccdcoe.org/uploads/2018/10/Art-10-Aladdins-Lamp.-The-Theft-and-Re-weaponization-of-Malicious-Code.pdf [dostęp: 21 XII 2020].

składa się z wielu małych sieci, które są administrowane przez różne podmioty, nie ma więc jednego miejsca, z którego można uzyskać pełny obraz określonej sieci docelowej. Także internet jest różnorodny, tak więc podejście uznane za przydatne w stosunku do jednych sieci może nie być skuteczne w innych miejscach[56]. Metoda RE może być pomocna również w przypadku zaginięcia części akt sprawy i potrzeby odtworzenia określonych wątków, przede wszystkim tych, które mają wartość dowodową lub zawierają plany realizacji sprawy.

Przedstawiona konstrukcja działania RE wobec Podmiotu A zakłada podejście blokowe (sektorowe) przy zrekonstruowaniu kategorii problemów, które powstają w konsekwencji funkcjonowania tego obiektu. Pozwala również – na podstawie posiadanych danych – na odtworzenie takiego samego obiektu lub uzyskanie innego, odpowiadającego w większym stopniu rzeczywistemu funkcjonowaniu badanego obiektu niż ten, który powstałby w wyniku czynności podjętych w ramach sprawy prowadzonej przez organy ścigania.

Poszczególne bloki (sektory) problemów mieszczą się w dokonaniu „zeskanowania" Podmiotu A przy użyciu już wcześniej zebranych aktualnych danych oraz nowych danych, a także przy użyciu metod analitycznych, w tym określenia mierzalnych parametrów matematycznych sieci przestępczej. Rozpoczęcie analizy może wynikać z wystąpienia określonego zdarzenia, np. zamachu terrorystycznego. W takiej sytuacji będzie możliwe nie tylko przeprowadzenie procesu RE w stosunku do urządzenia technicznego zniszczonego w zamachu (np. zastosowanego ładunku wybuchowego, wykorzystanych środków łączności), lecz także będzie można dokonać retrospektywnej oceny dotychczasowego rozpoznania sieci i ustalić, dlaczego nie doprowadziło ono do ujawnienia przygotowań do zamachu i określenia jego lokalizacji, a także do jego przerwania[57].

Jeżeli rezultatem zastosowania inżynierii odwrotnej będzie powstanie „doskonalszego" modelu Podmiotu A jako organizacji przestępczej, to powinno to spowodować poszerzenie wiedzy organów ścigania, dzięki czemu będzie można wyprzedzić dalszą aktywność przestępczą (analiza predykcyjna). Takie działania pozwolą skutecznie wyeliminować badaną organizację już w fazie przygotowania do przestępstwa, organy ścigania będą także mogły rozpocząć grę operacyjną, m.in. z wprowadzeniem własnej agentury czy też z wykorzystaniem imitacji takiej organizacji.

Model stworzony w wyniku procesu RE staje się pomocny m.in. przy odtwarzaniu struktury organizacji przestępczej (uzupełnianie ubytków struktury) lub rozpoznawaniu aktywności organizacji w sieci w obszarach, w których ma ona zdolności do działania bez pełnej informacji. Posługując się inżynierią odwrotną, będzie możliwe dokonanie oceny, na ile przestępcy przejęli systemy transformacyjne, transakcyjne, przemieszczania

---

[56] Hui Zhou i in., *Computer Network Reverse Engineering*, w: *Computer and Information Science 2011*, R. Lee (red.), Berlin 2011, s. 227–239, https://link.springer.com/chapter/10.1007/978-3-642-21378-6_18 [dostęp: 20 XII 2020].

[57] Przykłady zastosowania RE do urządzeń mobilnych zob. T. Heckmann, *Reverse engineering secure systems using physical attacks*, 2018, https://www.researchgate.net/publication/330618085_Reverse_engineering_secure_systems_using_physical_attacks [dostęp: 19 XII 2020].

przedmiotów, czyli na ile stworzyli alternatywne rozwiązania lub na jakim poziomie kontrolują funkcjonujące systemy dzięki kamuflowaniu swojej przestępczej działalności (dotyczy to także systemów bezpieczeństwa). Chodzi tu głównie o wyeliminowanie „fałszywego naśladownictwa" wykorzystywanego w celach przestępczych.

Podjęcie działań w zakresie inżynierii odwrotnej będzie wymagać rozłożenia na czynniki pierwsze całości wiedzy o Podmiocie A uzyskanej w danym momencie. Istotnym elementem procesu będzie ustalenie zgodności relacji „wpisanych" w konstrukcję z rzeczywiście zaistniałymi oraz stwierdzenie, czy przyjęte mierzalne relacje w sposób właściwy nadały atrybuty, a w konsekwencji – właściwości poszczególnym węzłom. Inaczej mówiąc, czy trafnie oceniono węzły na podstawie informacji o relacjach zachodzących między nimi, plasując je jako: przywódców, decydentów, pośredników i wykonawców. Ważne będzie także zbadanie, czy nie można ustalić atrybutów węzłów w inny sposób, co pomogłoby uzyskać ocenę odrębną od dotychczasowej. W ramach RE powinno być możliwe także ustalenie luk w relacjach (szczególnie tych, które były najważniejsze w ocenie węzłów) i uzupełnienie ich na tyle, żeby nowa konstrukcja umożliwiła weryfikację uzyskanego obiektu Podmiot A, a jednocześnie bardziej urealniła jego strukturę[58].

Przy założeniu, że obiekt ma strukturę sieci, jednym z działań będzie ustalenie parametrów tej struktury i sposobów ich mierzenia. Może to dotyczyć takich obszarów, jak: proces decyzyjny, posługiwanie się oprogramowaniem, wykorzystanie sieci społecznych, logistyka, lokalizacja GPS, posługiwanie się urządzaniami mobilnymi (w tym różnymi aplikacjami), transfer środków finansowych i innych aktywów. Pozyskiwanie parametrów można będzie podzielić na **wewnątrzpodmiotowe**[59] (zastosowane wyłącznie wobec analizowanego podmiotu) i **zewnątrzpodmiotowe** (uniwersalne, powszechnie stosowane wobec zachowań społecznych, indywidualnych w przestrzeni publicznej). Powinno się również wziąć pod uwagę relacje, jakie występują między węzłami (przygotowanie do dokonania statystycznej charakterystyki sieci). Podstawowym modelem analizowanym (mierzonym i przekształcanym) w procesie inżynierii odwrotnej jest Podmiot A. Uznając złożoność Podmiotu A, do jego rozłożenia na poszczególne elementy można wykorzystać analizę sieci kryminalnych jako metodę opartą na SNA (jest to związane z tym, że obiekt jest wycinkiem sieci społecznych, w których dochodzi do uzewnętrznienia działań przestępczych)[60]. Analiza sieci kryminalnych jest prowadzona

[58] Weryfikacja jest spowodowana tym, że w procesie inżynierii postępowej mogło dojść do zafałszowania oceny z powodu użycia wyłącznie jednego programu analitycznego, wpisania nieprawidłowych danych, subiektywnego myślenia analityka, kierowania się sugestiami lub rutyną, przyjmowania określonych zdarzeń za pewnik bez ich weryfikacji, złej oceny kodu organizacji przestępczej, pominięcia zdarzeń lub uznania niektórych za nieistotne z punktu widzenia całości prowadzonej analizy bądź przyjęcia niewłaściwego kodu typowanego dla rozpracowywanej organizacji przestępczej.

