Krzysztof Borkowski*

Cyberbezpieczeństwo w kryminalistyce

Streszczenie

Powszechnie spotykanym zjawiskiem jest stosowanie zamiennie pojęć cyberprzestępczość i cyberbezpieczeństwo. Rozróżnienie zakresu przedmiotowego obu pojęć w przypadku kryminalistyki wskazuje jednoznacznie na ukierunkowanie realizowanych zadań z obszaru taktyki i techniki. W odniesieniu do cyberbezpieczeństwa funkcja zapobiegawcza kryminalistyki sprowadza się do tworzenia rozwiązań wzmacniających odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Zapewnienie takiej odporności należy postrzegać w kontekście działalności podmiotów realizujących zadania publiczne z wykorzystaniem współpracujących ze sobą urządzeń informatycznych i oprogramowania poprzez przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego.

Słowa kluczowe: cyberprzestępczość, cyberbezpieczeństwo, kryminalistyka, systemy baz danych, zapora sieciowa

* Dr Krzysztof Borkowski, Wydział Zarządzania i Logistyki, Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie.

Właściwe zrozumienie złożoności zagadnienia wymaga w pierwszej kolejności wprowadzenia w zadania i funkcje kryminalistyki. Jej zadania wynikają przede wszystkim z celów postępowania karnego. Procesowa zasada prawdy materialnej nakazuje dokonywanie wszystkich rozstrzygnięć na podstawie ustaleń faktycznych, zgodnych z rzeczywistością. Do ustaleń faktycznych są stosowane czynności procesowe lub pozaprocesowe, ponieważ organ procesowy ma obowiązek uczynić wszystko, żeby dotrzeć do prawdy materialnej o zdarzeniu, jego okolicznościach oraz osób z nim związanych. Niektórych ustaleń faktycznych dokonuje się z wykorzystaniem kryminalistycznych czynności operacyjnych rozciągających się poza sferę zainteresowania prawa karnego procesowego. Czynności te często poprzedzają wszczęcie procesu karnego lub są prowadzone jednocześnie z toczącym się postępowaniem karnym. Kryminalistyka obejmuje obszary taktyki i techniki występujące w trzech etapach związanych z przestępczością, a mianowicie: podczas popełniania przestępstw, zwalczania ich i im zapobiegania. Taktyka kryminalistyczna (gr. *taktika* – sposób) zajmuje się badaniem sposobów popełniania przestępstw oraz opracowywaniem sposobów postępowania organów ścigania i wymiaru sprawiedliwości mających najskuteczniej doprowadzić do ujawnienia przestępstwa i wykrycia sprawcy, a także sposobów zapobiegania przestępstwom.

Cyberprzestępczość *versus* cyberbezpieczeństwo

Na każdym wymienionym etapie kluczowym elementem jest informacja, która jest gromadzona i przetwarzana w bazach danych policji oraz innych służb dbających o bezpieczeństwo publiczne. W tym miejscu należy właściwie rozgraniczyć dwa, często w sposób niefortunny stosowane zamiennie pojęcia – „cyberprzestępczość" i „cyberbezpieczeństwo". Polskie prawodawstwo do dzisiaj nie stworzyło jednolitej definicji cyberprzestępczości. W nieobowiązującym już rządowym programie ochrony cyberprzestrzeni RP cyberprzestępstwo definiowano jako czyn zabroniony popełniony w cyberprzestrzeni. Pojęcie przestępczości komputerowej nie jest obecnie zdefiniowane nawet na gruncie ustawy – Kodeks karny.

Tym samym w celu przybliżenia pojęcia i zagadnienia cyberprzestępczości, w zakresie choćby źródłosłowu, należy posługiwać się literaturą przedmiotu oraz dorobkiem prawa międzynarodowego. Według Macieja Siwickiego „Etymologiczne pojęcie cyberprzestępczość (ang. *cybercrime*) stanowi połączenie dwóch określeń cyber i crime. O ile to drugie określenie odnosi się wyraźnie do

pojęć »przestępstwo, zbrodnia, występek«, znacznie trudniejsza jest interpretacja zwrotu cyber, który nie stanowi oddzielnego słowa, ale jedynie część wyodrębnioną z angielskiego słowa cybernetics (Cybernetyka). Podczas, gdy cybernetyka stanowi naukę o strukturze, systemach sterowania, kontrolowania i komunikacji m.in. w inżynierii, biologii i naukach społecznych, obecnie można zauważyć, że wyodrębnianemu członowi cyber nadaje się nowe znaczenie niewiele związane z nauką, z której się wywodzi"[1].

W dalszej kolejności na uwagę zasługuje kwestia określenia „cyberprzestępczość" w aktach normatywnych na szczeblu międzynarodowym. Komisja Wspólnot Europejskich, która w komunikacie Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 2007 roku pt. „W kierunku ogólnej strategii zwalczania cyberprzestępczości" pod tym określeniem rozumie „czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom"[2]. W skład cyberprzestępstw wchodzą trzy rodzaje zamachów: tradycyjne formy takie jak oszustwo czy fałszerstwo popełnione przy użyciu elektronicznych sieci informatycznych i systemów informatycznych; publikacja nielegalnych treści w mediach elektronicznych (np. materiałów związanych z seksualnym wykorzystywaniem dzieci czy nawoływaniem do nienawiści rasowej); przestępstwa typowe dla sieci łączności elektronicznej, np. ataki przeciwko systemom informatycznym i typu DoS (Denial of Service) oraz sabotaż informatyczny.

