Rocznik Bezpieczeństwa Morskiego

PRZESTĘPCZOŚĆ TELEINFORMATYCZNA 2020

Pod redakcją:
Jerzego Kosińskiego
Grzegorza Krasnodębskiego

Gdynia 2021

Recenzenci:
prof. dr hab. Krzysztof FICOŃ
dr hab. Bartłomiej PĄCZEK

Wydawca:

Współwydawca:

ISSN 1898-3189

Spis treści

WSTĘP

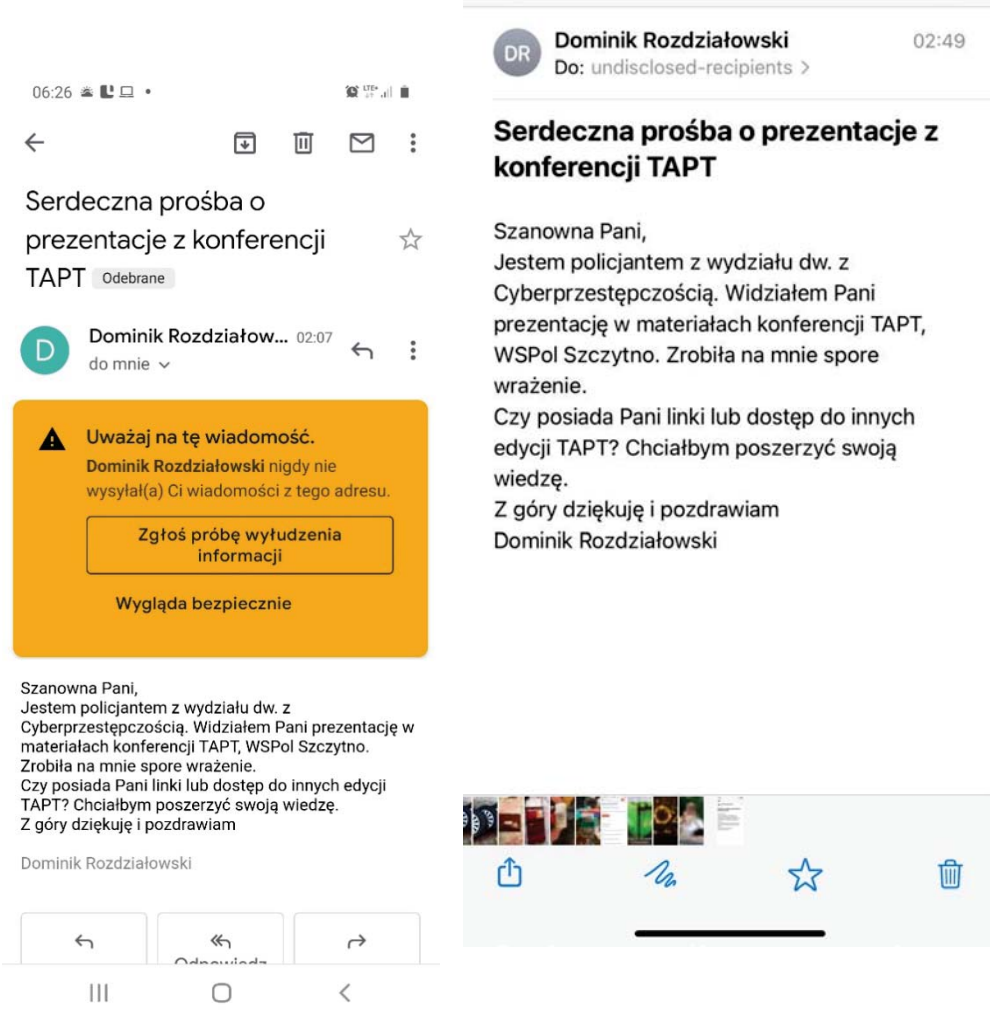
Rok 2020 będzie pamiętany jako rok, w którym rozpoczęła się pandemia COVID-19. Pandemia przyspieszyła wdrożenie nowych technologii wspierających transformację cyfrową, w szczególności wspomagających zdalną pracę i nauczanie. Sprawiła, że codzienne życie stało się uzależnione od właściwego wykorzystania środowiska cyfrowego. Uzależnionie od usług cyfrowych w pracy i szkole, w kontaktach z administracją publiczną i w wielu innych aspektach życia. Bezpośrednią konsekwencją tej sytuacji był błyskawiczny rozwój nowych form komunikacji cyfrowej i zdalnej pracy, skutkujący ogromnym wzrostem ilości przetwarzanych danych. Niestety, pandemia i masowe przechodzenie na pracę zdalną znacznie ułatwiły cyberprzestępcom zadanie. Jak podkreśla Europol w raporcie IOCTA 2020 (Internet Organised Crime Threat Assement)[1], przestępcy szybko zareagowali na pandemię, opracowali nowe sposoby działania, ale także dostosowali istniejące metody, tak by skorzystać z nowych, niespotykanych do tej pory na tak dużą skalę okoliczności.

Rok 2020 będzie pamiętany także jako rok, w którym nie odbyła się kolejna edycja Konferencji Naukowej pt. Przestepczość Teleinformatyczna XXI (PTXXI). Tematem wiodącym tej edycji miał być „łańcuch dowodowy". Niestety pandemia uniemożliwiła przeprowadzenie konferencji, ani w tradycyjnym terminie, ani w dodatkowym. Tym niemniej, jak w poprzednich latach, powstała monografia, w której znalazło się 16 rozdziałów. Większość z nich nie jest związana z tematem przewodnim planowanej konferencji. W monografii dominuje szerokie spojrzenie na tematykę cyberprzestępczości obejmujące zagadnienia prawne, techniczne i organizacyjne, przedstawione w wymiarze praktycznym i teoretycznym.

W roku 2020 zauważyliśmy także, że zarówno organizowanie konferencji, jak i publikowanie monografii ma sens. Potwierdzenie tego stwierdzenia przyszło z nieoczekiwanego miejsca. Prelegenci i autorzy rozdziałów zaczęli otrzymywać e-maile i SMSy, w których proszono ich o udostepnienie swoich wystąpień lub dostępu do monografii. Nie byłoby to dziwne, gdyby nie fakt, że występujący o te materiały ukrywali swoją tożsamość, podszywając się pod

[1] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.

różne osoby. Najciekwsze było podszycie się pod wielokrotnego prelegenta naszej konferencji – Dominika Rozdziałowskiego.