[59] Wyróżnienia w tekście pochodzą od autora (przyp. red.).

[60] Zob. K. Harężlak, M. Kozielski, *Metody analizy sieci kryminalnych*, „Studia Informatica" 2010, nr 2A, s. 35 i nast.

„do przodu" przez dokładanie komponentów do ustalonych węzłów sieci lub wprowadzanie do niej nowych węzłów (dekompozycja). W ramach procesu RE ważne będzie również ustalenie dla sieci stanu *zero-day* (czyli momentu rozpoczęcia działalności) dla luki, przez którą można zainstalować złośliwe oprogramowanie, ustalenie luk w rozwoju sieci, wskazanie pierwszego mocodawcy finansowego czy inspiratora działań przestępczych. W ramach RE należy określić stan początkowy, który będzie podstawą do „rozebrania sieci" na czynniki pierwsze. Ważne będzie ustalenie węzłów, wskazanie, jakie elementy oraz jakie rodzaje relacji wzięto pod uwagę w budowaniu krawędzi, np. czy relacje budowano na podstawie typowania udziału danej organizacji w określonym przestępstwie lub w kilku przestępstwach, o różnym stopniu rodzajowości. Czy, a jeśli tak, to jakie, relacje sieci z elementami spoza sieci (np. umieszczonymi w jej otoczeniu) wzięto pod uwagę? Co uwzględniono przy nadawaniu określonym węzłom przynależnej im wagowości (ścisłe kierownictwo, łącznicy, rekruci, bezpośredni wykonawcy, organizatorzy itp.) oraz przy badaniu relacji zachodzących między nimi (z wykorzystaniem obliczenia współczynnika korelacji r-Pearsona[61], który służy do sprawdzenia, czy dwie zmienne ilościowe są powiązane ze sobą związkiem liniowym).

Z uwagi na potrzebę dokonania ilościowej oceny poszczególnych węzłów do ich miarowania oraz skwantyfikowania ich relacji można wykorzystać **teorię grafów**. W badaniach istotne będzie także zbadanie atrybutu centralności poszczególnych węzłów zarówno w celu uzupełnienia informacji o sieci lub weryfikacji już posiadanych danych, jak i ustalenia rzeczywistego kierownictwa w sieci (mierzalność centralności stopnia, pośredniczenia lub bliskości). Przy analizie Podmiotu A należy mieć na uwadze, że wobec jego „odtworzenia" w procesie RE prawdopodobnie starano się zastosować specjalistyczne narzędzie analityczne, jakim posługują się analitycy kryminalni. Jeśli jednak wobec obiektu wykonywano czynności z zakresu SNA, to należy uwzględnić to, że analiza sieci społecznych może być nieadekwatnym (lub nie w pełni adekwatnym) instrumentem analitycznym, dlatego że różni się konstrukcją i wewnętrznymi relacjami od analizy sieci kryminalnych. Należy wziąć pod uwagę element manipulacji siecią na potrzeby kamuflażu – zarówno decydentów (w celu ich ukrycia w strukturze organizacji), jak i obszarów samej sieci, które są uznane za wrażliwe[62].

Kolejnym krokiem analizy będzie wizualizacja wyników w postaci grafu. Graf to zbiór punktów (zwanych wierzchołkami lub węzłami) połączonych krawędziami. Sieć przestępcza w znaczeniu matematycznym będzie określana jako graf wyrażony wzorem: $G = (V, E)$, gdzie V to zbiór węzłów (wierzchołków), $V(G) = \{v_1, v_2, ..., v_n\}$, a E to zbiór krawędzi: $E(G) = \{e_1, e_2, ..., e_n\}$. W większości zastosowań grafów w praktyce stosuje się grafy ważone, w których każdej krawędzi przyporządkowuje się liczbę

[61] Więcej na temat korelacji r-Pearsona zob. https://www.naukowiec.org/wiedza/statystyka/korelacja_745.html (przyp. red.).

[62] Nowatorskie badania w kierunku ujawniania kamuflażu w sieci prowadził M. Waniek. Zob. tenże, *Ukrywanie się w sieciach społecznych. Autoreferat*, https://depotuw.ceon.pl/bitstream/handle/item/2174/autoreferat-pl.pdf?sequence=3 [dostęp: 16 IV 2020].

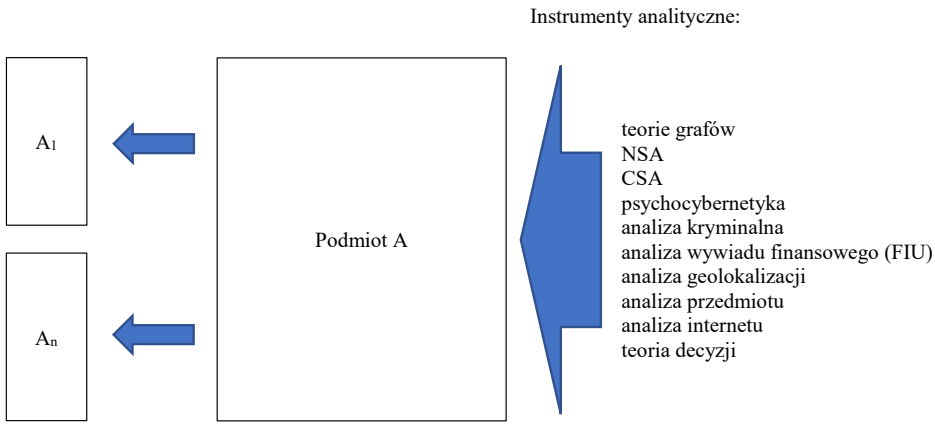
zwaną wagą tej krawędzi[63]. W ramach procesu RE będzie możliwe uzyskanie informacji o wierzchołku początkowym, a tym samym będzie można poddać ocenie, czy właściwe zdarzenie lub pewien określony czas zostały objęte działaniami organów ścigania w celu rozpracowania działalności grupy przestępczej. Sieć zostanie poddana analizie i „odtworzeniu" przepływu czynności, które będzie można odpowiednio zakwalifikować (jako przygotowanie do popełnienia przestępstwa, rozdysponowanie zysku przestępczego, wyznaczenie członka grupy do realizacji zleconego zadania, np. do modyfikacji cyberprzestrzeni i oprogramowania).

