GRZEGORZ WOŹNY

Modus operandi sprawców przestępstw komputerowych

Wstęp

Komputery i nowe technologie zostały stworzone przez ludzi by ułatwiać społeczeństwom wszystkie aspekty życia. Tworząc te wynalazki, autorzy mieli na celu zbudowanie narzędzi oraz urządzeń, które będą poprawiać naszą pracę, maksymalizować jej wydajność oraz skuteczność, jak również eliminować ludzkie błędy. Biorąc pod uwagę dynamikę rozwoju technologii IT, środki w nie inwestowane oraz coraz większe uzależnianie pracy od technologii informacyjnych, należy mieć na uwadze, że wszystkie efekty jakichkolwiek wykonywanych przez ludzi czynności, są przetwarzane przez komputery. Tutaj zaczyna się pole do popisu dla ludzi zwanych „hackerami", którzy wykorzystują aktualny stan nowych technologii, znajdują poprzez określone metody, schematy, algorytmy słabe punkty i wykorzystują je w praktycznie nieograniczonych celach głównie dla osiągnięcia określonych korzyści bądź uzyskania planowanego zachowania. W przypadku przestępców komputerowych ich aprecjacja jest ściśle związana z technologiami stosowanymi obecnie oraz wdrażanymi w przyszłości.

Hacker, który się nie rozwija staje się bezużyteczny a wręcz szkodliwy z tego względu, iż potencjalne błędy mogą narazić jego i współsprawców na ujawnienie przez organy ścigania. Inną kwestią jest to, że technologia stosowana kilka lat temu została wyparta przez taką, która wymaga innego sposobu działania. W ten sposób źródła naukowe i specyfikacje produktów, które są wykorzystywane do przeciwdziałania skutkom działania cyberprzestępców dezaktualizują się. Największym problemem jest sytuacja

gdzie na ochronę infrastruktury danych obowiązkowe jest poznanie słabych punktów, celem spełnienia określonych standardów istniejących w branży informatycznej oraz dostosowania do wciąż zmieniających się przepisów prawa materialnego. Sytuacja ta wymaga czasu i nakładu pieniędzy, a gdy problem i zabezpieczenia okazują się na tyle wystarczające pojawia się nowa technologia i prawo, do której trzeba dostosowywać swoje produkty. Nie można jednak zapominać o znaczącym wkładzie w rozwój i maksymalizację zysków. Technologie informacyjne, co kilka lat zmieniają swój kształt, jednak nie na tyle by odchodzić od rozwiązań powszechnie stosowanych przez producentów deweloperów i twórców. Działa to na zasadzie ewolucji i udoskonalania rozwiązań, powiększania zasięgu odbiorców i miniaturyzacji.

Istotą działania Hackingu według Jona Ericksona jest „znajdowanie nieprzewidzianych lub przeoczonych możliwości działania określonych praw lub właściwości w danej sytuacji, a następnie wykorzystanie ich w nowy, odkrywczy sposób w celu rozwiązania postawionego problemu. Problemem tym może być brak dostępu do systemu komputerowego”[1]. „Zazwyczaj tego rodzaju działania prowadzą do przezwyciężenia trudności w unikatowy sposób, niewyobrażalny dla tych, którzy są przywiązani do stereotypowych metod postępowania”[2]. Hackerzy poświęcają każdą chwilę na eksplorowanie zagadnień i wyszukiwanie ich słabych punktów Tutaj należy wyjaśnić, czym jest (w sensie ogólnym) wyżej wspomniane *modus operandi*, i dlaczego jest tak istotne z punktu widzenia szeroko rozumianych przestępstw komputerowych, których problem jest przez wielu śledczych uważany za niezwykle złożony i należący do czołówki przestępstw o najniższych statystykach wykrycia sprawców jak i odzyskania utraconych dóbr. Komputery w XXI w. odgrywają główną rolę w sterowaniu wszystkimi strukturami, gałęziami gospodarki i bezpieczeństwa państwa.