Hej!
Jestem młodą kobietą która stawia pierwsze kroki w branży infosec. Widziałam Pana prezentację w materiałach konferencji TAPT, WSPol Szczytno. Zrobiła na mnie duże wrażenie.
Czy posiada Pan może linki lub dostęp do innych edycji TAPT? Chciałabym poszerzyć moją wiedzę.
Z góry dziękuję :)
Alicja Balcerzak

Szanowny Panie,
Jako pracownik działu bezpieczeństwa sieciowego i informatycznego z branży bankowości, jestem czytelnikiem i fanem Pańskiej "Przestępczości Teleinformatycznej".
Posiadam kilka edycji, jednak brakuje mi materiałów z wystąpień prelegentów TAPT. Czy może Pan je udostępnić?
Z góry dziekuje i pozdrawiam

Dzięi zaobserwowaniu tego dodatkowego zainteresowania, utwierdziliśmy się w przekonaniu, że właśnie ten szeroki zakres tematyczny monografii sprawia, że każdy znajdzie w niej teksty, które będą go satysfakcjonować. Tym samym monografia jest przydatna wszystkim osobom, które interesują się zapewnieniem cyberbezpieczeństwa oraz ściganiem sprawców cyberprzestępstw, w szczególności studentom kierunków związanych z bezpieczeństwem wewnętrznym, kryminologią, prawem oraz informatyką.

Życząc czytelnikom przyjemnej lektury zachęcamy do kontaktu z redaktorami, w sprawie kolejnych edycji konferencji i monografii.

Jerzy Kosiński (j.kosinski@amw.gdynia.pl)
Grzegorz Krasnodębski (g.krasnodebski@amw.gdynia.pl)

ROZDZIAŁ 1

DZIAŁANIA MILITARNE W CYBERPRZESTRZENI – PRÓBA KLASYFIKACJI

dr hab. inż. Piotr DELA [2]

STRESZCZENIE: W rozdziale przedstawiono próbę klasyfikacji działań militarnych w cyberprzestrzeni. Punktem wyjścia było określenie celowości tychże działań, ukierunkowanych na efektywność oddziaływania w punktu widzenia, czasu, kosztu i stopnia osiągnięcia celu. Dodatkowo przedstawiono działania ochrono-obronne związane z szeroko pojmowanym bezpieczeństwem informacyjnym, a także klasyfikację poziomów działań w cyberprzestrzeni, przyjmując za punkt wyjścia klasyczny podział na działania strategiczne, operacyjne i taktyczne.

SŁOWA KLUCZOWE: cyberprzestrzeń, konflikt cybernetyczny, teoria walki, bezpieczeństwo cyberprzestrzeni.

1. Wstęp

Punktem wyjścia do określenia klasyfikacji działań militarnych w cyberprzestrzeni powinno być zidentyfikowanie celowości takich działań, a to wymaga w pierwszej kolejności zidentyfikowania czym w swojej istocie jest sam cel działania i jakie podmioty mogą go rea-

[2] Morskie Centrum Cyberbezpieczeństwa, p.dela@akademia.mil.pl; ORCID: 0000-0003-3643-3759.

lizować. Cel, według zapisów encyklopedycznych, to: do *czego się dąży, co się chce osiągnąć*[16]. W prakseologii cel rozumiany jest jako planowy wynik każdego racjonalnego działania. Cel ten wyznaczany jest przez podmiot działania i w zależności od przyjętego przez niego systemu wartości może być określany jako **stopniowalny** lub **niestopniowalny** [1]. W **celu stopniowalnym** określone są warunki brzegowe jego osiągnięcia w kategoriach takich jak: **ilość**, **jakość**, **miejsce**, **czas**. **Cel niestopniowalny** oznacza, iż w warunkach jego osiągnięcia przyjęto, że może być, jako całość, osiągnięty lub nieosiągnięty.

Podmiot działania, wymieniany w powyższych definicjach, jest postrzegany różnie, w zależności od sposobu jego zorganizowania i umiejscowienia w nadrzędnym systemie bezpieczeństwa. Podmiotami tymi mogą być jednostki, społeczność, grupy formalne i nieformalne, związki wyznaniowe, stowarzyszenia, organizacje, firmy, państwa, organizacje międzynarodowe. Każdy z nich ma swój własny system wartości a tym samym ich cele działania mogą być odmienne. Oczywiście będą one pochodną rodzaju kooperacji w której uczestniczą, ukierunkowaną na współpracę, rywalizacje lub walką.

Próbując zidentyfikować walkę, bo z nią są związane działania militarne w cyberprzestrzeni, należy zauważyć, że termin ten ma wiele znaczeń, szczególnie współcześnie, gdzie jest on jest używany do opisu zarówno *walki zbrojnej*, *walki politycznej* czy też jakikolwiek innej formy rywalizacji. Walka, a tym bardziej walka zbrojna stanowią kategorie podstawowe w sztuce wojennej. Także w prakseologii walka i walka zbrojna mają swoje odzwierciedlenie w ogólnej teorii walki i są określane często jako kooperacja negatywna [9].

W klasycznym ujęciu Tadeusza Kotarbińskiego wyróżnia się kooperację pozytywną, identyfikowaną jako współdziałanie, i kooperację negatywną, utożsamianą z walką. Podstawą takiej klasyfikacji jest zgodność (kooperacja pozytywna) lub niezgodność (kooperacja negatywna) celów podmiotów kooperujących. Mirosław Sułek podzielił występujące kooperacje na trzy działy: współpracę, rywalizację i walkę [18]. Podstawą wyjściową takiego podejścia były formy stosunków międzyludzkich. W tym ujęciu współpraca oznacza odniesienie, przez wszystkich kooperantów, korzyści, które mogą mieć charakter materialny lub niematerialny, a najbardziej wyrazistym przykładem współpracy jest gospodarka i szeroko rozumiana ekonomia [18]. W rywalizacji korzyści postrzegane są zgoła odmiennie. To co jest zyskiem dla jednej strony jest jednocześnie stratą dla strony drugiej, a wartość ich jest tożsama. W wymiarze międzynarodowym rywalizacja zmierza do osiągniecia potęgi światowej i procentowego udział kooperantów w jej całości. Jak podaje Sułek, rywalizacja jest działalnością regulacyjną, zmierzającą do ustalenia proporcji pomiędzy współpracą a walką, a osią tej rywalizacji są stosunki sił [18]. Walka w ujęciu Mirosława Sułka oznacza kooperację, w której wszystkie strony

ponoszą straty. Może być ona prowadzona w różnych obszarach i na różnych poziomach. Logika takiego postępowania prowadzi do zwycięstwa silniejszego [18].