Należy zauważyć, że ważnym elementem charakteryzującym cyberprzestępczość nie jest przedmiot ochrony, np. bezpieczeństwo przetwarzanych elektroniczne danych, ale narzędzie przestępstwa. Wspólną cechą kategorii czynów zabronionych związanych z treścią informacji jest odwołanie się do określonego sposobu działania sprawcy polegającego na szeroko rozumianym rozpowszechnianiu lub prezentowaniu w sieciach komputerowych lub teleinformatycznych informacji zakazanych przez prawo. W skład tak rozumianych przestępstw, związanych z treścią informacji, wchodzą m.in. przestępstwa związane z różnego rodzaju intelektualnym oddziaływaniem na psychikę oraz emocje innych osób w celu np. wywołania podniecenia seksualnego, wrogości

1 M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 15.

2 Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów – W kierunku ogólnej strategii zwalczania cyberprzestępczości {SEK(2007) 641} {SEK(2007) 642}, https://eur-lex.europa.eu/legal-content'PL/PDF/?uri=CELEX:52007DC0267 [dostęp: 15.06.2023].

wobec określonej grupy osób, poniżenia lub przekonania ich do określonych poglądów lub postaw.

Przejście do pojęcia „cyberbezpieczeństwo" wymaga szerszego omówienia i przybliżenia oddziaływania. Optymalnym rozwiązaniem i jednocześnie punktem wyjścia do rozważań jest powołanie się na definicję zawartą w ustawie o krajowym systemie cyberbezpieczeństwa. Według rzeczonej ustawy cyberbezpieczeństwo to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[3]. Zgodnie z art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne system informacyjny należy rozumieć jako system teleinformatyczny stanowiący zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego[4].

Na podstawie delegacji ustawowej zawartej w art. 68 ustawy o krajowym systemie cyberbezpieczeństwa uchwałą nr 125 Rady Ministrów z 22 października 2019 roku przyjęto „Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024"[5].

Zgodnie z definicjami wprowadzonymi przez wyżej wymieniony dokument strategiczny cyberzagrożenie należy rozumieć jako wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów teleinformatycznych, użytkowników takich systemów oraz innych osób[6]. Cel główny przedmiotowej strategii został zdefiniowany jako podniesienie odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.

3 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2022, poz. 1863, art. 2, pkt 4.

4 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ibidem, poz. 1087.

5 *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, Warszawa 2019.

6 Zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz. Urz. UE 2019, L 151/15.

Podsumowując dotychczasowe rozważania, należy zwrócić uwagę, że najważniejszym elementem definicji cyberbezpieczeństwa jest stan odporności systemów informatycznych, dlatego poziom cyberbezpieczeństwa należałoby rozpatrywać pod kątem poziomu odporności systemów informatycznych na działania wyczerpujące dalsze elementy definicji ustawowej (bezpieczeństwo informacji). Warto na tym etapie zaakcentować, że w definicji cyberbezpieczeństwa brak jest elementów odnoszących się do przestępczości, a zatem brak jest elementów, które umożliwiałyby ocenę stanu cyberbezpieczeństwa z punktu widzenia istniejącej przestępczości, w tym przestępczości o charakterze mogącym mieć potencjalny wpływ na obszar cyberbezpieczeństwa. Dlatego kluczowym elementem do oceny stanu rozumianego jako cyberbezpieczeństwo jest stan oczekiwanej odporności systemów na wszelkie działania, nie tylko o charakterze przestępczym, naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Warto zwrócić uwagę, że jednym z pięciu celów szczegółowych wyznaczonych przez wspomnianą wyżej „Strategię Cyberbezpieczeństwa Rzeczypospolitej na lata 2019–2024" są zadania ukierunkowane na podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty, czyli zdarzenia zdefiniowane jako mogące mieć niekorzystny wpływ na cyberbezpieczeństwo[7].

Istotne, w nawiązaniu do zadań stawianych przed kryminalistyką, jest to, że zarówno cel główny, jak i poszczególne cele szczegółowe opisane w „Strategii Cyberbezpieczeństwa Rzeczypospolitej na lata 2019–2024" nie odnoszą się wprost do cyberprzestępczości. Zwiększenie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym, opisano jedynie jako jedno z wielu zadań realizowanych w ramach programu „Rozwój krajowego systemu cyberbezpieczeństwa". Niemniej jednak warto zwrócić uwagę na zakres działania, nakreślony w aspekcie techniki kryminalistycznej. Technika kryminalistyczna (gr. *technikos* – kunsztowny) obejmuje badanie środków technicznych wykorzystywanych do popełniania przestępstw oraz opracowywanie środków stosowanych przez organy ścigania i wymiaru sprawiedliwości w toku dochodzenia przestępstw, a także środków pomocnych w zapobieganiu przestępczości. W odniesieniu do przedmiotowej strategii niezmiernie istotne są zapisy wskazujące, że „W zakresie

7 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa..., art. 2, pkt 4.

zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze hybrydowym (w tym działań o charakterze terrorystycznym) ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. W tym celu wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw, a szczególnie istotne znaczenie ma prawidłowe zabezpieczenie dowodów cyfrowych"[8].