[1] J. Erickson, *Hacking. Sztuka penetracji*, Gliwice 2004, s. 9.
[2] *Ibidem*.

Ze względu na określone wzory i stan obecnej wiedzy dzisiaj praktycznie niemożliwym jest uniknięcie działań hackerów, którzy wypełniają znamiona przestępstw komputerowych oraz przestępstw towarzyszących przestępstwom komputerowym. Wynika to z faktu rozległości i stopnia skomplikowania szeroko rozumianej dziedziny Informatyki i komputerów. Z tego powodu wykorzystując komputer, smartfon, tablet a nawet zegarek można z pomocą wiedzy i technologii wypełnić znamiona znakomitej większości artykułów znajdujących się w Kodeksie Karnym, Kodeksie Wykroczeń, przepisach ustaw pozakodeksowych, a także innych ustaw i dyrektyw obowiązujących na terenie Rzeczypospolitej Polskiej.

W ogólnym ujęciu kryminalistyki *modus operandi* jest to „charakterystyczny dla danego sprawcy sposób działania. Indywidualność tego sposobu jest determinowana przez szereg czynników, takich jak osobowość sprawcy, jego sprawność fizyczna, poziom wykształcenia, umiejętności i upodobania, czasem przestępczą specjalność, posiadane narzędzia, wypróbowana i sprawdzona przy innych przestępstwach metoda postępowania i wiele innych. Czynniki te, ich wielość i wzajemne kombinacje powodują, że nieraz nawet banalne z pozoru przestępstwo, sprawca popełnia w sposób tylko dla siebie właściwy, indywidualny”[3]. W ujęciu technologii informacyjnych *modus operandi* jest charakterystycznym postępowaniem, polegającym na bezpośrednim bądź pośrednim sposobie działania lub zaniechania, poprzez które można przejąć kontrolę nad każdym elementem technologii komputerowej. Tutaj Hacker ma znaczącą i istotną przewagę nad śledczymi zarówno poprzez miejsce, z którego popełnił czyn zabroniony, jak i czas, jaki upłynął od momentu jego popełnienia do wykrycia przez pokrzywdzonego określonego stanu. W zależności od umiejętności, jakich nabył, to hacker decyduje, co pozostawia dla śledczych. Jednakże należy mieć na uwadze, iż *modus operandi* jest narzędziem ułatwiającym selekcję osób i grup podejrzanych o popełnienie czynu zabronionego. Samo powiązanie i wytypowa-

[3] J. Widacki, *Kryminalistyka*, Warszawa 2012.

nie osoby podejrzanej, nie przesądza o podstawie do identyfikacji konkretnego podejrzanego, a także samego zachowania w ujęciu dowodowym. Dotychczas zbadane *modus operandi* oraz opisy sprawców i grup ukazują kilka ważnych czynników, dzięki którym badanie sposobów działania jest niezwykle istotne i pomocne, ułatwiając tym samym ujawnienie konkretnego człowieka, który popełnił dany czyn zabroniony.

Pierwszym z nich jest rozproszenie kompetencji i podział zadań. Drugim jest kwestia umiejętności hackera ze względu na wybrany przez niego cel. Trzecim jest wykorzystywanie braku wiedzy, umiejętności i przede wszystkim świadomości ofiar, (nawet przeciętny Kowalski może być ofiarą cyberprzestępców). Najważniejszą kwestią potrzebną do właściwego zbadania *modus operandi* jest za żmudne przeprowadzenie oględzin, których wyniki pozwalają odpowiedzieć na pytanie, w jaki sposób sprawca dokonał przestępstwa. By odpowiedzieć na te pytania i zebrać kompleksową wiedzę, która byłaby przydatna do analizy samego działania, przeprowadzający tą czynność muszą posiadać równie rozległą wiedzę, co sprawcy.