W sensie ogólno-prakseologicznym walka to: *wszelkie działanie przynajmniej dwupodmiotowe (przy założeniu, że zespół może być podmiotem), gdzie jeden przynajmniej z podmiotów przeszkadza drugiemu. Oba podmioty nie tylko dążą obiektywnie do celów niezgodnych, lecz nadto wiedzą o tym i liczą się w budowaniu planów działania też z działaniem strony przeciwnej. Obie strony zmuszają się wzajemnie w sposób osobliwie intensywny do pokonywania trudności, a więc pośrednio – do usprawnienia techniki działania* [9]. Wymienione w definicji podmioty są, z punktu widzenia nauk o bezpieczeństwie, podmiotami bezpieczeństwa. To obywatele, społeczeństwa, organizacje a także państwa. Najistotniejszym przypadkiem walki z punktu widzenia tematu rozważań jest walka na poziomie państw, w której wykorzystywane są wszystkie dostępne narzędziami takie jak dyplomacja, służby, siły zbrojne, potencjał naukowy i gospodarczy. Ten rodzaj walki jest domeną polityki, a siły zbrojne są jednym z wielu narzędzi wykorzystywanych w walce, oczywiściej jednym z najważniejszych.

W dalszej części przedstawiano najważniejsze elementy walki w cyberprzestrzeni, poczynając od klasyfikacji celów działania, poprzez bezpieczeństwo informacyjne skupione na ochronie zasobów, kończąc na klasyfikacji poziomów działań militarnych w cyberprzestrzeni.

2. Cele działań w cyberprzestrzeni

Analizując cele realizowane w walce w cyberprzestrzeni, na pierwszy plan wysuwa się *cel polityczny*, który pojmowany jest jako oczekiwany efekt postępowania w sferze politycznej. To najczęściej rezultat wzajemnych relacji i oddziaływań pomiędzy wszystkim uczestnikami życia politycznego. Są nimi zarówno partie polityczne, społeczeństwa, elity, ośrodki władzy jak i grypy nacisku, formalne i nieformalne. Działania związane z realizacją celów politycznych ukierunkowane są na wzmocnienie, utrzymanie lub osłabienie poszczególnych podmiotów polityki. W kooperacji negatywnej działania te mogą zmierzać, w stosunku do podmiotu politycznego do osamotnienia, zdezawuowania, zmuszenia, destabilizacji, zmiany, upadku.

Wszystkie powyższe cele ukierunkowane są na osłabienie lub wręcz zniszczenie podmiotu politycznego, podyktowane realizacją własnych interesów, przeciwstawnych do interesów atakowanego podmiotu. Największego znaczenia w tym obszarze odgrywa oddziaływanie informacyjne realizowane najczęściej za pomocą dezinformacji i propagandy, ukierunkowane zarówno na obiekt oddziaływania ale także na jego otoczenie. Należy jednak

pamiętać o tym, że mogą być wykorzystane także elementy oddziaływania informatycznego i kinetycznego, zgodnie z zasadą synergii, zespolenia działań kierunkowych na maksymalizacje efektów działania. Realizacja potencjalnego celu jakim jest upadek państwa może być wielostopniowa i rozłożona w długim okresie czasu. W pierwszej kolejności atakujący będzie prowadził kampanie informacje ukierunkowane na społeczeństwo w celu jego skłócenia, wytworzenia coraz większych podziałów i budowania nastrojów niezadowolenia. Równocześnie, w społeczności międzynarodowej prowadzona będzie kampania informacyjna ukierunkowana na osłabienie wizerunku państwa i jego obywateli. Szerzone będą nieprawdziwe informacje na temat atakowanego społeczeństwa, bazujące najczęściej na stereotypach i uprzedzeniach. Faza takiego oddziaływania może być realizowana przez długie lata do momentu, aż agresor uzna, że nadszedł odpowiedni czas do dalszej eskalacji konfliktu, polegającej na wprowadzeniu elementów oddziaływania informatycznego i kinetycznego. Poprzez zniszczenie lub czasowe obezwładnienie kluczowych elementów infrastruktury krytycznej w połączeniu z oddziaływaniem kinetycznym np. na decydentów mających autorytet w społeczeństwie można doprowadzić do wywołania masowych protestów, strajków a nawet zamachu stanu. Wszystko zależy od siły oddziaływania agresora i odporności atakowanego państwa.

Następnym potencjalnym celem realizowanym w walce w cyberprzestrzeni jest *cel ekonomiczny,* związany z aktywnością podmiotu w sferze gospodarczej. Dla podmiotów takich jak państwo cele ekonomiczne podyktowane są zrównoważonym rozwojem kraju, rozwojem gospodarki, bogaceniem się społeczeństwa, a jego wymiernymi wyznacznikami są takie elementy jak: produkt krajowy brutto, dług publiczny, zdolność kredytowa, stosunek eksportu do importu, poziom zamożności społeczeństwa. Realizacja powyższego wymaga od państwa posiadania odpowiednich zasobów materiałowych, energetycznych, ludzkich, technologicznych, produkcyjnych i finansowych. Tym samym, w kooperacji negatywnej ukierunkowanej na cele ekonomiczne można oddziaływać między innymi na zasoby, technologie, przemysł, system finansowy.

Powszechnie znane są przypadki państwa, które w swojej działalności w cyberprzestrzeni ukierunkowane są na inwigilację i kradzież technologii, co pozwala im skutecznie rozwijać własną gospodarkę. Zaznane są również przypadki działalności ukierunkowane na uzależnienie państwa, np. od surowców energetycznych lub też nawet ich pozbawienia. W przypadku zasobów ludzkich, sterowanie przekazem informacyjnym szkalującym dane społeczeństwo, powielającym stereotypy i uprzedzenia, może być ukierunkowane na odstręczenie potencjalnych emigrantów od rynku pracy atakowanego podmiotu. Z kolei generowanie podziałów i niepokojów społecznych może skutkować także zwiększeniem emigracji

zarobkowej, tym samym pozbawieniem atakowanego państwa rąk do pracy. Poprzez szerzenie fałszywych informacji na temat sytuacji gospodarczej i ekonomicznej danego państwa można doprowadzić do obniżenia ratingów zdolności kredytowej państwa, tym samy doprowadzić do jego głębokiej zapaści ekonomicznej i społecznej. Wroga działalność wymierzona w podstawy ekonomiczne innego podmiotu bezpieczeństwa wymaga jednak czasu i przede wszystkim informacji, zarówno zdobytej (wykradzionej), zmodyfikowanej, jak i celowo spreparowanej.

Kolejnym istotnym celem realizowany w trakcie kooperacji negatywnej w cyberprzestrzeni jest *cel społeczny*. W większości państw demokratycznych to społeczeństwo jest tym elementem, który kształtuje ustrój państwa i wybiera przedstawicieli odpowiedzialnych za prowadzenie polityki. Najogólniej rzecz ujmując społeczeństwo decyduje, w którą stronę podąża państwo. Jeżeli istnieje potencjalna możliwość wyznaczenia tego kierunku, na drodze oddziaływania w cyberprzestrzeni, umożliwiająca realizację własnych interesów bez potrzeby eskalacji konfliktów, to działania takie będą podejmowane coraz częściej. Oczywiście cele te mogą być powiązane równocześnie z celami politycznym, jak chociażby podczas wpływania na wyniki wyborów czy też referendów. Oddziaływania negatywne na społeczeństwo może być ukierunkowane najczęściej na rozbicie, zubożenie, załamanie, zbuntowanie, przestraszenie.