Zastosowanie inżynierii odwrotnej w obszarze przestępczości wiąże się z weryfikacją osiągniętego wyniku (obrazu Przedmiotu A), symulacją działań przy użyciu odpowiedniego algorytmu umożliwiającą wykrycie kamuflowania się węzłów w sieci, dodaniem nowych danych nieznanych jeszcze podczas prowadzenia sprawy lub tych samych danych, ale ponownie zweryfikowanych. Ta ostatnia czynność może zostać uzupełniona o niewykryty cykl działania przestępczego, który można połączyć z potwierdzonym przestępczym „efektem" działalności członków grupy. Wynikiem analizy będzie wyciągnięcie wniosków dotyczących hierarchiczności w grupie, przyjętego procesu decyzyjnego, wariantu działań optymalnego dla osiągnięcia zysku przestępczego bądź innego, który skutkował ograniczeniem zysku, ale zapewnił wyższy poziom bezpieczeństwa nielegalnej działalności (ustalenie przyczyny podjęcia takiej decyzji). Oceniając czynności: poprzedzającą i następującą, można uzyskać wiedzę na temat tego, czy grupa przestępcza miała odpowiedni własny potencjał do realizacji przestępczego przedsięwzięcia, czy też musiała się posiłkować elementami z otoczenia, a także czy pominięto dystrybucję aktywów, informacji, udziału w realizacji zadania określonych członków, czy i co było przyczyną ograniczenia osobowego udziału w przestępczej realizacji (np. posiadanie lub pozyskanie złośliwego oprogramowania, sposób jego użycia wedle procesu RE).

Inżynier prowadzący analizę może uzyskać jednocześnie wiedzę na temat, z jakim rodzajem sieci przestępczej ma do czynienia (lub jaki potencjał ma ta sieć) oraz czy jest to sieć deterministyczna, w której czas wykonania czynności zmierzających do popełnienia przestępstwa jest jednoznacznie określony (zdeterminowany). W takim rodzaju sieci każdy zaplanowany etap musi być zrealizowany, aby osiągnąć wyznaczony cel. Analityk będzie też mógł sprawdzić, czy sieć ma charakter stochastyczny, tzn. taki, że w danym przypadku trudno będzie określić czas wykonania czynności (sieć o charakterze losowym). W tym drugim przypadku będzie można określić stopień zorganizowania w grupie oraz podporządkowania, czy grupa ma potencjał wykonawczy, czy jest on ograniczony bądź nie ma go w ogóle, a także czy występują czynniki ograniczające w czasie przygotowanie do przestępstwa. Wnioskiem może być również stwierdzenie, że organy ścigania nie miały wiedzy na temat czasu popełnienia przestępstwa, co wyzwala

[63] Szerzej zob. A. Woźniak, *Grafy i sieci w technikach decyzyjnych*, „Infrastruktura i Ekologia Terenów Wiejskich" 2010, nr 4, s. 1–188, http://agro.icm.edu.pl/agro/element/bwmeta1.element.dl-catalog-0eeb75a5-4306-49e7-ab42-ce3dd480539a [dostęp: 16 VI 2020].

potrzebę „dosztukowania" brakującego elementu całości, czyli oceny tego, gdzie i w jakim czasie doszło do przestępstwa (typowanie będzie się odbywało w przedziale czasowym między najwcześniejszym możliwym a najpóźniejszym dopuszczalnym terminem). Na schemacie 3 przedstawiono zastosowanie instrumentów analitycznych wykorzystywanych w analizie grup przestępczych metodami stosowanymi w ramach procesu RE.



Schemat 3. Zastosowanie instrumentów analitycznych na potrzeby inżynierii odwrotnej do Podmiotu A (do organizacji przestępczej).

Źródło: Opracowanie własne.

Na podstawie analizy obiektowej, zarządzania i logistyczno-finansowej oraz ze źródeł zewnętrznych będzie możliwe zgromadzenie danych o Podmiocie A. Platformą do dalszych działań w ramach RE będzie dotychczasowa platforma analityczna lub inna, wykorzystywana na potrzeby inżynierii postępowej, dlatego też przed posłużeniem się zgromadzonymi danymi w ramach RE niezbędne będzie ich techniczne opracowanie oraz weryfikacja, a czasami także walidacja. Wiąże się to przede wszystkim z potrzebą wyeliminowania błędów związanych z techniczną stroną analizy (np. użyciem różnych programów) oraz weryfikacją zapisów językowych (np. odmienności zapisów nazwisk, nazw miejscowości, co często występuje przy transkrypcji z cyrylicy lub języka arabskiego). Powodzenie całego procesu zależy od dokładności opracowywanych informacji lub danych na poszczególnych etapach. Pozyskanie danych będzie można przeprowadzić w ramach analizy obiektowej, w której należałoby także dokonać ustalenia celu, jaki został założony przy uzyskaniu Podmiotu A (analiza całościowa, częściowa realizacja założeń lub brak ich realizacji).

Stan wyjściowy dla RE jest istotny z punktu widzenia zakładanego celu, tj. czy chce się uzyskać ponową ocenę obiektu po uzupełnieniu braków w jego funkcjonowaniu (Podmiot A_1), czy dąży się do zbudowania całkiem nowego modelu (Podmiot A_n),

w przypadku, gdy uznano, że model Podmiotu A powstał w wyniku błędu. Całość działań powinna być oparta na strukturze sieciowej rozpatrywanej organizacji jako najbardziej skutecznego modelu analitycznego na potrzeby dalszych czynności w ramach RE. W grę będzie wchodziło np. przyjęcie innych niż dotychczas atrybutów do oceny węzłów tej samej sieci. Analiza obiektowa powinna więc obejmować węzły sieci, krawędzie oraz atrybuty (właściwości) węzłów (ocenie powinno się poddać wszystkie składowe, które są szczegółowo analizowane i rozwijane). Analiza obiektowa to źródło informacji o Podmiocie A. Po ponownej ocenie Podmiotu A będzie można uzyskać ten sam Podmiot A_n, który stanie się ulepszoną wersją Podmiotu A, uzyskaną w wyniku uzupełnienia wiedzy o poszczególnych jego elementach lub też nowy Podmiot A_1, który będzie stanowił odzwierciedlenie Podmiotu A, ale w nowej, „lepszej" wersji (otrzymanie docelowego modelu parametrycznego). Dzięki modelowi A_1 będzie możliwe podjęcie działań, które skuteczniej zneutralizują analizowany Podmiot A, lub zyskanie czasu na przeprowadzenie gry na potrzeby jego neutralizacji.

Pierwszy przypadek zaistnieje wtedy, gdy w wyniku zastosowania RE zostanie stwierdzone, że dotychczasowe działania prowadzone „do przodu" nie zawierają istotnego błędu, a jedynie wiedza o Podmiocie A była niepełna. Drugi natomiast – gdy po zastosowaniu RE uzna się, że kierowano się błędnymi założeniami i informacjami, w wyniku czego uzyskano Podmiot A, który jest nieadekwatny do rzeczywistości, co spowodowało niezrealizowanie zakładanego celu działania. Będzie ono uzależnione między innymi od możliwości pozyskania danych o obiekcie oraz od tego, jakich czynności analitycznych nie wykonano w ramach inżynierii postępowej. Na temat pierwszego podejścia w zakresie „uzupełnianie posiadanych informacji" pisał w swojej pracy dotyczącej poszukiwania węzłów ukrytych Marcin Waniek. Wskazał on, że (…) *ze względu na tę trudność w modyfikowaniu istniejącej sieci, kierujemy swoją uwagę na inne pytanie, mianowicie rozważamy, w jaki sposób można zbudować sieć ukrytą od zera tak, aby jej przywódcy pozostali ukryci, jak również aby utrzymywali swój wpływ na pozostałych członków sieci. Nasze rozwiązanie opiera się na pomyśle, aby otoczyć przywódców grupą zaufanych „kapitanów", których rolą jest ukrycie przywódców oraz pośredniczenie w ich komunikacji z pozostałymi członkami sieci*[64]. Tworzenie nowego modelu wydaje się bardziej możliwe do zrealizowania i sprowadza się do wykonania nieprzeprowadzonych analiz lub też ich ponownego dokonania, ale z uwzględnieniem takich konfiguracji, które w sposób najbardziej prawdopodobny wypełnią luki informacyjne dotyczące rozpoznawanego obiektu.