Do tego dochodzi pewnego rodzaju znajomość działania komponentów systemu komputerowego – zarówno od strony Hardware jak i Software. Następną kwestią jest zbadanie korelacji wszystkich składowych wewnętrznych jak i zewnętrznych, wynikających z tworzenia i przetwarzania danych i operacji. Kolejną ważną dla badaczy kwestią (zarówno z punktu widzenia takich dziedzin jak kryminalistyka, kryminologia, wiktymologia) jest wiedza o przestępstwach komputerowych, sposób oględzin, zabezpieczanie śladów oraz samo wytypowanie, poprzez zebranie wszystkich informacji. Badanie *modus operandi* przy przestępstwach komputerowych również opiera się na udzieleniu odpowiedzi na tzw. 7 złotych pytań wykrywczych[4]. Do zebrania wszystkich dowodów istotnych i wymaganych do ujęcia sprawcy, potrzebna jest perfekcyjna znajomość języków programowania,

[4] J. Widacki, *Kryminalistyka*, Warszawa 2012.

w których tworzono systemy operacyjne, bazy danych, sterowników sprzętowych oraz samej architektury sprzętu, poprzez które przetwarza się istotne dla hackerów dane[5].

Ze względu na brak wiedzy, oraz doświadczenia śledczych w zakresie oględzin powoduje nieskorelowanie, z pozoru nieistotnych czynników lub dowodów, które potem giną zwykle po wyłączeniu sprzętu. Niemożliwym jest późniejsze odzyskanie, zabezpieczenie i wykorzystanie tych dowodów. Liczba wydań czy wydawnictw przedstawiających badania zachowań przestępców komputerowych odnośnie samej procedury, a w szczególności zabezpieczania śladów i wzorów, które pomagają zestawić zebrany materiał dowodowy do konkretnej osoby, jest stosunkowo niewielka. Bazuje ona na ogólnych zasadach, i zachowaniach śledczych oraz biegłych w postępowaniu dowodowym. Największym, a zarazem najtrudniejszym powodem tego stanu rzeczy jest ciągła i nieprzerwana dezaktualizacja jakichkolwiek źródeł naukowych, tutoriali, instrukcji, dyrektyw, zarządzeń czy rozkazów z zakresu technologii informatycznych.

Groteską można nazwać oficjalne źródła policyjne dotyczące oględzin, które w głównych założeniach opierają się na archaicznych rozwiązaniach sprzed około dekady. W przypadku cyberprzestępczości nie ma jednego sztywnego algorytmu przeprowadzenia oględzin gdyż przestępcy komputerowi znają doskonale procedury przeprowadzenia czynności dowodowej. Sam sposób zachowania się sprawcy ewoluuje i pomimo wypełnienia określonych znamion przestępstwa czy też wykroczenia, najistotniejszym jest kwestia dostosowywania się sprawców do obecnej mody czy też trendów, jakie również dosięgły samo *modus operandi*.

W tym przypadku rozpoczęcie przez biegłego procedury oględzin może uruchomić pułapkę pozostawioną przez sprawcę, uniemożliwiając tym samym jakiekolwiek znalezienie i zbadanie śladów, potencjalnie użytecznych do ujawnienia konkretnej osoby, która popełniła czyn zabroniony. W ten sposób pomimo dez-

[5] Technologie informacyjne posiadają charakterystykę modułową (model OSI) Atak na jeden element wpływa negatywnie na działanie pozostałych.

aktualizacji baz danych można z określonych zachowań wydobyć detale na tyle indywidualne, że pomimo nie stosowania określonego algorytmu przestępstwa, można na podstawie dowodu z sposobu zachowania się sprawcy dokonać indywidualizacji przestępstwa.

Najlepsze rozwiązania dotyczące czynności oględzin, która jest podstawą do badania *modus operandi*, są w Stanach Zjednoczonych, Niemczech i Francji. Zaczynając od ścisłej współpracy z koncernami i producentami technologii informatycznych, USA przoduje odnośnie stanu zbadania problemu. Niestety podstawową kwestią odnośnie badań są zasadnicze różnice w systemach prawa procesowego USA i Polski oraz szybkość nowelizacji przepisów prawa materialnego odnośnie czynów sprawczych, konkretnego *modus operandi* oraz samej kryminalizacji i dekryminalizacji tych zachowań.