W myśl zasady dziel i rządź, działanie na rozbicie społeczeństwa podyktowane jest osłabieniem woli społeczeństwa do przeciwstawienia się wszelkim przeciwnościom i zagrożeniom. Łatwiej jest bowiem rywalizować z przeciwnikiem, który nie stanowi jedności, nie ma poparcia w całości społeczeństwa, nie może liczyć na jego poświęcenie i oddanie, zwłaszcza w sytuacjach kryzysowych. Pogłębianie i generowanie podziałów może mieć różnorodne podłoże, zarówno światopoglądowe, kulturowe, ideologiczne, jak też ekonomiczne. Różne są drogi i sposoby takiego oddziaływania lecz wspólny cel – zniszczenie wspólnoty narodowej. Najczęściej oddziaływanie takie będzie miało postać precyzyjnie przygotowanej i prowadzonej kampanii propagandowej, rozłożonej w czasie, umożliwiającej realizację przyjętych celów strategicznych. Co więcej, cyberprzestrzeń umożliwia jej prowadzenie w oderwaniu od uwarunkowań geograficznych, administracyjnych i czasowych, i jest tym bardziej skuteczna, im bardziej złożone jest społeczeństwo podmiotu oddziaływania.

Nie powinno zapominać się o *celu religijnym*, związanym bezpośrednio z atakiem na systemy wartości dominujące w danym społeczeństwie. Z jednej strony dąży się do radykalizacji poglądów, z drugiej do ich osłabienia. To także przeciwstawienie wyznawców jednej religii przeciwko wyznawcom innej i dążenie do zwiększenia zasięgu własnej wiary i wartości poprzez działania ukierunkowane na zastraszenie lub konwersję. Wojny religijne zawsze były

nieodzownym elementem historii ludzkości. Oczywiście ich charakter podyktowany był często nie tylko celem ideologicznym, lecz także czystą pragmatyką zdobycia władzy, zajęcia terenu, przejęcia zasobów, wzbogacenia się, niemniej jednak ich przebieg i zakres zawsze związany był z rozwojem ludzkości. I chociaż można zgodzić się z poglądem, że ich współczesny wymiar może być także krwawy, jak w przypadku wojny toczonej przez tak zwane państwo islamskie, to coraz większą aktywność ugrupowań religijnych możemy obserwować w cyberprzestrzeni. Jest to doskonałe środowisko propagowania idei, znajdowania i pozyskiwania zwolenników i wyznawców, radykalizowania poglądów, szerzenia strachu i terroru. To także środowisko komunikacyjne, pozwalające na tworzenie organizacji rozproszonych, umożliwiające koordynowanie działań umotywowanych ideologicznie, wymierzonych zarówno w przeciwników religijnych, jak i w społeczeństwa bazujące na innych systemach wartości. W tą działalność wpisują się różnego rodzaju fundamentaliści religijny, stosujący jako sposób oddziaływania zamachy terrorystyczne.

Pozostał do omówienia jeszcze *cel militarny*, związany bezpośrednio z działaniami sił zbrojnych w piątym wymiarze walki jaką jest cyberprzestrzeń. Identyfikując walkę w cyberprzestrzeni można pokusić się o dygresję, że może posiadać ona charakter zarówno walki zbrojnej, jak i niezbrojnej, może być walką wspieraną lub też walką wspierającą inne rodzaje walk. Cele realizowane w cyberprzestrzeni będą wynikały z przyjętych celów operacyjnych i strategicznych, roli i miejsca walki w cyberprzestrzeni w systemie nadrzędnym. Mogą być one ukierunkowane zarówno na destrukcję zasobów przeciwnika, osłabienie jego potencjału, przejęcie lub utrzymanie trenu, zyskanie czasu, ochronę i osłonę własnych zasobów militarnych i cywilnych. Obywać się to będzie za pomocą kampanii informacyjnych, oddziaływania informatycznego i kinetycznego, przy uwzględnieniu synergii z innymi rodzajami działań.

Carl von Calusewitz odnosząc się od celów i środków walki stwierdził, że *jeżeli wojna jest aktem przemocy, aby zmusić przeciwnika do wykonania naszej woli, to powinno zawsze chodzić jedynie i wyłącznie o powalenie wroga, to znaczy jego obezwładnienie* [2]. Do przeszkód stojących na drodze realizacji powyższego celu zaliczył trzy przedmioty: siły zbrojne, kraj i wolę nieprzyjaciela. Następnie określił sposób postepowania z poszczególnymi przedmiotami. W przypadku sił zbrojnych, to ich zniszczenie, doprowadzenie do stanu, w którym nie będą zdolne do dalszej walki. Z kolei kraj należy zdobyć, ponieważ mogą być w nim odtwarzane nowe siły zbrojne. Końcowym elementem wojny powinno być złamanie woli przeciwnika, zmuszenie do ustępstw, spełnienie żądań i poddania narodu. Ta swoista triada klasycznych elementów wojny był wyznacznikiem sposobu rozegrania wojen przez praktycznie cały okres historii ludzkości. I zapewne nadal nią może być w odniesieniu do wybranych

podmiotów prawa międzynarodowego. Niemniej jednak powinniśmy się zastanowić, a co jeżeli odwrócilibyśmy hierarchię wartości i na pierwszy plan wysunęli osłabienie lub nawet zniszczenie woli przeciwnika? Czy zagwarantuje to osiągniecie przyjętych celów działania? Czy trzeba zająć kraj i zniszczyć siły zbrojne aby wygrać wojnę? Tym bardziej, że współczesne pojęcie wojny zostało rozmyte, a każdy konflikt zbrojny niesie za sobą niepewność wyniku końcowego i związany jest z kosztami ekonomicznymi i społecznymi. Patrząc przez pryzmat powyższego można założyć, że sukces może być odniesiony poprzez zmianę priorytetów oddziaływania i ukierunkowanie ich na ludzi, którzy decydują o kierunkach funkcjonowania podmiotów jakimi są państwa.