W inżynierii odwrotnej dodatkowym wsparciem dla analizy obiektowej są analizy: zarządzania i logistyczno-finansowa. Pozwalają one dokładniej zbadać procesy zachodzące w ramach samego Podmiotu A oraz jego relacje z otoczeniem. Powinny

[64] M. Waniek, *Ukrywanie się w sieciach społecznych*…, s. 4. Zob. także: M. Waniek, T.P. Michalak, T. Rahwan, *Hiding in Multilayer Networks*, 2019, s. 1–24, arXiv, 14 XI 2019 r., https://arxiv.org/pdf/1911.05947.pdf [dostęp: 20 XII 2020].

one być też całkowicie obiektywne[65]. Pierwsza z nich wywodzi się z wprowadzenia SNA do zarządzania strukturami organizacyjnymi, druga pozwala ocenić kanały zewnętrznego zasilania środkami finansowymi, dysponowania nimi w ramach organizacji, w tym podział na zyski osobiste oraz zapewniające bezpieczeństwo finansowe organizacji, z uwzględnieniem zaangażowania środków w przedsięwzięcia przestępcze (np. organizację przemytu narkotyków, dokonanie zamachu terrorystycznego). Analiza logistyczno-finansowa pozwala również na ocenę kanałów pozyskania i wykorzystywania logistycznych aktywów na potrzeby organizacji, np. utrzymanie „dziupli" do przechowywania i demontażu kradzionych samochodów, znalezienie miejsca na laboratorium do produkcji narkotyków syntetycznych, zapewnienie bazy szkoleniowej dla terrorystów. W ramach pozyskiwania nowych danych, zwłaszcza zewnętrznych, będzie dochodziło do procesu dyskretyzacji (digitalizacji lub kwantowania), czyli przekształcania danych zdobytych analogowo w dane cyfrowe, którymi posługuje się analiza kryminalna[66] przy budowie obiektu – Podmiotu A. W takim przypadku należy pamiętać o ocenie prawdziwości zgromadzonych danych i ich weryfikacji, tak aby nie dopuścić do wygenerowania kolejnego obiektu z błędem lub aby nie dokonać niewłaściwej korekty analizowanego obiektu. Takie dane powinny być wprzężone w proces obowiązkowej walidacji.

Przeprowadzenie wymienionych trzech etapów RE, tj. analiz: obiektowej, zarządzania i logistyczno-finansowej, powinno pozwolić na przejście do kolejnego, ostatecznego etapu procesu RE, czyli wytworzenia i wdrożenia danych. Należałoby się tu posłużyć metodą analizy kryminalnej lub innym rodzajem analizy sieciowej, która po przetworzeniu danych powinna umożliwić uzyskanie wyniku. Zarówno w analizie obiektowej, jak i zarządzania trzeba uwzględnić struktury komunikacyjne organizacji stanowiące centrum przepływów informacji w organizacji i mogące tuszować i zamazywać rzeczywistą strukturę sieci. Wsparciem będzie też analiza internetowa, dzięki której będzie można scharakteryzować zarówno poszczególne węzły, jak i sposób działania organizacji. W grę będą wchodziły takie analizy, jak: *readability analysis* (analiza, jak czytelny jest dany tekst), *structural analysis* (analiza struktury sieci), *link analysis* (analiza powiązań między węzłami w sieci), *form analysis* (analiza formularzy do wypełnienia)[67] oraz *content analysis* (analiza treści, stosowana

[65] Obiektywizm wiąże się z przyjęciem założenia, że za dane uznaje się nie informacje uzyskane od informatora, lecz te dostarczane z GPS statków wodnych, przeprowadzonych odpraw towarów w portach, towaru przyjętego do hurtowni, przemieszczania się samochodów dostawczych itp.

[66] W zakresie ponownej oceny przebiegu poszczególnych przestępstw kryminalnych, identyfikacji wielu innych przestępstw wykazujących związek z tymi zasadniczymi, określania struktury siatek przestępczych oraz analizowania zakresu i sposobu prowadzenia działalności przestępczej zob. M. Kobylas, *Analiza kryminalna dla studentów bezpieczeństwa wewnętrznego*, Szczytno 2014, s. 13.

[67] Analiza formularzy to narzędzie przeznaczone dla witryn, które aktywnie używają formularzy do wypełniania. Analiza formularzy pomaga firmom zrozumieć, w jaki sposób użytkownicy wchodzą w interakcję z formularzami w ich witrynie internetowej, a także ocenić ich formularze w celu zidentyfikowania problemów, które mogą utrudniać użytkownikom pomyślną konwersję, https://www.indicative.com/data-defined/form-analysis/ [dostęp: 20 XII 2020].

zarówno do form słownych, jak i graficznych)[68]. Przejrzenie danych w internecie w ramach analizy kryminalnej powinno być przeprowadzone zarówno na poziomie dostępnym, jak i na poziomie sieci ukrytych. Struktura sieci jest odzwierciedleniem i przestępstw jawnych, widocznych (śladów pozostawionych w sieci, w rzeczywistości), i ukrytych, niewidocznych (nieujawnionych śladów pozostawionych w sieciach internetowych i w rzeczywistości). Do przestępstw ukrytych będzie można zaliczyć: ślady sieciowe, które mogą zostać wykryte dopiero po dokonaniu grafowania, wysoko zakonspirowane sieci szpiegowskie, kradzieże podstawowego oprogramowania w systemach teleinformatycznych obrony, bezpieczeństwa itp. i zastosowanie w nich złośliwego oprogramowania, co może być wykryte dopiero po analizie wykonanej w ramach procesu RE.