Zarys powyższej analizy wskazuje jednoznacznie, że podstawowym i dominującym elementem cyberbezpieczeństwa ukształtowanego przez polski system prawny jest stan odporności systemów informacyjnych na określone działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Odporności rozumianej jako zdolność do szybkiego dostosowywania się i odzyskiwania zdolności do działania po znanych lub nieznanych zmianach środowiska poprzez całościowe wdrożenie zarządzania ryzykiem, planowania awaryjnego i ciągłości działania. Przytoczone definicje jednoznacznie wskazują na najważniejsze elementy stanu rozumianego jako cyberbezpieczeństwo. Podstawowym elementem określającym ten stan jest niewątpliwie odporność systemów informacyjnych, odporność osiągana poprzez wiele skomplikowanych procesorów wzajemnie powiązanych ze sobą, w ramach których możemy przykładowo wskazać takie obszary, jak: zarządzenie ryzykiem, planowanie awaryjne, planowanie i wdrożenie mechanizmów ciągłości działania, ale także obszary związane z budowaniem świadomości i kompetencji społecznych w sferze cyberbezpieczeństwa. Podstawowym celem zapewnienia oczekiwanego stanu odporności systemów informacyjnych jest zapewnienie bezpieczeństwa przetwarzanych w tych systemach danych lub oferowanych przez te systemy usług.

Należy także podkreślić, że zgodnie z narodowymi standardami cyberbezpieczeństwa (NSC), zaimplementowanymi z National Institute of Standards and Technology (NIST), odporność należy rozpatrywać także w kontekście odzyskania zdolności działania po znanych lub nieznanych zmianach środowiska, zatem katalog potencjalnych działań wpływających na stan odporności systemów informacyjnych jest bardzo duży i otwarty. Powinien on być rozumiany jako wszelkie zmiany w środowisku chronionej infrastruktury

8 *Strategia Cyberbezpieczeństwa Rzeczpospolitej*..., s. 17.

teleinformatycznej, dlatego nie może być zawężany jedynie do zmian będących wynikiem działań człowieka wywołujących zdarzenia o cechach (znamionach) przestępstwa.

Przestępstwo to czyn człowieka zabroniony przez ustawę pod groźbą kary jako zbrodnia lub występek, bezprawny, zawiniony i społecznie szkodliwy w stopniu większym niż znikomym[9]. Zbiór zdarzeń określanych jako przestępstwa to już zjawisko społeczne o ustalonej dynamice oraz strukturze, a występujące na określonym terytorium w określonych czasie, wypełnia definicję przestępczości w ujęciu kryminologicznym. Zwalczanie przestępczości ogólnie można określić jako ustrukturyzowany proces, na który składa się wiele działań mających na celu ograniczanie i eliminację przestępczości. Należy zauważyć, że w obszernym katalogu zdarzeń skutkujących zmianą w chronionym środowisku teleinformatycznym, czyli oddziałujących na stan odporności tych systemów, będzie znajdować się również grupa zdarzeń związanych z działaniem człowieka, podlegająca ocenie pod kątem znamion czynów zabronionych, zatem mogących stanowić przestępstwa.

Reasumując, oczywiście można wyodrębnić zbiory, elementy zdarzeń, czynności, procesów, w których występuje korelacja pomiędzy cyberbezpieczeństwem w obszarze infrastruktury teleinformatycznej administracji publicznej a procesem rozumianym jako zwalczanie cyberprzestępczości. Wydaje się, że elementem wzajemnych korelacji i współpracy są, i będą, zdarzenia odziaływujące na odporność systemów informacyjnych, będące jednocześnie wynikiem działania człowieka, działania wyczerpującego znamiona czynu zabronionego. Jednakże zdarzenia te będą stanowiły jedynie wycinek, podzbiór z całości zdarzeń i czynników skutkujących zmianami w środowisku chronionej infrastruktury teleinformatycznej, odziaływujących na odporność systemów informacyjnych, niebędących efektem działalności przestępczej. Ponadto wydaje się, że zwalczanie tego typu cyberprzestępczości nie może oddziaływać bezpośrednio na poziom oczekiwanej odporności systemów informacyjnych, a zatem na zagrożenia bezpieczeństwa danych. Należy podkreślić, że to właśnie na podstawie stanu odporności tychże systemów na zagrożenia, rozumianego również jako zdolność do odparcia danego zagrożenia, powinno się oceniać stan cyberbezpieczeństwa, nie zaś na podstawie liczby i charakteru zdarzeń występujących w obszarze chronionej infrastruktury teleinformatycznej. Ponadto przez odporność należy rozumieć nie tylko

9 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U 1997, nr 88, poz. 553.

zdolność od odparcia zagrożenia, lecz także zdolność, jak już wcześniej wspomniano, do odtworzenia, przywrócenia stanu pierwotnego po wystąpieniu zdarzenia określonej kategorii.