Celem niniejszego opracowania było przyjrzenie się zjawisku Hackingu i powiązanych z nim przestępstw komputerowych, precyzyjne określenie roli *modus operandi* w czynnościach dochodzeniowo-śledczych, określenie danych sposobów działania przestępców w ujęciu określonych kryteriów. Ukazanie roli tych przestępców w dzisiejszym świecie i umiejscowienie ich działań w określonych znamionach czynów zabronionych.

Problematyka *modus operandi* zawiera trzy główne aspekty determinujące te kwestie.

Aspekt pierwszy przedstawia ogólną charakterystykę problemu osoby Hackera zjawiska Hackingu i przestępstw komputerowych, które są ze sobą ściśle powiązane ze względu na nakładające się na siebie konkretne zachowania wypełniające znamiona określonych czynów. Genezę zjawiska, którą pierwotnie zaczęli nie informatycy, ale matematycy tworząc określone, logiczne i uporządkowane systemy, będące pierwowzorami dla inżynierów i elektroników, którzy z kolei dzięki zaadaptowaniu tak istotnej dziedziny wiedzy jak matematyka, uzależnili świat od tych dóbr. Konkretne pionierskie wyobrażenia naukowców, inżynierów, matematyków, i pasjonatów nie spowodowałyby tego, że dzisiaj eks-

pansja wszelkiego rodzaju systemów informatycznych stworzy pewnego rodzaju nowy świat, który rządzi się własnymi prawami niezależnymi od uwarunkowań zewnętrznych. Hackera, jako sprawcę, oraz ujęcie socjologiczne, postrzeganie i opiniowanie przez społeczeństwo ich działań. Tutaj w grę wchodzi praca operacyjno-rozpoznawcza, szczegółowe określenie urządzenia elektronicznego i tego, w jakich aspektach hacker może być szczególnie niebezpieczny. R. Taylor oraz U. Sieber (wybitni naukowcy badający od lat problem cyberprzestępczości dla niemieckich służb mundurowych) stworzył podział, dzięki, któremu pozornie takie same czyny zabronione penalizowane z tego samego artykułu różnią się właśnie sposobem działania. Podziały te przedstawiają się następująco.

Podział Siebera:

1. Przestępstwa w zakresie ochrony danych (naruszenie praw jednostki);
2. Przestępstwa gospodarcze z użyciem komputerów:
   a) manipulacje komputerowe:
      — operacje rozrachunkowe;
      — manipulacje bilansowe;
      — manipulowanie stanem kont bankowych;
      — nadużycia kart bankomatowych i innych środków płatniczych;
      — nadużycia telekomunikacyjne;
      — oszustwa handlowe;
      — fałszerstwo;
   b) sabotaż i szantaż komputerowy;
   c) hacking komputerowy;
   d) szpiegostwo komputerowe;
   e) kradzieże software'u i inne formy piractwa dotyczące produktów przemysłu komputerowego;
   f) oszustwa komputerowe;
   g) fałszerstwo dokumentów;
3. Inne rodzaje przestępstw;

a) rozpowszechnianie za pomocą komputerów informacji pochwalających użycie przemocy, rasistowskich i pornograficznych;
b) użycie techniki komputerowej w tradycyjnych rodzajach przestępstw[6].
c) zorganizowana działalność przestępcza:
   — prostytucja,
   — handel narkotykami i innymi substancjami psychoaktywnymi(tzw. Dopalacze), i innymi środkami niebezpiecznymi,
   — przemyt papierosów i alkoholu,
   — przemyt i handel dziełami sztuki, materiałami historycznymi,
   — nielegalny Hazard (kasyna, zakłady bukmacherskie),
   — wyłudzenia i haracze,
   — handel bronią i materiałami wybuchowymi, i radioaktywnymi,
   — kradzieże i paserstwo.