Jak już wspomniano, w wyniku wykorzystania metody RE będzie można otrzymać Podmiot A_1 lub Podmiot A_n. Stworzenie nowych obiektów jest związane między innymi z wypełnieniem luki informacyjnej, luki dotyczącej zarządzania obiektem wynikającej z braku wiedzy o rozpoznawanym obiekcie bądź pozyskanej z tego obiektu, a także z niewykorzystaniem środków technicznych. Zastosowanie RE umożliwi poszerzenie wiedzy o funkcjonowaniu rozpatrywanego obiektu dotyczącej: zmiany kierownictwa, zmiany stylu zarządzania, ustalenia nowych nieznanych zdarzeń przestępczych, uzupełnienia składu osobowego organizacji, weryfikacji ról w samej organizacji i jej otoczeniu oraz przypisania członkom organizacji nowych czynów przestępczych. Będzie to możliwe w wyniku „dosztukowania" do Podmiotu A tych elementów, które dają jego obraz całościowy. Ten nowy model Podmiotu A jest rezultatem nie tylko pozyskania nowych informacji (lub przeanalizowania ich na nowo i otrzymania odmiennych wniosków), lecz także zastosowania innych technik pomiarowych i analitycznych. Tym samym zasób analiz wymienionych w opracowaniu nie jest skończony i może być uzupełniony np. o nowe analizy kryminalistyczne śladów (także te wdrożone do badań jako wynik rozwoju technologicznego czy badań naukowych). Dzięki temu będzie można ustalić sprawców, którzy byli dotychczas nieznani, lub wykazać inny przebieg zdarzenia przestępczego. Nie ulega wątpliwości, że w przypadku danych otrzymanych z badań kryminalistycznych ich odmienność lub ich większe sprecyzowanie może być wynikiem zarówno zastosowania niewykorzystanej do tej pory w sprawie metody badawczej, jak i bardziej precyzyjnych urządzeń technicznych, obliczeniowych bądź wykorzystania danych przetworzonych w bazach danych nieznanych organom ścigania.

Zastosowanie w analizowanej sprawie inżynierii postępowej jest realizowane głównie pod kątem ekonomiki postępowania organów ścigania, co może spłycać działania operacyjne oraz dowodowe jedynie do czynów możliwych do udowodnienia oraz do postawienia zarzutów kierowania i zakładania organizacji przestępczej (grupy lub związku). Tym samym będą pominięte wątki uboczne, których udowodnienie wymaga znacznego nakładu sił i środków. Taki tryb postępowania może być także

[68] J. Scoccimaro, S. Rugaber, *Reverse Engineering of Web Pages*, https://www.cc.gatech.edu/projects/PageSleuth/documents/icpc.pdf [dostęp: 30 IV 2020].

wynikiem taktyki śledczej przyjętej przez prokuratora. Rezultat końcowy – odmienna konstrukcja Podmiotu A – może zostać osiągnięty po zastosowaniu metody analizy kryminalnej, w której wykorzystano inny niż dotychczas program analityczny. W analizie zarządzania będzie można ustalić relacje między kierownictwem organizacji a wykonawcami, a także sprawdzić, czy dobór celu, wykonawców, decyzji i środków jest prowadzony na zasadzie optymalizacji zysku, czy też przez zminimalizowanie kosztów wykonawczych. Aby uwzględnić wskazane preferencje, należy zastosować grafy ważone. Ustalenie preferencji może być pomocne przy określeniu, czy przywódcy tak samo traktują wszystkich wykonawców, czy też dokonują ich gradacji, stosując obiektywne (obojętne) wyznaczniki, czy też kierują się własnymi preferencjami (subiektywne wyznaczniki). Wynikiem takiej analizy powinno być ustalenie schematu postępowania kierownictwa, które może kierować się kosztami wykonawstwa (minimum nakładów przy maksimum zysku) albo realizacją celu za wszelką cenę (bez względu na poniesione koszty).

Przeprowadzenie analizy logistyczno-finansowej obiektu będzie wymagało uwzględnienia przynajmniej dwóch płaszczyzn aktywności przestępczej – logistycznej i finansowej. Pierwsza będzie związana z korzystaniem przez sprawców przestępstw z tych systemów, które są ogólnodostępne (np. firmy świadczące usługi pocztowe, firmy kurierskie, przewozy kontenerowe statkami, transport lądowy lub kolejowy, transport międzynarodowy, sortownie, hurtownie, lokalni dystrybutorzy, giełdy towarowe). Druga płaszczyzna – finansowa – jest związana z instrumentami oferowanymi w ramach usług takich instytucji, jak banki, towarzystwa ubezpieczeniowe, ale również z usługami oferowanymi na czarnym rynku (nielegalne przemieszczanie towarów oraz środków finansowych, np. przemyt fizyczny towarów, system „czarna hawala", nielegalne rozliczenia gotówkowe, wykorzystanie podmiotów rejestrowanych na obszarach *offshore*). Przedmiotowe obszary będą wymagały badań ilościowych (liczby powiązań w określonym czasie), ale w kontekście relacji międzyosobowych.

Zastosowanie analizy sieciowej w badaniach relacji nieformalnych (społecznych, interpersonalnych) może niejednokrotnie być narzędziem służącym ujawnieniu dodatkowych informacji kryjących się w ramach istniejących sformalizowanych struktur wewnątrz- i międzyorganizacyjnych, niewidocznych dla innych ilościowych metod badawczych[69]. Na analizę logistyczno-finansową działań organizacji przestępczych należy patrzeć m.in. pod kątem typowania rozwiązań jako najbardziej optymalnych z punktu widzenia zysku biznesowego. Można pod to podciągnąć przeprowadzenie procederu legalizacji środków (prania brudnych pieniędzy), tak aby skorzystać z formalno-prawnych i organizacyjnych rozwiązań niezbędnych do wykazania legalności aktywów, które pozostają w dyspozycji organizacji. Innym przykładem będzie zapewnienie sobie kontroli lub powołanie podmiotów w obszarze logistyki i finansów, które będą źródłem pierwotnych dochodów dla organizacji przestępczej.

[69] C.R. Carter, L.M. Ellram, W. Tate, *The Use of Social Network Analysis in Logistics Research*, „Journal of Business Logistics" 2007, nr 1.

Analiza sieci obiektu może również ujawnić potrzebę zoptymalizowania własnych celów przestępczych przy wykorzystaniu formalnych kanałów dystrybucji towarów czy środków finansowych. Takie działania będą wynikały z konieczności zapewnienia bezpieczeństwa i tajności operacjom koordynowanym przez członków struktury przestępczej lub terrorystycznej. Poszerzenie analizy obiektu pod kątem udziału w procederze prania pieniędzy bądź finansowania terroryzmu będzie wymagało przeprowadzenia dodatkowego miarowania obiektu przy wykorzystaniu jednostki wywiadu finansowego i zastosowanej analizy opartej na ryzyku w ramach AML/CFT[70] instytucji obowiązanej oraz analizy wywiadu finansowego przeprowadzonej bezpośrednio w jednostce. Aspekty odwrotnej rekapitulacji powinny zostać uwzględnione w ramach inżynierii odwrotnej obiektu Podmiot A. W przypadku zastosowania pomiaru obiektu pod kątem analizy finansowej będzie możliwe przyjęcie rozwiązania ocennego opartego na modelu organizacji przestępczej jako modelu biznesowego przedsiębiorstwa[71]. Zarówno model zorganizowanej grupy przestępczej jako model (nielegalnego) przedsiębiorstwa, jak i model biznesowy organizacji terrorystycznej zbliżają się do modeli ekonomicznych tego rodzaju układów grupowych[72]. Model ekonomiczny uwzględnia przede wszystkim zachowania związane z nielegalną dystrybucją towarów, usługami związanymi z ich wytwarzaniem oraz z redystrybucją zysków otrzymanych w wyniku handlu nimi. Podobnie jak każde przedsiębiorstwo organizacja terrorystyczna także wymaga pewnych podstawowych zasobów, które są niezbędne do tego, aby mogła istnieć. Przy takim spojrzeniu na funkcjonowanie organizacji terrorystycznej należy mieć na uwadze to, że ze względu na jej możliwości funkcjonalne, w tym ofensywne (operacyjne), powinna ona spełniać określone wymogi absorpcji środków. Pozytywna ocena organizacji jest możliwa jedynie wówczas, gdy za dedykowane środki jest ona w stanie zrealizować cel stawiany jej przez sponsorów, czyli po prostu być skuteczna.