Dążąc do ostatecznego podkreślenia odrębności obszaru cyberbezpieczeństwa od cyberprzestępczości, warto przytoczyć także definicję z rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z 17 kwietnia 2019 roku w sprawie ENISA. Według rzeczonego dokumentu cyberbezpieczeństwo oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami. Wobec tego cyberbezpieczeństwo należy rozumieć nie jako stan społecznego poczucia bezpieczeństwa, lecz postrzegać jako sprecyzowane działania ukierunkowane na ochronę infrastruktury teleinformatycznej bądź jako stan infrastruktury sieci i systemów informatycznych określany mianem odporności.

Uzupełnienie powyższego uzasadnienia znajdziemy w słowniku ważniejszych pojęć z dziedziny cyberbezpieczeństwa, opracowanym na podstawie narodowych standardów cyberbezpieczeństwa (National Standards Cybersecurity – NSC). Warto przytoczyć takie definicje, jak:

– „cyberincydent – określony jako działania podejmowane przez użytkownika sieci komputerowej, których rezultatem jest rzeczywisty lub potencjalny niekorzystny wpływ na system informatyczny lub na informacje przetwarzane w tym systemie”[10];

– „incydent – zdarzenie, które faktycznie lub potencjalnie zagraża poufności, integralności lub dostępności systemu informatycznego lub informacji, które system przetwarza, przechowuje lub przesyła, a także zdarzenie, które stanowi naruszenie lub bezpośrednie zagrożenie naruszenia zasad bezpieczeństwa, procedur bezpieczeństwa lub zasad dopuszczalnego użytkowania”[11];

– „źródło zagrożenia – intencja i metoda ukierunkowane na celowe wykorzystanie podatności w zabezpieczeniach lub sytuacje i metody, które mogą przypadkowo wykorzystać podatność”[12];

– „zdarzenie – każda dająca się zaobserwować zmiana w systemie”[13].

10 *Słownik kluczowych pojęć z zakresu cyberbezpieczeństwa*, NSC 7298, wer. 1.0, Warszawa 2021, s. 119.
11 Ibidem, s. 85.
12 Ibidem, s. 245.
13 Ibidem, s. 98.

Jednocześnie należy zauważyć, że w przywoływanym słowniku brakuje definicji cyberprzestępstwa, cyberprzestępczości, a także innych definicji ogólnych odnoszących się do przestępczości, co wydaje się, że podkreśla całkowitą odrębność zagadnień.

Powyższa analiza jednoznacznie wskazuje, że tych dwóch pojęć, tj. „cyberbezpieczeństwo" i „cyberprzestępczość" nie można utożsamiać, dlatego że definiują one zupełnie inne obszary. Cyberbezpieczeństwem można określić stan o zdefiniowanych ustawowo parametrach opisanych jako odporność systemów informacyjnych na zagrożenia bezpieczeństwa przetwarzanych w nich danych. Cyberprzestępczość należy rozumieć jako zjawisko społeczne polegające na występowaniu przestępczości w danym czasie, i w tym przypadku, w danej infrastrukturze, której wspólną cechą nie jest przedmiot ochrony (np. bezpieczeństwo danych), a narzędzie służące do jej popełniania – system informatyczny, system teleinformatyczny, sieć teleinformatyczna. Jedną z kategorii tych przestępstw będą te, których przedmiotem działania sprawców będzie bezpieczeństwo danych przetwarzanych w systemach informacyjnych, a podmiotem przestępstwa – administracja publiczna w zakresie utrzymywanych systemów.

Wydaje się, że zwalczanie cyberprzestępczości w aspekcie cyberbezpieczeństwa można rozpatrywać jedynie jako wpływ tego działania na zjawisko występowania przestępstw godzących w bezpieczeństwo danych przetwarzanych w chronionych systemach informacyjnych. Jednakże niezależnie od skuteczności tego działania oraz niezależnie od przestępczości, której przedmiotem zamachu jest bezpieczeństwo danych przetwarzanych w systemach informacyjnych, fundamentalnym elementem cyberbezpieczeństwa pozostaje odporność rozumiana jako zdolność do odpierania zagrożenia bezpieczeństwa danych, w tym przeciwdziałania zagrożeniom będących m.in. skutkiem działania o charakterze przestępczym. Należy zauważyć, że nawet ograniczenie pewnej wybranej grupy zdarzeń oddziałujących na bezpieczeństwo danych przetwarzanych w systemach informacyjnych, będące np. skutkiem skutecznego zwalczania cyberprzestępczości, nie może skutkować obniżeniem akceptowalnego poziomu odporności tych systemów na występujące lub mogące wystąpić zagrożenia, odporności rozumianej także w kontekście odtworzenia stanu sprzed zdarzenia, a zagrożenia rozumiane w szerokim kontekście zmian w chronionym środowisku teleinformatycznym nie tylko związane z umyślnym działaniem człowieka – wyczerpujących znamiona czynów zabronionych.