3. Bezpieczeństwo informacyjne

W pierwszej kolejności uwagę skupimy na działaniach związanych z ochroną i obroną własnych zasobów informacyjnych i systemów krytycznych. Działania te są ukierunkowane na jak najlepsze wykorzystanie czasu w celu zwiększeniu poziomu ochrony własnych zasobów między innymi poprzez poznanie i likwidację podatności, identyfikowaniu zamiarów i możliwości potencjalnego przeciwnika, przeciwstawieniu się wrogim kampaniom informacyjnym, utrzymaniu sprawności i funkcjonalności chronionych zasobów informacyjnych. Niestety nadal można zaobserwować, że nie wszystkie podmioty bezpieczeństwa ukierunkowują swoją działalność na ochronę posiadanych zasobów. Niektóre są wręcz nieświadome istniejących zagrożeń lub też nie widzą takiej potrzeby. Najczęściej podmiotami tymi są ludzie, którzy o znaczeniu ochrony zasobów informacyjnych dowiadują się post factum, w chwili gdy staną się ofiarami przestępstwa popełnionego w cyberprzestrzeni. Dotyczy to także małych organizacji i najczęściej podyktowane jest kosztami ochrony. Bezpieczeństwo bowiem kosztuje zarówno w aspekcie organizacyjnym, ludzkim, jak i pod względem materiałowym. Niemniej jednak dla podmiotów jakimi są państwa, korporacje, organizacje międzynarodowe ochrona posiadanych zasobów jest priorytetem, warunkującym skuteczność jakiegokolwiek działania. Cele realizowane podczas ochrony i obrony zasobów informacyjnych i teleinformatycznych wpisują się w obszar *bezpieczeństwa informacyjnego*, które w odróżnieniu od *bezpieczeństwa informacji*, jest pojęciem złożonym i dużo trudniejszym do uchwycenia. Bezpieczeństwo, najogólniej rzecz ujmując, postrzegane jest w dwóch wymiarach: statycznym i dynamicznym. Ten pierwszy mówi nam, że bezpieczeństwo jest stanem psychicznym lub prawnym związanym z brakiem zagrożeń. Z punku widzenia procesu, bezpieczeństwo rozumiane jest jako ciągła działalność podmiotu bezpieczeństwa na rzecz poprawy i osiągnięcia pożądanego poziomu bezpieczeństwa. To działalność nas samych, ale przede wszystkim dzia-

łalność takich podmiotów jak państwa i organizacje międzynarodowe. W tym obszarze działalność ta jest przeciwwagą dla destabilizacji, ukierunkowaną nie tylko na utrzymanie ładu, porządku i pokoju, ale także na zapewnieniu poczucia bezpieczeństwa wśród obywateli. W tym obszarze niezmiernie ważne jest umiejętne kreowanie bezpieczeństwa informacyjnego, polegającego nie tylko na ochronie własnych zasobów informacyjnych lecz przed wszystkim na przeciwstawieniu się wrogim kampaniom informacyjnym ukierunkowanym na osłabienie i destabilizację podmiotów bezpieczeństwa. Informacja jest bowiem nie tylko celem (obiektem) wrogiego oddziaływania, ale także, a może przede wszystkim, narzędziem ataku.

Przejdziemy zatem do zidentyfikowania bezpieczeństwa informacyjnego i zacznijmy od jej składowej a mianowicie bezpieczeństwa informacji, którego definicje są różnorodne, uwzględniające różne aspekty i obszary odpowiedzialności. Najogólniej rzecz ujmując *bezpieczeństwo informacji to stan, w którym zapewniona jest swoboda dostępu i przepływu informacji połączona z racjonalnym i prawnym wyodrębnieniem takich kategorii, które podlegają ochronie ze względu na bezpieczeństwo podmiotów, których dotyczą* [3]. To także *stan lub ochrona przed niekontrolowanymi stratami i skutkami, kombinacja usług zapewniających poufność, integralność i dostępność* [12].

Niestety w literaturze przedmiotu często mylone jest bezpieczeństwo informacyjne z bezpieczeństwem informacji. Ten dysonans wynika z podejścia do klasyfikacji podmiotowej i przedmiotowej bezpieczeństwa. W klasyfikacji podmiotowej informacja nie występuje jako podmiot bezpieczeństwa, nie jest postrzegana jako byt. Co więcej, patrząc przez pryzmat samej definicji informacji, często jest ona postrzegana jako wytwór ludzkiego umysłu uwarunkowana aparatem poznawczym i danymi, które ten aparat postrzega, przetwarza i na podstawie której podejmuje działania. Z tego też względu występują definicje, które mówią nie o bezpieczeństwie informacji a o bezpieczeństwie danych. W klasyfikacji przedmiotowej wymieniane jest bezpieczeństwo informacyjne jako bezpieczeństwo przymiotnikowe podmiotu bezpiczeństwa. Może być nim człowiek, społeczeństwo, organizacja, państwo, organizacja międzynarodowa. A skoro tak, to nasuwa się pytanie, czy tylko i wyłącznie poprzez ochronę zasobów informacyjnych możemy zapewnić bezpieczeństwo informacyjne podmiotu jakim jest chociażby państwo?

Bezpieczeństwo informacji w swojej istocie ogranicza się do zapewnienia trzech atrybutów informacji takich jak: poufność, dostępność i integralność [12]. Osiągane jest w trzech obszarach: organizacyjnym, technicznym i fizycznym poprzez implementację między innymi systemu zarządzania bezpieczeństwem informacji bazującym na przyjętych normach, np. ISO 27001. Bezpieczeństwo informacyjne wykracza w istotny sposób poza ramy obowiązujących

norm. Informacja, funkcjonująca w przestrzeni informacyjnej, stała się narzędziem i środkiem realizacji przyjętych celów działania. W bezpieczeństwie informacyjnym, oprócz zapewnienia bezpieczeństwa informacji, niezwykle istotne jest stosowanie elementów walki informacyjnej z elementami dezinformacji i propagandy. Jej umiejętne wykorzystanie pozwala nie tylko na działanie z pozycji dodatniej w stosunku do potencjalnych adwersarzy, ale także pozwala kreować rzeczywistość stawiającą dowolny podmiot bezpieczeństwa, zarówno w korzystnym, jak i niekorzystnym świetle. Co więcej, każdy podmiot bezpieczeństwa musi być równocześnie świadomy, że także on może być celem oddziaływania informacyjnego, ukierunkowanego na dyskredytację, zmniejszenie wpływów, poniesienie wymiernych strat. Zdolność skutecznego przeciwstawienia się wrogiej kampanii informacyjnej i zdolność do identyfikacji, kto za nią stoi staje się newralgicznym elementem funkcjonowania każdego państwa i najważniejszym czynnikiem skutecznego działania. Spłaszczanie problemu tylko i wyłącznie do ochrony zasobów informacyjnych nie gwarantuje działania z pozycji dodatniej w XXI wieku.