W ramach miarowania Podmiotu A będzie można dodatkowo przeprowadzić analizę psychocybernetyczną[73], w której wykorzystuje się metodę dynamizmu

---

[70] *Anti Money Laundering/Counter Financing of Terrorism* – zbiorcze określenie przepisów i zasad, które muszą stosować firmy świadczące usługi finansowe, aby zapobiegać praniu brudnych pieniędzy i finansowaniu terroryzmu. Procedury z tym związane polegają głównie na monitorowaniu podejrzanych transakcji. Za: https://cryps.pl/definicja/aml-cft-anti-money-laundering-counter-financing-of-terrorism/ [dostęp: 1 II 2021] – przyp. red.

[71] W zakresie modelu biznesowego organizacji przestępczej typu kryminalnego zob. D.C. Smith, *Paragons, Pariahs and Pirates: A Spectrum-Based Theory of Enterprise*, „Crime & Delinquency" 1980, nr 3.

[72] Odnośnie do modelu biznesowego organizacji terrorystycznej zob. G. Ortmann, *Deconstructing the Business of Terrorism. A Case Study of JNIM in Mali*, CERIS, http://www.ceris.be/fileadmin/library/Research-Papers-Online/Thesis-Deconstructing_the_business_of_terrorism.pdf [dostęp: 30 IV 2020].

[73] Psychocybernetyka może przyczynić się do wytypowania właściwych przywódców organizacji przestępczej, którzy są zdolni do kierowania działaniami nie tylko o charakterze wykonawczym (dokonywania przestępstw, także zorganizowanych), lecz także potrafią pokierować organizacją jako bytem organizacyjnym zdolnym do utrzymania funkcjonalnej równowagi organizacji

charakteru, zmierzającą do ustalenia rzeczywistego kierownictwa organizacji. Zastosowanie cybernetyki w odniesieniu do charakteru człowieka, głównie dynamizmu charakteru, pozwala na ocenę relacji w ramach organizacji przestępczej oraz na typowanie charakteru przywództwa organizacji. Jest to dodatkowy element, który organy ścigania muszą poddać ocenie i analizie przy planowaniu i realizowaniu działań taktycznych zarówno wobec poszczególnych członków organizacji przestępczej, jak i organizacji jako całości. Te działania mogą być nacechowane poszukiwaniem słabych punktów charakterologicznych osób angażujących się w przestępczość zorganizowaną i działania terrorystyczne (profilowanie cybernetyczne)[74]. Tym samym miarowanie będzie mogło być wynikiem zastosowania zarówno metod ilościowych (wynikających z zastosowania SNA), jak i jakościowych (analiza psychocybernetyczna).

Zwieńczeniem procesu inżynierii odwrotnej zastosowanego wobec Podmiotu A (jako obiektu wyjściowego) powinno być przeprowadzenie czynności analitycznych w ramach analizy kryminalnej lub alternatywnego programu analitycznego umożliwiającego taką ocenę dotychczasowych danych, które mogą wykreować obiekty: A_1 lub A_n. Zastosowanie alternatywnego programu analitycznego może przyczynić się do tego, że zostanie przeprowadzona analiza jakościowa tego samego obiektu pod kątem nasycenia go takimi wnioskami i oceną faktów, które przyczynią się do skutecznej reakcji organów ścigania i w rezultacie – do neutralizacji struktury przestępczej. Reakcja powinna być skierowana na wyeliminowanie najbardziej istotnych węzłów sieci, precyzyjne określenie miejsca poszukiwania śladów (dowodów), a także ustalenie miejsca, w których jest gromadzone mienie przestępcze lub jaki jest poziom zaangażowania ich w inwestycjach.

Zastosowanie RE powinno umożliwić także opracowanie specjalnych narzędzi analitycznych przystosowanych do wybranego obiektu. Należy jednak pamiętać, że organy ścigania muszą działać w granicach prawa, a ich instrumenty przeciwdziałania, głównie te o charakterze operacyjno-rozpoznawczym, są ściśle sformalizowane i reglamentowane prawnie. Stąd też wnioskowanie będzie dotyczyło zaproponowania zmian w aktualnych przepisach, które będą obowiązywać w przyszłości. Proces RE należy ocenić pod kątem działań pragmatycznych. Bardziej zatem należałoby ją postrzegać jako wprowadzanie nowych rozwiązań, np. zastosowanie nowego programu analitycznego bądź nowej metody badawczej z zakresu kryminalistyki. Podstawową wadą wykorzystania RE będzie ryzyko stworzenia kolejnych luk w analizach, bez uzyskania optymalnego rozwiązania, które może okazać się nieefektywne i droższe w realizacji, jak również to, że sam proces pochłonie zasoby, które można by było przeznaczyć na rozwój i badania w zakresie inżynierii postępowej. Inżynieria odwrotna powinna być uznana za działanie

w czasie. Zob. M.A. Kędzierski, *Zastosowanie rozwinięcia teorii układów samodzielnych na potrzeby typowania przywództwa organizacji przestępczej – analiza psychocybernetyczna*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 129.

[74] Zob. tamże, s. 128 i nast.; M.H. Górny, *Psychocybernetyka w pracy Policji – zarys zagadnienia*, „Kwartalnik Prawno-Kryminalistyczny" 2010, nr 5, s. 97 i nast.

ostateczne, wprowadzone w przypadku braku powodzenia inżynierii postępowej, która wobec zorganizowanych form przestępczości wykorzystuje tradycyjne rozwiązania operacyjno-śledcze i analityczne. Metody wprowadzane w ramach procesu RE mogą być pomocne przy przygotowywaniu kolejnych etapów rozpoznania tych struktur przestępczych, które charakteryzują się wysokim poziomem przetrwania (sieci mafijne, terrorystyczne). Odwrotnością RE jest aktywne i wieloaspektowe działanie w ramach inżynierii postępowej, w różnych kierunkach i przy jak najszerszym wykorzystaniu instrumentów, jakimi dysponują organy ścigania, służby i inne podmioty w celu przeciwdziałania aktywności zorganizowanych grup przestępczych i organizacji terrorystycznych, w tym korzystanie z nowatorskich badań sieci opartych na teorii grafów.