Cyberbezpieczeństwo w taktyce i technice kryminalistycznej

Bezpieczeństwo informacji w obszarze kryminalistyki obejmuje różnorodne działania ukierunkowane zarówno na ochronę infrastruktury teleinformatycznej, jak i systemów informatycznych. Sama tylko realizacja jej funkcji wykrywczej polega na ukierunkowaniu taktyki (kryminalistycznej) bezpośrednio na osobę i w związku z tym na zdobywanie i wykorzystanie głównie osobowych źródeł informacji (OZI). Takie działania wymagały stworzenia struktury na poziomie centralnym w postaci Ogólnopolskiej Bazy Osobowych Źródeł Informacji (OBOZI). Zgodnie z wytycznymi zawartymi w deklaracji berlińskiej (1994) oraz z konferencji w Tampere (1999) stanowi ona jeden z elementów narzędzia wspomagającego pracę Policji w ramach wywiadu i analizy kryminalnej[14].

Funkcjonowanie wywiadu kryminalnego opiera się na trzech filarach: analizie kryminalnej, werbunku oraz wsparciu informatycznym, tworzących System Meldunku Informacyjnego (SMI). Architektura utworzonego systemu informacyjnego ma bardziej złożoną strukturę, ponieważ stanowi on jeden z elementów większego tworu – System Informacji Operacyjnych (SIO). Działania z taktyki kryminalistycznej wykorzystują wiele innych systemów informacyjnych funkcjonujących w ramach realizowanych ustawowych zadań policji. Zarówno Krajowy System Informacji Policyjnej (KSIP), jak i Krajowe Centrum Informacji Kryminalnych, System Automatycznej Identyfikacji Daktyloskopijnej (Automatated Fingerprint Identification System – AFIS) oraz baza profili genetycznych (GENOM) działają w chronionej zamkniętej sieci teleinformatycznej, do której dostęp jest kodowany, nałożone są hasła oraz funkcjonuje weryfikacja poziomu dostępu.

W walce z przestępczością kryminalistyce przypada także doniosłe zadanie opracowywania i adaptacji środków technicznych do ujawniania, zabezpieczania, a następnie wykorzystania rzeczowych źródeł informacyjnych, czyli badania dowodów rzeczowych. Najważniejszym zadaniem kryminalistyki jest identyfikacja na podstawie śladów, przy czym ślady te mogą mieć bardzo różną naturę – od powszechnie znanych śladów linii papilarnych, przez ślady narzędziowe, po ślady biologiczne (genetyka) – osób, zwierząt lub rzeczy, od której ślad pochodzi. W tym obszarze również powstają rozwiązania, które funkcjonują na bazie

14 W. Ignaczak, *Wybrane zagadnienia analizy kryminalnej*, Szczytno 2005, s. 8.

systemów informacyjnych. Dobrym przykładem będzie tutaj system kryminalistycznego wsparcia w identyfikacji pojazdów (Forensic Aid for Vehicle Identyfication – FAVI), który jako pierwszy polski system zostanie udostępniony online na platformie ekspertów Europolu (Europol Platform for Experts – EPE). Po blisko 5 latach od wystąpienia z tą inicjatywą[15] oraz rozpoczęcia prac nad wdrożeniem rozwiązań gwarantujących bezpieczeństwo danych i odporność systemu na zagrożenia mogące być m.in. skutkiem działań o charakterze przestępczym, zaistniała możliwość uruchomienia dostępu do chronionego systemu informacyjnego za pośrednictwem internetu. Najważniejsze dla tego rozwiązania i jemu podobnych jest wprowadzenie zabezpieczenia poprzez wieloetapową autoryzację użytkownika (np. eksperta Europolu). W obecnych czasach silne hasło nie stanowi gwarancji bezpiecznego korzystania z takich systemów. Niezbędne staje się włączenie dodatkowej weryfikacji, tzw. uwierzytelniania dwuskładnikowego (Two Factor Authenticaton – 2FA). Dodatkowa weryfikacja pomoże chronić skutecznie nie tylko konta użytkownika, lecz także hasła do nich. Zastosowanie uwierzytelnienia dwuskładnikowego daje do wyboru kilka możliwości. To przede wszystkim jednorazowe kody generowane w aplikacji lub wysyłane SMS-em, ale też klucz sprzętowy w postaci małego urządzenia generującego kody (token), które pozwalają potwierdzić, że to właśnie my próbujemy zalogować się do komputera, serwisu czy aplikacji. Drugim składnikiem może być zabezpieczenie biometryczne w postaci odcisku palca, skanu twarzy czy obrazu tęczówki. Po skonfigurowaniu 2FA podczas logowania – za każdym razem – oprócz hasła będzie wprowadzany także np. specjalny kod. Ten dodatkowy składnik jest znany tylko użytkownikowi, więc jeśli nawet hasło wycieknie lub zostanie utracone w inny sposób, to cyberprzestępca nie włamie się na konto podlegające ochronie.