Dodatkowo należy dostrzec rolę użytkowników, jako ofiar jako cel ataków cyberprzestępczych. W tym zakresie wykonano badanie na grupie ludzi w wieku produkcyjnym, którzy w ramach specyfiki pracy i życia z technologiami komputerowymi muszą być obeznane. Badania jasno pokazują, że ludzie są świadomi zagrożeń ze strony cyberprzestępców, ale kuleje tutaj konkretna, wiedza oraz doświadczenie jak zapobiec określonym atakom i przestępstwom. Hackerzy nie działają z określonych uwarunkowań. Nie każdy Hacker jest profesjonalistą, który nie zostawia określonych śladów jasno mogących doprowadzić do jego osoby Jeden z byłych hakerów Bill Landreth wyróżnia, co najmniej pięć kategorii różnicujących grupę hakerów. Jego zdaniem można tu wyodrębnić:

[6] U. Sieber, *Przestępczość komputerowa, a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, Przegląd Policyjny 1995, nr 3(39).

- **Nowicjuszy** (The Novis), których pociągają np. gry komputerowe czy zawartość zbiorów i danych, ale ich działania w odniesieniu do systemów są nie do przewidzenia;
- **Analityków** lub badaczy (The Student) zainteresowanych poznaniem różnego rodzaju komputerów bez czynienia jakichkolwiek szkód;
- **Turystów** (The Tourist) traktujących systemy komputerowe jak łamigłówki, do których nie powracają po ich rozwikłaniu;
- **Wandali** (The Crasher) dążących umyślnie do wyrządzenia użytkownikom komputerów jak największych szkód; ich głównym zajęciem jest tworzenie coraz to wymyślniejszych wirusów, których celem jest destrukcja systemu, kasowanie danych, ataki zakłócenie pracy serwerów, przetwarzanie stron WWW;
- **Złodziei** (The Thief) działających na ogół na rzecz firm konkurencyjnych.

Do tego podziału warto dodać jeszcze trzy inne kategorie:

- **Zdobywców** (Score Keler), którzy włamują się dla sprawdzenia własnych umiejętności;
- **Szpiegów** (Spys), którzy włamują się w ściśle określonym celu, np. po to, aby wykraść informację, uszkodzić lub zdestabilizować system;
- **Cyberterrorystów** (Cyberterrorists), którzy wykorzystują własne umiejętności tylko po to, by destabilizować, uszkadzać systemy lub wykradać dane.

Aspekt drugi zawiera przedstawione elementy *modus operandi* w zakresie praktycznym tzn. Metodyka chronologiczna Hackera ze względu na poszczególne etapy działania. Hacker wykonując zadanie nie może podejść do niego bez rzetelnego wykonania rekonesansu. Sprawdzenie celu pozwala mu podejść do niego w sposób zorganizowany i konkretny. Przygotowuje określone modele włamania. Zestawienie form ataków wykorzystywanych do przestępstw komputerowych, w szczególności na wykorzysta-

nie błędów ludzkich w dokonaniu czynów przestępnych. Sposoby rejestrowania i przypisywania zachowań wykorzystywanych do działalności Hackerskiej.

Podstawową kwestią dla cyberprzestępcy jest wykonanie wszystkich elementów *modus operandi* zgodnie z założonymi wcześniej przez sprawcę. Planowanie sposobu działania zawsze się rozpoczyna od zapewnienia sobie odpowiedniego poziomu bezpieczeństwa i anonimowości, zapewnianego poprzez połączenia szyfrujące, serwery pośredniczące, połączenia obce. Czy Szyfrowane transmisje rozproszone typu VPN[7] lub TOR. Przygotowanie do ataku czy popełnienia czynów zabronionych to podstawa i swoiste 4 przykazania, które Hacker dla danego celu musi mieć opanowane do perfekcji a potem rozpracować je metodycznie w stopniu zarówno indukcyjnym, jak i dedukcyjnym