Podsumowanie

Zastosowanie inżynierii odwrotnej do analizy organizacji przestępczych typu sieciowego wydaje się jak najbardziej możliwe. Rozwiązania proponowane obecnie wskazują na to, że jest możliwe dokonanie oceny działań organizacyjnych przez badanie procesu decyzyjnego przywódców, taktyki przestępczej czy mechanizmów stosowanych przy cyberatakach. Wykorzystanie RE w stosunku do tak rozbudowanych podmiotów, jak sieci przestępcze czy terrorystyczne, które chrakteryzują się zmiennością, a czasem małą mierzalnością atrybutów, będzie niejako kreatorem wektorowym. Oznacza to, że zastosowanie RE w bardziej wymiernych obszarach powinno się przełożyć na zwiększenie mierzalności samej sieci. Wydaje się, że RE może być stosowana głównie w badaniu przedmiotu przestępstwa (w tym zamachów terrorystycznych), procedur decyzyjnych tworzonych przez organy ścigania na potrzeby budowania taktyki kontrprzestępczej, ale także w badaniu każdego zdarzenia, w którym organizacja przestępcza posługuje się autonomicznym oprogramowaniem służącym do popełniania przestępstw. Należy pamiętać, że również same sieci przestępcze pozyskują specjalistów z zakresu inżynierii odwrotnej. Dzięki tym osobom organizacje przestępcze mogą rozpracowywać i przekształcać oprogramowania służące celom militarnym, strategicznym czy logistycznym, wykorzystywanym przez organy państwowe działające głównie w dziedzinie bezpieczeństwa i w sferze militarnej. Dlatego wielkim wyzwaniem dla organów odpowiadających za bezpieczeństwo państwa jest podejmowanie działań zabezpieczających – zarówno dotyczących dysponowania tożsamością czy technikami logistycznymi w zabezpieczeniu operacji militarnych, jak i bronią jądrową. W konsekwencji matryca aktywności w obszarze inżynierii odwrotnej, a w przypadku sieci przestępczej – „brudnej" inżynierii odwrotnej, staje się podstawą do wagowania wytypowanych elementów sieci i do prowadzenia działań analitycznych na tej strukturze organizacyjnej. Inżynieria odwrotna w zakresie analizy sieci jest działaniem wtórnym, ale strategicznym, pomocnym w modelowaniu kontrataków na poszczególne wagowane węzły oraz na całe struktury sieci (zwłaszcza te działające w cyberprzestrzeni).

Bibliografia

Blaha M.R., *A Manager's Guide to Database Technology: Building and Purchasing Better Applications*, wyd. 1, [bmw] 2000, Pearson.

Carter C.R., Ellram L.M., Tate W., *The Use of Social Network Analysis in Logistics Research*, „Journal of Business Logistics" 2007, nr 1, s. 137–168.

Chatagnier J.T., Mintz A., Samban Y., *The Decision Calculus of Terrorist Leaders*, „Perspectives on Terrorism" 2012, nr 4–5, s. 125–144, https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2012/issue-4/the-decision-calculus-of-terrorist-leaders--j.tyson-chatagnier-alex-mintz-and-yair-samban.pdf [dostęp: 20 XII 2020].

Chikofsky E.J., Cross II J.H., *Reverse engineering and design recovery: a taxonomy*, „IEEE Software" 1990, nr 1, s. 13–17.

Czakon W., *Sieci w zarządzaniu strategicznym*, Warszawa 2012, Wolters Kluwer Business.

Fronczak A., Fronczak P., *Świat sieci złożonych: Od fizyki do Internetu*, Warszawa 2009, Wydawnictwo Naukowe PWN.

Gagg C., *Domestic product failures – Case studies*, „Engineering Failure Analysis" 2005, nr 5, s. 784–807.

Górny M.H., *Psychocybernetyka w pracy Policji – zarys zagadnienia*, „Kwartalnik Prawno-Kryminalistyczny" 2010, nr 5, s. 92–97.

Harężlak K., Kozielski M., *Metody analizy sieci kryminalnych*, „Studia Informatica" 2010, nr 2A, s. 35–46.

Hui Zhou i in., *Computer Network Reverse Engineering*, w: *Computer and Information Science* 2011, R. Lee (red.), Berlin 2011, Springer, s. 227–239, https://link.springer.com/chapter/10.1007/978-3-642-21378-6_18; [dostęp: 20 XII 2020].

Kachel S. i in., *Zastosowanie inżynierii odwrotnej do procesu odtwarzania geometrii układu wlotowego silnika RD-33 w samolocie MIG 29*, „Prace Instytutu Lotnictwa" 2011, nr 213, s. 66–84, http://ilot.edu.pl/PIL/PIL_213.pdf [dostęp: 14 IV 2020].

Kędzierski M., *Zastosowanie rozwinięcia teorii układów samodzielnych na potrzeby typowania przywództwa organizacji przestępczej – analiza psychocybernetyczna*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 128–144.

Klimas P., *Podejście sieciowe w logistyce*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 2015, nr 249, s. 38–48.

Kobylas M., *Analiza kryminalna dla studentów bezpieczeństwa wewnętrznego*, Szczytno 2014, WSPol.

Kowalska-Musiał M., *Strukturalna metodologia pomiaru sieci społecznych – rys historyczny i współczesne obszary zastosowań*, „Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie" 2013, nr 28, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ekon-element-000171350117 [dostęp: 15 II 2021].

Kurzynowski T. i in., *Proces inżynierii odwrotnej w zastosowaniach kryminalistycznych*, „Problemy Kryminalistyki" 2014, nr 285, s. 4–46.

Lewandowski M., *Pomiar mediów społecznościowych jako element zarządzania wiedzą i informacją w przedsiębiorstwach*, „Acta Universitatis Nicolai Copernici. Zarządzanie" 2018, nr 4, s. 115–122, https://apcz.umk.pl/czasopisma/index.php/AUNC_ZARZ/article/view/AUNC_ZARZ.2018.049/17178 [dostęp: 16 IV 2020].

Pawluszko T., *Poliheurystyczna teoria podejmowania decyzji w analizie bezpieczeństwa*, „Colloquium Pedagogika – Nauki o Polityce i Administracji" 2020, nr 1, https://colloquium.amw.gdynia.pl/index.php/colloquium/article/view/164/157 [dostęp: 15 II 2021].

Polanowska-Sygulska B., *Użyteczność a maksymalizacja bogactwa: Filozoficzne zakorzenienie poglądów Chicagowskiej szkoły law & economics*, „Archiwum Filozofii Prawa i Filozofii Społecznej" 2011, nr 1, s. 5–14, http://archiwum.ivr.org.pl/1115/uzytecznosc-a-maksymalizacja-bogactwa-filozoficzne-zakorzenienie-pogladow-chicagowskiej-szkoly-law-economics/ [dostęp: 10 II 2021].

Smith D.C., *Paragons, Pariahs and Pirates: A Spectrum-Based Theory of Enterprise*, „Crime & Delinquency" 1980, nr 3, s. 358–386.

Szelewski M., Wieczorowski M., *Inżynieria odwrotna i metody dyskretyzacji obiektów fizycznych*, „Mechanik" 2015, nr 12, s. 183–188, http://www.mechanik.media.pl/pliki/do_pobrania/artykuly/22/40_183_188.pdf [dostęp: 15 IV 2020].