Sformułowane wcześniej odniesienie do podobnych rozwiązań nabiera szczególnego znaczenia w przypadku kontrowersyjnego w ostatnim czasie narzędzia dostarczonego przez firmę Clearview AI. Rozwiązanie to służy do rozpoznawania ludzkich twarzy, korzystając z bazy danych zawierającej ponad 30 mld obrazów[16]. Zebrane zdjęcia wielu ludzi z całego świata pochodzą z ogólnodostępnych źródeł internetowych, w tym takich serwisów

15 Spotkanie szefów jednostek krajowych Europolu (Heads of Europol National Units – HENU) w Hadze 13–14 listopada 2018 r.

16 B. Francuz, *Wykorzystują twoje zdjęcia z Facebooka i nic im nie zrobisz. Clearview AI już się z tym nawet nie kryje*, https://android.com.pl/tech/583507-clearview-ai-baza-30-miliardow-zdjec/ [dostęp: 10.04.2023].

społecznościowych, jak: Facebook, Twitter i Google. Pomimo wywołującego kontrowersje sposobu pozyskiwania zdjęć, zarówno bez zgody serwisów, jak i użytkowników, zastosowana technologia z powodzeniem była już używana przez służby policyjne, m.in. amerykańskie i kanadyjskie organy ścigania. Kwestią nadrzędną rozważań oprócz kryminalistycznych walorów tego narzędzia, czyli identyfikacji osób oraz skutecznego monitorowania ich zachowania jest odporność tego systemu na możliwe warianty zainfekowania w wyniku pobierania plików z globalnie działającej sieci.

Z czysto ekonomicznego podejścia do zapewnienia bezpieczeństwa przetwarzanych w tych systemach danych „produkcja" przeznaczonych do tego zabezpieczeń jest zbyt droga. Naturalnym i skutecznym rozwiązaniem na dziś jest implementacja zabezpieczeń funkcjonujących w sieci, np. Web Application Firewall (WAF). Ten system ochrony aplikacji webowych, tj. stron internetowych, pozwala dzięki prostemu modelowi działania na automatyczną kontrolę treści wchodzących do aplikacji (bez ingerencji użytkownika). Zabezpieczenia w systemie ochrony WAF bazują na czarnej i białej liście aplikacji:

– czarna lista (blacklist) pozwala na tworzenie listy/indeksu elementów, które mają być przez serwer identyfikowane jako niebezpieczne, tj. takie, które podlegają blokadzie, a następnie zmienione lub po prostu odnotowane w logach serwera jako próba wykonania działań zastrzeżonych;

– biała lista (whitelist) pozwala z kolei na utworzenie akceptowanych przez serwer, które zostaną udostępnione np. na stronie WWW.

Czarna i biała lista oraz następstwa ich działania są kontrolowane przez administratora, który tworzy konfiguracje WAF na podstawie charakterystyki ruchu generowanego przez aplikacje i zachowań użytkowników. Technologia ta buduje model zachowań, a jednocześnie zapewnia stałą aktualizację już wdrożonych mechanizmów zabezpieczeń. WAF skupia swoje działania na ochronie stron WWW, czyli najczęstszych celów hakerów, którzy poprzez ingerencję w witryny, bazy danych i zawartość aplikacji dokonują kradzieży danych lub innych oszustw.

Ogromnym wyzwaniem dla współczesnej kryminalistyki jest postęp technologiczny i rosnąca dywersyfikacja infrastruktury IT, gdyż wymuszają one opracowywanie i wdrażanie nowych dodatkowych procedur cyberbezpieczeństwa. Dzięki zastosowaniu tanich technologii obliczeniowych, chmury, big data, analityki i technologii mobilnych fizyczne przedmioty mogą udostępniać i zbierać dane przy minimalnej interwencji człowieka. Ponadto nowa rzeczywistość pracy hybrydowej i zdalnej potęguje zagrożenia ze strony cyberprzestępców. W ciągu ostatnich kilku lat jedną z najważniejszych technologii XXI wieku

stał się internet rzeczy (Internet of Things – IoT), czyli oznacza sieć obiektów fizycznych – „rzeczy", które są wyposażone w czujniki, oprogramowanie i inne technologie w celu łączenia się i wymiany danych z innymi urządzeniami i systemami za pośrednictwem internetu. Urządzenia te obejmują zarówno zwykłe przedmioty gospodarstwa domowego, jak i zaawansowane narzędzia przemysłowe. W tym niezwykle skomunikowanym świecie systemy cyfrowe mogą rejestrować, monitorować i dostosowywać każdą interakcję między połączonymi rzeczami. Według szacunków ekspertów do roku 2025 liczba urządzeń, które umożliwiają bezproblemową komunikację między ludźmi, procesami i przedmiotami, wzrośnie do 22 mld. Niewątpliwie ta technologia (IoT) staje się wyznacznikiem zmian, które przy stałym rozwoju systemów łączności, zwiększonym dostępie do platform obliczeniowych w chmurze oraz ciągłym postępom w uczeniu maszynowym i analityce przesuną do przodu granice czerpania korzyści z niej i z technologii pokrewnych.