1. **Footprinting** to wykonanie kompletnego planu systemu informatycznego gdzie kładziony jest szczególny nacisk na profil zabezpieczeń. Cyberprzestępca nie może zaniedbać tego etapu gdyż jest ona najważniejsza dla losów samego ataku przestępczego. Dlatego footprinting musi być wykonywany w sposób niezwykle staranny;
2. **Wyliczanie** jest szukaniem określonych dostępnych i aktywnych węzłów i urządzeń które są najsłabszym punktem systemu. Zadanie musi być wykonywane gdyż działania w sieci są prowadzone na bieżąco i informacje zebrane podczas samego rekonesansu mogą być nieaktualne;
3. **Skanowanie** jest to ostateczny etap przed rozpoczęciem ataku czy przestępstwa. Po znalezieniu słabego punktu w określonym elemencie sieci komputerowej, Hacker korzystając z najróżniejszych narzędzi może przejąć kontrolę najpierw nad kluczowym, z punktu widzenia ataku elemen-

[7] VPN (Virtual Private Network) – prywatna sieć wirtualna polega na stworzeniu logicznego połączenia sieci po między klientami korzystającymi z połączenia. Zaletą tego rozwiązania jest brak jakichkolwiek fizycznych śladów w postaci urządzeń czy Danych pakietowych czy ciasteczek. Wszystkie dane giną po zakończeniu transmisji i ponownym uruchomieniu obu komputerów.

tem dokonując włamania, oszustwa, wymuszenia, kradzieży czy użycia wpływu socjotechnicznego;

4. **Algorytm działania** samo algorytmowanie to już nic innego jak wdrożenie tego przygotowania i wykonywanie określonych czynności i wcielanie samego *modus operandy* w życie.

Tak naprawdę same techniczne i psychologiczne aspekty działania ograniczają sprawcę jedynie posiadanie umiejętności dotyczące łamania określonych zabezpieczeń, i docierania do właściwego celu. Oraz jego wyobraźnia, która może mu pomagać zarówno w dokonywaniu przestępstw.

Aspekt trzeci charakteryzuje skutki i efekty działalności Hackerów, zmiany systemu prawnego w Polsce, oraz formy minimalizowania szkodliwych ataków i włamań poprzez działalność służb ochrony bezpieczeństwa publicznego a także firm i organizacji komercyjnych działających w sferach działalności IT. Ukazanie słabości ścigania sprawców, ich bezkarność, i bezczelność jest „solą w oku" organów ścigania. Wszelkie uwarunkowania prawne pozostają w tyle za nowoczesnymi formami sprawczymi cyberprzestępców. Przestępcy komputerowi i hackerzy coraz śmielej i chętniej wykorzystują te formy uzyskania konkretnych korzyści. Proces badawczy i wykrywczy bywa żmudny i bardzo trudny choć w każdym przypadku można uzyskać potencjalną lokalizację z którego dokonano przestępstwa.

Hacking i przestępstwa komputerowe pojawiły się jeszcze podczas etapów projektowych i testowych sieci szkieletowych, które prowadziły siły zbrojne USA oraz amerykańskie uczelnie techniczne tworząc wspólne agencję DARPA[8] pod koniec lat 60. ubiegłego stulecia, które pozwalały osiągnąć przewagę. Przełom lat 60. i 70. XX w. To rywalizacja na wszystkich polach z ZSRR podczas Zimnej Wojny, a także rozwój sieci telekomunikacyjnych i teleinformacyjnych i bankowych na automatyczne dała początek

[8] Amerykańska agencja rządowa zajmująca się rozwojem technologii wojskowych wykorzystywanych przez siły zbrojne USA.

do jednej z najbardziej dochodowej gałęzi przestępstw, która na dobre zaczęła się rozwijać w XXI wieku. Począwszy od lat 70., skala przestępstw sprawców nieujawnionych z roku na rok staje się coraz większa. Narzędzia te powodują, że bezpośrednio i pośrednio, zgodnie z Prawem Moore'a[9] skala przestępczości komputerowej i Hackingu na świecie będzie rosła wprost proporcjonalnie i za 2 lata straty związane z tą działalnością mogą się podwoić w związku ze stanem obecnym i sięgnąć 1 bln USD w roku 2017.