Tarapata Z., *Czy sieci rządzą światem? Od Eulera do Barabasiego*, „Biuletyn Instytutu Systemów Informatycznych" 2012, nr 10, s. 31–51, http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-article-BWA0-0055-0012 [dostęp: 15 IV 2020].

Wawrzynek Ł., *Analiza sieci społecznych w identyfikacji i wzmacnianiu potencjału innowacyjnego zespołów pracowniczych*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Research Papers of Wrocław University of Economics" 2017, nr 496, s. 183–204.

Wekerle T., Loures da Costa L.E.V., Trabasso L.G., *Design for Autonomy: An Integrated Product Development Tool for Reengineering of Complex Products for the Brazilian Space Sector*, w: *Transdisciplinary Engineering: Crossing Boudaries*, seria: Advances in Transdisciplinary Engineering, t. 4, 2016 r., e-book, s 632–641.

Woźniak A., *Grafy i sieci w technikach decyzyjnych*, „Infrastruktura i Ekologia Terenów Wiejskich" 2010, nr 4, s. 1–188, http://agro.icm.edu.pl/agro/element/bwmeta1.element.dl-catalog-0eeb75a5-4306-49e7-ab42-ce3dd480539a [dostęp: 16 IV 2020].

Źródła internetowe

Blaha M.R., *Reverse Engineering for Product Assessment*, informIT, 13 X 2001 r., https://www.informit.com/articles/article.aspx?p=23692&seqNum=6 [dostęp: 18 XII 2020].

Breeman K., *How does reverse engineering relate to forensics and solving crimes?*, https://www.quora.com/How-does-reverse-engineering-relate-to-forensics-and-solving-crimes [dostęp: 14 IV 2020].

Chen D., *Reverse-engineering the Org Chart*, https://talkingtalent.prosky.co/articles/reverse-engineering-the-org-chart [dostęp: 21 XII 2020].

Chikofsky E., Cross II J.H., *Encyclopedia of Software Engineering*, 2002, https://onlinelibrary.wiley.com/doi/abs/10.1002/0471028959.sof285 [dostęp: 15 IV 2020].

Heckmann T., *Reverse engineering secure systems using physical attacks*, 2018 r., https://www.researchgate.net/publication/330618085_Reverse_engineering_secure_systems_using_physical_attacks [dostęp: 19 XII 2020].

Hendricks B., *Reverse Engineering in Digital Forensics*, rozdział 4, lekcja 9, https://study.com/academy/lesson/reverse-engineering-in-digital-forensics.html [dostęp: 19 XII 2020].

Kapliński O., *Drzewa decyzyjne i użyteczność decyzji*, http://sipb.sggw.pl/Monografia_2015/Strony%20odRekomendowane_metody-11.pdf [dostęp: 11 II 2021].

Knicker M., *What Are The Types of Reverse Engineering and Why Does it Matter?*, https://www.qpluslabs.com/blog/what-are-the-types-of-reverse-engineering-and-why-does-it-matter/ [dostęp: 15 IV 2020].

Morzy M., Ławrynowicz A., *Wprowadzenie do analizy sieci społecznych*, Poznań 2010/2011, Instytut Informatyki Politechniki Poznańskiej, https://socnetwork.files.wordpress.com/2011/02/podstawowe-wc582ac59bciwoc59bci.pdf [dostęp: 16 IV 2020].

Ortmann G., *Deconstructing the Business of Terrorism. A Case Study of JNIM in Mali*, CERIS, http://www.ceris.be/fileadmin/library/Research-Papers-Online/Thesis-Deconstructing_the_business_of_terrorism.pdf [dostęp: 30 IV 2020].

Scoccimaro J., Rugaber S., *Reverse Engineering of Web Pages*, https://www.cc.gatech.edu/projects/PageSleuth/documents/icpc.pdf [dostęp: 30 IV 2020].

Waniek M., *Ukrywanie się w sieciach społecznych. Autoreferat*, https://depotuw.ceon.pl/bitstream/handle/item/2174/autoreferat-pl.pdf?sequence=3 [dostęp: 16 IV 2020].

Waniek M., Michalak T.P., Rahwan T., *Hiding in Multilayer Networks*, 2019, s. 1–24, https://arxiv.org/pdf/1911.05947.pdf [dostęp: 20 XII 2020].

Akty prawne

*Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych (*Dz. Urz. UE L 111 z 5 V 2009 r.), https://eur-lex.europa.eu/legal-content/pl/TXT/?uri=CELEX%3A32009L0024 [dostęp: 15 II 2021].

Decyzja nr 338 Komendanta Głównego Policji z dnia 12 października 2016 r. w sprawie Systemu Informacji Operacyjnych (Dz. Urz. KGP z 2016 r. poz. 65.).

Decyzja nr 126 Komendanta Głównego Policji z dnia 5 kwietnia 2013 r. w sprawie prowadzenia w Policji zestawu zbiorów danych „System Informacji Operacyjnych" (Dz. Urz. KGP z 2013 r. poz. 29, ze zm.).

The Digital Millennium Copyright Act of 1998, U.S. Copyright Office Summary, grudzień 1998 r., https://www.copyright.gov/legislation/dmca.pdf [dostęp: 15 II 2021].

Abstrakt

Inżynieria odwrotna może być wykorzystana do odtwarzania lub modyfikacji obiektów fizycznych oraz zastosowana do programów komputerowych. Nowym wyzwaniem jest jej wykorzystanie w celu zwiększenia skuteczności przeciwdziałania i zwalczania przestępczości kryminalnej i terrorystycznej (zwłaszcza przestępczości zorganizowanej). Odwrócenie procesów analitycznych przez analizę obiektową, analizę zarządzania, analizę logistyczno-finansową, a także wykorzystanie analizy kryminalistycznej i psychocybernetycznej daje możliwość udoskonalenia instrumentów walki z zorganizowaną formą popełniania przestępstw. Dzięki uzupełnieniu braków stwierdzonych w analizie i ponownej ocenie obiektu będzie można otrzymać ten sam obiekt, ale we „wzbogaconej" wersji, lub inny obiekt będący „doskonalszym" modelem analizowanego podmiotu. W konsekwencji będzie możliwe skuteczniejsze i efektywniejszej zneutralizowanie organizacji przestępczej działającej w formie zorganizowanej, w obszarze kryminalnym czy terrorystycznym.

Słowa kluczowe: inżynieria odwrotna, analiza kryminalna, analiza sieci społecznych.

The possibility of using reverse engineering to combat network – type criminal organisation

Abstract

Reverse engineering for the most part now refers to the restoration or modification of physical objects and computer programmes. A new challenge in the fight against crime is the use of reverse engineering to improve the measures of preventing and combating criminal and terrorist crime. Reversing processes through object-oriented analysis, as well as through management, logistics, financial, forensic and psycho-cybernetic analyses is a new outlook on improving the instruments to fight organized crime. As a result, by remedying the identified deficiencies and re-assessing the object, one will be able to get the same object but in the "enhanced" version or another object related to the analysed entity. Consequently, it will be possible to neutralize a criminal or terrorist organization more effectively and efficiently.

Keywords: reverse engineering, criminal analysis, analysis of social networks.