Oprócz spodziewanych korzyści w szybkim tempie zaczyna się krystalizować wizja podatności na cyberatak w miejscu, gdzie świat fizyczny spotyka się ze światem cyfrowym i współpracują ze sobą. Wszystko to, czym sterujemy bezpośrednio z wykorzystaniem smartfona, a więc zarówno smart TV, sprzęt audio czy domowe kamery, jak i ekspresy do kawy, odkurzacze i pralki może być tą samą drogą zainfekowane złośliwym oprogramowaniem. Ujmując sprawę w aspekcie kryminalistycznym, czyli wykrywania, zwalczania i zapobiegania przestępczości, włamanie przez pralkę lub uzyskanie dostępu do lodówki dla cyberprzestępcy nie będzie pozbawione sensu. Urządzenia pracujące w jednej sieci łączą się ze sobą. Cyberprzestępca będzie poszukiwał najsłabszego ogniwa, np. niezabezpieczonej kuchenki, i tą drogą może wykraść wrażliwe dane ze służbowego laptopa, na którym pracujemy w domu. Oczywiście, są już dostępne pakiety bezpieczeństwa sieciowego, które umożliwiają identyfikację wszystkich urządzeń w sieci domowej i pozwalają na ich ochronę.

Obecnie trudno jest jednoznacznie wskazać, gdzie technologia IoT jest narażona w większym stopniu na cyberzagrożenia, czy w sieci urządzeń domowych czy w sieci urządzeń przemysłowych. Biorąc przykładowo pod uwagę branżę motoryzacyjną, wydaje się mimo wszystko, że jednak dotyczy to bardziej drugiego z wymienionych przypadków. Oprócz korzyści z zastosowania IoT w liniach produkcyjnych czujniki mogą wykrywać potencjalne awarie urządzeń w pojazdach już poruszających się po drogach i ostrzegać kierowcę przez przekazywanie mu szczegółowych informacji i zaleceń. Dzięki zbiorczym informacjom zebranym przez aplikacje z wykorzystaniem IoT producenci i dostawcy z branży motoryzacyjnej mogą dowiedzieć się więcej o tym jak

utrzymać samochody w ruchu oraz odpowiednio informować ich właścicieli. IoT stanowi rewolucję w motoryzacji, umożliwia tworzenie skomunikowanych samochodów. Dzięki IoT właściciele samochodów mogą obsługiwać je zdalnie, np. wezwać samochód przez telefon. Dzięki możliwościom IoT w dziedzinie komunikacji między urządzeniami samochody będą nawet mogły, w uzasadnionych przypadkach, same umawiać się na wizyty serwisowe. Skomunikowany samochód umożliwia producentom ciągłe ich unowocześnianie za pomocą nowego oprogramowania, co stanowi podstawową różnicę między nim a tradycyjnym modelem samochodu, który po wyjeździe z fabryki traci na wydajności i wartości.

Należy zwrócić uwagę, że cały pakiet wymienionych korzyści z IoT dla branży motoryzacyjnej to tylko fragment skali potencjalnych źródeł wycieku danych wrażliwych. Istota zagadnienia dotyczy przestępczości samochodowej, gdzie do wymienionych różnorodnych danych o pojeździe dodać należy choćby dane identyfikacyjne pojazdów, które są zapisane w ich podzespołach. Naruszenie integralności takiego systemu może skutkować niewyobrażalnymi stratami materialnymi i co najistotniejsze, niekontrolowanym wzrostem nie tylko przywołanej wyżej przestępczości samochodowej, lecz także przestępczości w pełnym tego słowa znaczeniu. Jak zostało wcześniej wspomniane, obecnie gwarancji cyberbezpieczeństwa dla tych danych, tj. odporności systemu na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych, należy upatrywać w implementacji opracowanych już rozwiązań dla sieci teleinformatycznych w postaci systemów wykrywania i zapobiegania włamaniom, np. Intrusion Detection System (IDS) i Intrusion Prevention System (IPS). Samo wdrożenie systemu NIDS/NIPS wymaga ciągłego dostosowywania go do zmieniających się zagrożeń i charakteru ruchu sieciowego.

Zakończenie

Jeżeli chodzi o podjętą tematykę, to niebezpodstawnie wprowadzono rozgraniczenie pojęć „cyberbezpieczeństwo" i „cyberprzestępczość", a także zaakcentowano podział zadań z obszaru taktyki i techniki kryminalistycznej. Cyberprzestępczość z definicji obejmuje czyny przestępcze dokonane z użyciem sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takim sieciom i systemom. W aspekcie przedmiotowych rozważań to ten trzeci rodzaj z wymienionych obejmuje przestępstwa typowe dla sieci

łączności elektronicznej, tj.: ataki przeciwko systemom informatycznym, ataki typu DoS oraz sabotaż informatyczny. W rozumieniu cyberbezpieczeństwa ważny jest stan odporności systemów informatycznych jako zdolność do odpierania zagrożeń (przeciwdziałania zagrożeniom) bezpieczeństwa danych, w tym zagrożeniom, które są m.in. skutkiem działania o charakterze przestępczym. Nie stoi to bynajmniej w sprzeczności z zapisami „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024", w której wskazuje się jeden z jej celów jako „[...] zwiększania zdolności do zwalczania cyberprzestępczości", dla której „[….] szczególnie istotne znaczenie ma prawidłowe zabezpieczenie dowodów cyfrowych"[17].