O ile podczas rozwoju technologii problem był zamknięty na terenie USA, to przestępstwa komputerowe i hacking stały się problemem międzynarodowym na przełomie lat 90tych XX w. Obecnie blisko 2 mld ludzi na całym świecie, regularnie korzystających z technologii informacyjnych jest narażonych na wszelkie formy działań przestępczych, ze strony elektroniki zewsząd nas otaczającej.

Ze względu na wielość odmian i ciągły rozwój technologii, źródła naukowe przestają być częściowo aktualne jednakże ich użyteczność wciąż jest na wysokim poziomie ze względu zmieniających się czynności wykonywane do popełnienia przestępstwa, samo przestępstwo kradzieży, oszustwa etc. wciąż nim pozostaje zmieniają się narzędzia i sposób ich użycia. Ogólna Literatura przedmiotu, która opisuje w sposób aktualny te zagadnienia to Czasopisma fachowe, specyfikacje techniczne, biuletyny bezpieczeństwa oraz artykuły organizacji, portali i firm zajmujących się określonymi zagadnieniami z zakresu metodyki tematu. Źródła te najlepiej oddają istotę problemu gdyż skupiają się na najnowszych i najpopularniejszych formach działania przestępców oraz wyczerpująco przedstawiają sposoby zapobiegania, walki i minimalizacji skutków.

[9] Trend wykładniczy zaobserwowany w 1965 r. przez inżyniera firmy Intel Gordona Moore'a która pierwotnie głosiła głosi, iż co 18 miesięcy (obecnie, co 24 miesiące) liczba tranzystorów a co za tym idzie moc obliczeniowa komputerów podwaja się. Twierdzenie *per analogium* wykorzystuje się w całej branży IT oraz w badaniach zjawisk przestępstw komputerowych.

Polskojęzyczna literatura tematu to przede wszystkim przedruki i tłumaczenia anglojęzycznych niemieckojęzycznych i francuskojęzycznych wydawnictw i artykułów. W tym polu jednak szczególnie wysoko należy odnotowywać wszelkie publikacje naukowców i prawników badających temat przestępczości komputerowej w sferach prawa polskiego głównie A. Adamskiego, który jako pierwszy ustandaryzował prawne pojęcia dotyczące przestępstw komputerowych w prawie polskim i J. Wójcika, który publikował szereg artykułów prawnych przedstawiających problematykę przestępstw komputerowych. P. Podreckiego, który również przedstawiał temat prawa internetowego w zmienionej formule. Mimo że niektóre pozycje zostały wydane kilka i kilkanaście lat temu, co w technologiach informatycznych i prawie powoduje, że część informacji staje się nieaktualna to jednak są to dzieła, które zawierają pewne uniwersalne informacje i poglądy użyteczne w temacie oraz portali bezpieczeństwa niebezpiecznik.pl; hack.pl; Hackin8. Literatura obcojęzyczna w związku z większym stopniem zbadania tematu aspektów kryminalistyki komputerowej jest bogatsza Szczególnie wysoko należy ocenić źródła prof. U. Siebera wybitnego niemieckiego badacza, który zapoczątkował temat badań i różnicowania przestępstw komputerowych i Hackingu. Jego badania zostały użyte w przekładach innych badaczy i naukowców opisujących te zagadnienia. Dodatkowo by poznać i rozróżnić tematykę *modus operandi* należało również sięgnąć do źródeł wydanych przez byłych hackerów, ekspertów ds. bezpieczeństwa oraz pracowników firm produkujących rozwiązania zabezpieczające systemy komputerowe, m.in. „Sztuka podstępu" aut. K. Mitnick, „Sztuka penetracji" aut. J. Erickson, „Informatyka śledcza. Przewodnik po narzędziach open source" aut C. Altheide, H. Carvey, a także „Vademecum Hackingu" aut. S. McClure, J. Scambray, G. Kutz.