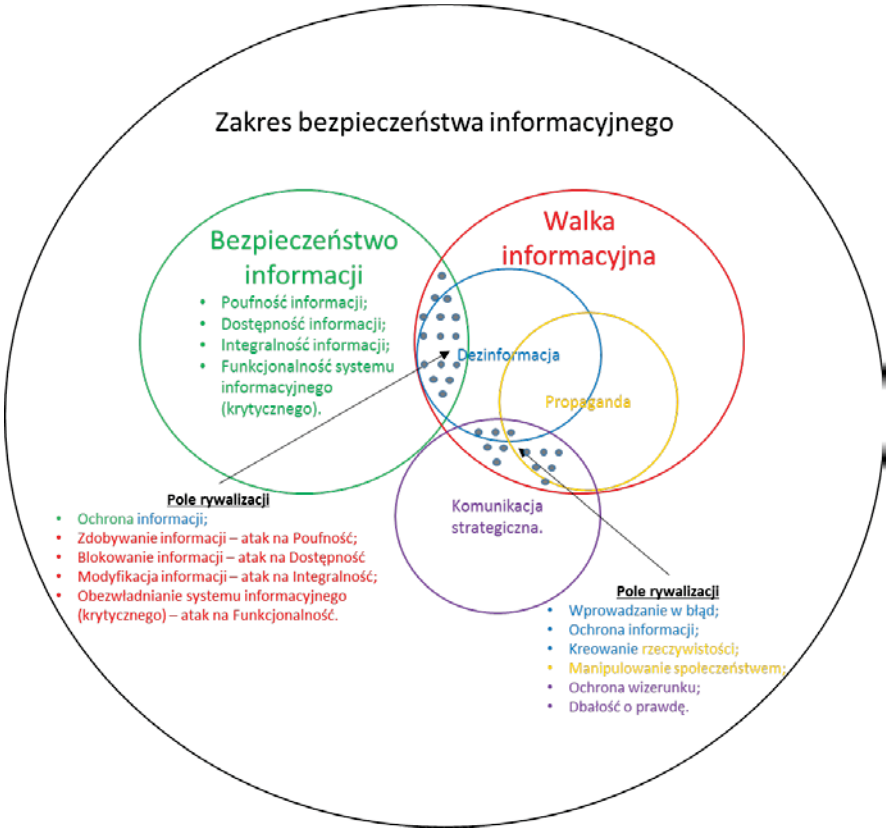
Bezpieczeństwo informacyjne to transsektorowy obszar bezpieczeństwa, który odnosi się do środowiska informacyjnego (przestrzeni informacyjnej). Jest to proces, którego celem jest zapewnienie prawidłowego i zarazem bezpiecznego funkcjonowania podmiotu bezpieczeństwa w przestrzeni informacyjnej poprzez panowanie we własnej infosferze w celu zabezpieczenia własnych interesów, w przypadku państwa – interesów narodowych. Realizacja powyższego wymaga: zapewnienia odpowiedniej ochrony posiadanych zasobów informacyjnych, przeciwstawienia się wrogim działaniom dezinformacyjnym i propagandzie oraz prowadzenie aktywnych, informacyjnych działań ofensywnych wobec adwersarzy. Zadania te powinny znaleźć odzwierciedlenie w strategii każdego państwa, a ich implementacja umożliwi stworzenie systemu bezpieczeństwa informacyjnego [6]. Bezpieczeństwo informacyjne występuje w środowisku wewnętrznym, zewnętrznym, militarnym, niemilitarnym, osobowym, społecznym, technologicznym i wielu innych.

Bezpieczeństwo informacyjne jest najbardziej wrażliwym obszarem bezpieczeństwa, zarówno w państwie, jak również na arenie międzynarodowej. Ma wpływ na skuteczność i efektywność funkcjonowania całego systemu bezpieczeństwa zarówno narodowego, jaki i międzynarodowego. Dodatkowo należy zauważyć, że działania podejmowane w obszarze bezpieczeństwa informacyjnego muszą być podejmowane z uwzględnieniem praw człowieka i obywatela, a w szczególności poszanowania prawa do prywatności i wolności słowa, co nie jest takie proste i oczywiste.

Nieodzownym elementem bezpieczeństwa informacyjnego jest walka informacyjna. Jest ona elementem polityki podmiotów bezpieczeństwa takich jak państwa czy też korporacje, a ich głównym celem jest działanie z pozycji dodatniej w stosunku do konkurenta (przeciwnika). Zdobywanie informacji, ochrona własnych zasobów informacyjnych oraz prowadzenie kampanii informacyjnych będą odgrywały coraz większą rolę w otaczającym nas świecie. W obszar bezpieczeństwa informacyjnego wchodzi także komunikacja strategiczna, jako narzędzia skutecznego kształtowania pozytywnego wizerunku podmiotu bezpieczeństwa jakim jest państwo, zarówno we własnym społeczeństwie, jak i na arenie międzynarodowej. Komunikacja strategiczna postrzegana jest jako *synteza działań informacyjnych danego podmiotu strategicznego (np. państwa, sojuszu, koalicji) ukierunkowanych na kształtowanie poglądów, ocen, opinii itp. oraz decyzji innych podmiotów z otoczenia korzystny dla własnych interesów strategicznych* [7]. Jej znaczenie wzrosło wraz z rozwojem mediów i możliwością dotarcia do szerokiego grona odbiorców. W tym obszarze coraz większą rolę odgrywa cyberprzestrzeń i będące jej składową portale społecznościowe, stanowiące doskonałe środowisko do prowadzenia kampanii informacyjnych. Komunikacja strategiczna [7] realizowana jest w takich obszarach jak dyplomacja publiczna, public affairs – komunikacja społeczna, operacje informacyjne, operacje psychologiczne.

Dyplomacja publiczna odpowiada za kreowanie pozytywnego wizerunku państwa poza jego granicami, na drodze działalności informacyjnej i kulturowej, promowaniu wartości i tożsamości historycznej wśród tych wszystkich odbiorców, którzy stanowią społeczność międzynarodową. Public Affairs w swoim przekazie ukierunkowane jest na społeczeństwo wewnętrzne danego państwa, realizowane rozmaitymi narzędziami komunikowania wewnątrzpaństwowego. Z kolei operacje informacyjne mogą posiadać charakter, zarówno ofensywny, jak i defensywny. Działania ofensywne podejmowane są w celu *wpływania na informację i systemy informacyjne przeciwnika przy jednoczesnej ochronie własnej informacji i systemów informacyjnych. Stosowane są we wszystkich fazach operacji, w tym działań militarnych oraz na każdym poziomie wojny* [7]. Działania defensywne są związane z *przedsięwzięciami na rzecz ochrony systemów informacyjnych oraz szeroko rozumianej poprawy komunikacji w płaszczyznach: polityki, procedur, operacji, personelu i technologii, oddziałujących na sprawność zarządzania państwem* [7]. Ostatni element komunikacji strategicznej – *operacje psychologiczne* – związane są z pozyskiwaniem, kreowaniem i pozycjonowaniem informacji, które z dużym prawdopodobieństwem wpłyną na sposób postrzegania rzeczywistości przez odbiorców [7]. Mogą one mieć charakter operacji przeciwko woli narodu, operacji przeciwko decydentom przeciwnika, operacji przeciwko żołnierzom przeciwnika, konfliktu kulturowego.