Należy mieć świadomość, że poziom cyberprzestępczości ciągle rośnie i na pierwszą połowę roku 2023 szacuje się, że 30% przestępstw jest popełnianych z użyciem komputera lub telefonu. Tym samym rolą techniki kryminalistycznej jest opracowanie rozwiązań umożliwiających przechwycenie tzw. śladów ulotnych, czyli zdeszyfrowanych informacji, które pozwalają odtworzyć wszystkie działania komputera. W obszarze techniki kryminalistycznej pojawiają się również rozwiązania pozwalające na usprawnienie obiegu informacji, a przy okazji na zredukowanie „pracy przy biurku". Do takich należy opracowany system umożliwiający rejestrację, automatyczne etykietowanie, a także wymianę informacji na temat dowodów, począwszy od pierwszego kontaktu z ofiarami, świadkami i przestępcami po finalną digitalizację dowodów i szybki dostęp w chmurze. Każdy z przywołanych systemów, które pozwalają na realizację zadań zarówno z techniki kryminalistycznej, jak i taktyki kryminalistycznej, stanowi strategiczny obszar cyberbezpieczeństwa pozostający w wyłącznych merytorycznych kompetencjach komórek organizacyjnych Komendy Głównej Policji i komend policji (kraj) odpowiedzialnych za bezpieczeństwo danych przetwarzanych w utrzymywanej infrastrukturze teleinformatycznej tej formacji.

Znacznym wyzwaniem zarówno dla tych systemów, jak i dla działań z zakresu taktyki kryminalistycznej jest zapewnienie zdolności do odpierania zagrożeń bezpieczeństwa danych, zwłaszcza wówczas, gdy działania te są związane z korzystaniem z otwartych źródeł informacji, z OSINT (Open Source Inteligence) podczas chociażby prowadzenia białego wywiadu. Poruszając aspekt bezpieczeństwa w przestrzeni „cyber", powinno się mieć świadomość, że negatywny wpływ na bezpieczeństwo leży po stronie człowieka, choćby poprzez zlecenia wykonania zabezpieczeń w ramach podwykonawstwa. Warto

17 *Strategia Cyberbezpieczeństwa Rzeczypospolitej*..., s. 17.

również zwrócić uwagę na bezpieczeństwo ogólne w kontekście aplikacji IoT wykorzystywanych także w galanterii elektronicznej, gdzie pozwalają monitorować nie tylko warunki środowiskowe, ale i zdrowie ludzi. Aplikacje tego typu, mimo że pomagają ludziom lepiej zrozumieć stan ich zdrowia, a lekarzom umożliwiają zdalne monitorowanie pacjentów, utwierdzają tylko w przekonaniu, że cyberbezpieczeństwo dla kryminalistyki stanowi otwarty rozdział.

Bibliografia

Gańko K., Kania D., Troszczyńska-Roszczyk E., *Poradnik ABC cyberbezpieczeństwa*, Warszawa 2022.
Hanausek T., *Kryminalistyka. Zarys wykładu*, Kraków 2009.
Ignaczak W., *Wybrane zagadnienia analizy kryminalnej*, Szczytno 2005.
Kryminalistyka a nowoczesne technologie, red. V. Kwiatkowska-Wójcikiewicz, D. Wilk, J. Wójcikiewicz, Kraków 2019.
Siwicki M., *Cyberprzestępczość*, Warszawa 2013.
Słownik kluczowych pojęć z zakresu cyberbezpiczeństwa, NSC 7298, wer. 1.0, Warszawa 2021.
Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, Warszawa 2019.
Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy, red. B. Hołyst, Warszawa 2014.
Vademecum bezpieczeństwa informacyjnego, t. 1, red. O. Wasiuta, R. Klepka, Kraków 2019.
Wrzesień M., Olejnik Ł., Ryszawa P., *IDS/IPS: systemy wykrywania i zapobiegania włamaniom do sieci komputerowych*, „Pomiary. Automatyka. Robotyka" 2013, nr 2.
Współczesny wymiar bezpieczeństwa publicznego. Kształtowanie bezpiecznych przestrzeni. Działania profilaktyczne, red. T. Kośmider, L. Kołtun, Warszawa 2019.
Zubańska M., *Nowe technologie w kryminalistyce. Aspekty prawne i kryminalistyczne*, Olsztyn 2019.

Cybersecurity for forensics

Abstract

It is common to use terms like cybercrime and cybersecurity interchangeably. The distinction between the subject scope of both terms in the case of forensic science clearly indicates the direction of the tasks carried out in the areas of tactics and technology. In contrast to cybersecurity, the preventive function of forensic science is to create solutions that strengthen the resistance of information systems to actions that violate the confidentiality, integrity, accessibility, and authenticity of processed data or related services offered by these systems. Ensuring such resilience should be perceived in the context of the activities of entities performing public tasks with the use of cooperating IT devices and software by processing, storing, sending, and receiving data via telecommunications networks using a terminal device appropriate for a given type of telecommunications network.

Key words: cybercrime, cybersecurity, forensics, database systems, firewall