Na rysunku 1 przedstawiono dwa główne obszary odpowiedzialności bezpieczeństwa informacyjnego.



Pierwszy z nich polega na zapewnieniu bezpieczeństwa informacji w aspekcie zachowania poufności, dostępności i integralności informacji oraz utrzymania funkcjonalności systemów informacyjnych i krytycznych. Drugi obszar związany jest z przeciwstawieniem się dezinformacji i propagandzie, w celu ochrony własnego wizerunku i dbałości o prawdę.

Rys. 1. Obszary odpowiedzialności bezpieczeństwa informacyjnego. Źródło: opracowanie własne.

Bezpieczeństwo informacyjne w zależności od podmiotu, który go realizuje i przyjętych celów działania może mieć wymiar, zarówno pozytywny, jak i negatywny. W wymiarze pozytywnym na pierwszy plan wysuwa się ochrona własnych zasobów informacyjnych i dbałość o wizerunek i prawdę. Tym samym istotnego znaczenia, oprócz ochrony informacji, nabiera komunikacja strategiczna. Oczywiście nie powinniśmy zapominać o działaniach ofensywnych ukierunkowanych na zdobywanie informacji o potencjalnym przeciwniku, przy

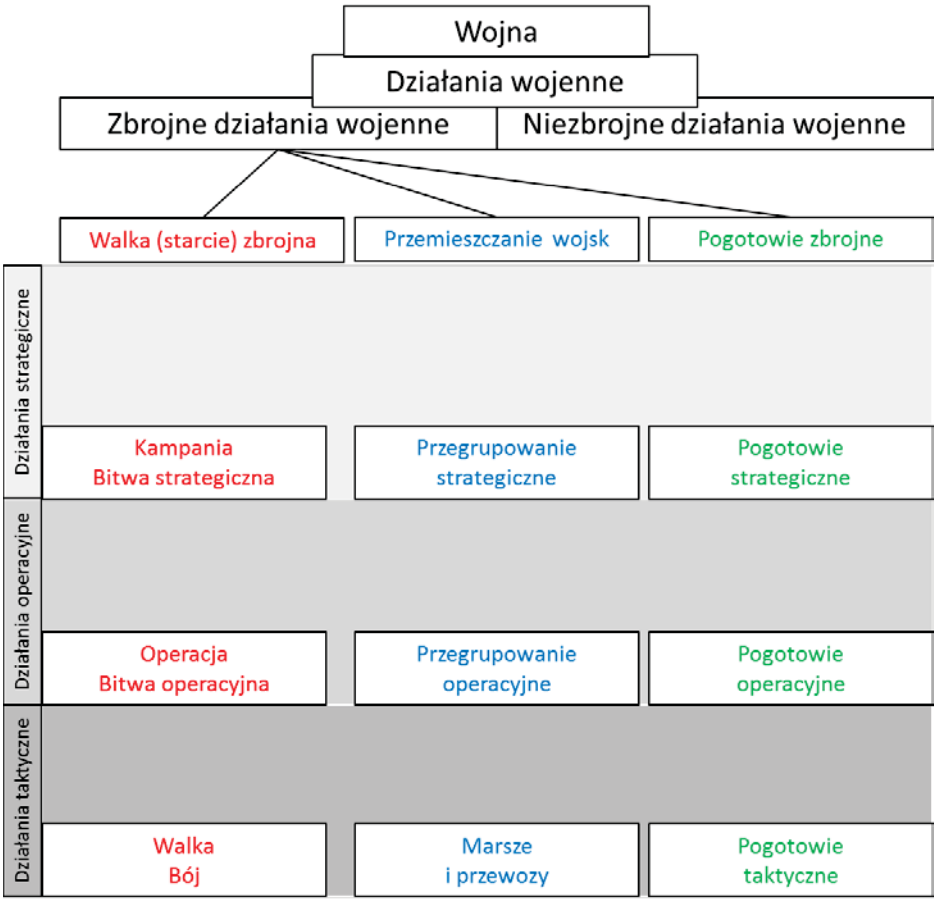
czym rozpoznaje powinno być prowadzone w celu zwiększenia poziomu własnego bezpieczeństwa. Bezpieczeństwo informacyjne w wymiarze negatywnym ukierunkowane jest na zdobywanie informacji o stronie przeciwnej, podyktowane celami agresywnymi, kreowanie rzeczywistości poprzez szerzenie dezinformacji i propagandy, uzupełniona ochroną informacji, która gwarantuje skuteczność dwóch pierwszych obszarów. Tym samym mamy tutaj do czynienia z sytuacją, w której informacja jest istotnym narzędziem oddziaływania na wszystkie podmioty bezpieczeństwa, z ukierunkowaniem w pierwszej kolejności na społeczeństwa i państwa.

4. Poziomy działań w cyberprzestrzeni

Identyfikacja celów działań pozwala nam przejść do określenia poziomów działań w walce w cyberprzestrzeni.

Szczegółowa typologia stosowana w sztuce wojennej wyróżnia trzy poziomy: taktyczny, operacyjny i strategiczny. Na poziomie taktycznym wyróżnia się walkę, pogotowie taktyczne oraz marsze i przewozy. Na poziomie operacyjnym występują operacje, pogotowie operacyjne i przegrupowanie. Natomiast na poziomie strategicznym wymienia się kampanie, przegrupowanie strategiczne i pogotowie strategiczne. Oczywiście podział ten nie jest jedynym sposobem klasyfikacji występującym w literaturze przedmiotu. Niemniej jednak pozwala on na pewną systematykę teorii stuki wojennej. Na rysunku 2. przedstawiono za Stanisławem Koziejem podstawowe kategorie sztuki wojennej. Uwagi wymaga wyodrębnienie *niezbrojnych działań wojennych*, postrzeganych jako polityczna kooperacja negatywna realizowana bez zniszczenia przeciwnika za pomocą siły zbrojnej, często zamiennie określane jako *konflikt niezbrojny* [10]. Inne interpretacje poszczególnych kategorii można zaleźć także w opracowaniach teoretyków walki zbrojnej [2, 5, 15].

Mając na uwadze powyższą klasyfikację niezmierne trudnym zadaniem jest sklasyfikowanie walki w cyberprzestrzeni i przypisanie jej do odpowiedniego poziomu i rodzaju działań. W tym miejscu powinno zadać się pytania: Czy możemy mówić o walce w cyberprzestrzeni, czy być może o walce z wykorzystaniem cyberprzestrzeni? Czy jest to walka wspierana czy wspierająca? Czy nosi ona charakter walki zbrojnej czy też może walki niezbrojnej? Czy walka taka będzie występowała na wszystkich poziomach sztuki wojennej? Jak rozumieć marsze, przewozy, przegrupowanie operacyjne i przegrupowanie strategiczne w środowisku jakim jest cyberprzestrzeń? Jakie elementy będą użyte w pogotowiu strategicznym a jakie w pogotowiu operacyjnym?



Rys. 2. Podstawowe kategorie sztuki wojennej. Źródło: [10].

Patrząc przez pryzmat historii wojen i wojskowości, cyberprzestrzeń stała się kolejnym obszarem walki zbrojnej i zarazem walki niezbrojnej, na równi (jeżeli nie ważniejszym) z lądem, wodą, powietrzem i kosmosem. Co więcej stała ona się kluczowym obiektem oddziaływania w klasycznie pojmowanej walce zbrojnej. Oczywiście można zacytować więcej definicji walki, niemniej jednak ich analiza wskazała cechy wspólne, takie jak: forma zorganizowana, posiadanie sił i środków, dążenie do pokonania przeciwnika. Z tego też względu każdą walkę, w tym walkę w cyberprzestrzeni, należy utożsamiać przez system składający się z elementów wewnętrznych będących ze sobą w odpowiedniej relacji, elementów zewnętrznych znajdujących się w otoczeniu warunkujących funkcjonowanie elementów wewnętrznych (poprzez odpowiednie powiązania zwrotne i relacje), celowość działania. Nie

można w tej walce ograniczać się tylko do cyberprzestrzeni i tylko do obrony. System walki w cyberprzestrzeni musi być integralnym elementem systemu walki sił zbrojnych, zdolnym do działań zarówno defensywnych jak również ofensywnych.

Odwrócę kolejność identyfikacji i w pierwszej kolejności przeanalizuje **strategię**, która przez wielu teoretyków wymieniana jest jako najstarszy dział sztuki wojennej. Jej definicji jest tyle, ilu autorów się nią zajmowało, a jej postrzeganie zmieniało się istotnie na przestrzeni wieków, tak jak zmieniało się postrzeganie sztuki wojennej. Pozwolę sobie na skrócenie całego procesu ewolucji w postrzeganiu i rozumieniu strategii i przedstawienie tego, co jest najważniejsze z punktu widzenia podejmowanych rozważań.

Zacznijmy od klasyków, a mianowicie Sokratesa, który uznał, że *strategia jest dobrodziejstwem bogów, stanowi bowiem dla kraju środek zapewniający mu wolność i szczęście* [6]. Czym zatem jest ten środek, który warunkuje wolność i dobrostan? W ujęciu militarnym to nic innego jak *sposób postepowania w przygotowaniu i prowadzeniu danej konkretnej wojny, kampanii lub bitwy, obrany i zastosowany przez najwyższe ogniwa władzy państwowej, naczelne dowództwo sił zbrojnych lub naczelne dowództwo danego konkretnego teatru działań wojennych* [15]. Takie ujęcie, w warunkach współczesności jest mocno zawężone i nie uwzględnia zmian zachodzących w podejściu do konfliktów i wojen. Jak mówiłem wcześniej zatarte zostały bowiem granice pomiędzy tym, co jeszcze nie jest wojną, a tym co wojną już jest. Zdaniem Andrzeja Polaka *strategia jest badaniem sytuacji politycznej i ogólnych kierunków rozwoju, dla osiągania założonych celów politycznych* [14]. Tym samym to polityka determinuje sposób postepowania, a w obszarze militarnym kierunki rozwoju sił zbrojnych, ich potencjału, sposobów wykorzystania, co zgodne jest z prymatem polityki nad strategią. W ujęciu historycznym strategia związana była tylko z siłami zbrojnymi. W wyniku ewolucji zaczęły przeważać poglądy, że to nie tylko obszar militarny, ale przede wszystkim obszar cywilny podporządkowany polityce państwa. Treści zawarte w strategiach zaczęły uwzględniać pozamilitarne dziedziny aktywności podmiotów bezpieczeństwa jakimi są państwa, a strategia wojskowa (militarna) stała się ich specyficzna częścią [19]. Tym samym, to co dotyczyło przez wieki aspektów militarnych, stało się jedną z wielu części polityki państwa, które jako podmiot strategicznego myślenia kształtuje odpowiednie strategie, podporządkowane obszarom swojej działalności. W tym obszarze na pierwszy plan wysuwa się strategia bezpieczeństwa, czy też strategia bezpieczeństwa narodowego, jako działalność państwa ukierunkowanego na zachowanie i poprawę pożądanego poziomu bezpieczeństwa państwa i obywateli. Oczywiście osiągnięcie oczekiwanego poziomu bezpieczeństwa wymaga aktywności państwa w wielu obszarach, takich jak: gospodarka, ekonomia, oświata, ochrona zdrowia, obrona narodowa i wiele innych. Tym samym w przedmiotowych obszarach działalności

państwa pojawiły się strategie szczegółowe, takie jak: strategia gospodarcza, ekonomiczna, obronna, bezpieczeństwa informacyjnego i inne.

W literaturze przedmiotu często można spotkać się z takimi pojęciami związanymi ze strategią jak: planowanie, zarzadzanie, myślenie strategiczne, kontrola strategiczna czy też polityka strategiczna. Są one związane z ogólną teorią zarzadzania, a ich główny obszar dociekań obejmuje [4]: cele, plany, otoczenie i zmiany. Strategia to także wzorzec lub plan, który powinien integrować główne cele, polityki i sekwencje działań organizacji w jedną spójną całość [11]. W tym ujęciu strategia jest długofalowym określaniem celów, skupieniem uwagi na przyszłości [14], a jej głównym zadaniem jest przygotowanie do zupełnie nowej, przyszłej rzeczywistości. A to wymaga spostrzegawczości, wyobraźni i odwagi [14].

Czym zatem powinna wyrażać się strategia państwa w obszarze skutecznego prowadzenia walki w dobie cyberprzestrzeni? Odpowiedź na powyższe pytanie nie jest prosta i jednoznaczna, niemniej jednak niezwykle istotna. Punktem wyjścia do jej budowania powinny być cele, które państwo przyjęło za priorytetowe, służące maksymalizacji rozwoju gospodarczego, zwiększenia zamożności społeczeństwa, zwiększeniu poziomu bezpieczeństwa i znaczenia państwa na arenie międzynarodowej. Mogą to być cele czysto polityczne, ale również ekonomiczne, społeczne, kulturowe, edukacyjne, militarne i inne. To państwo decyduje, jakie kompetencje są niezbędne, aby powyższe cele realizować. Dodatkowym elementem wpływającym na określenie strategii państwa powinny być zasady, którymi powinno się kierować w rozwoju pożądanych kompetencji. To wszystko powinno być rozłożone w czasie, uwarunkowane własnymi możliwościami i prognozami rozwoju sytuacji, zarówno wewnętrznej, jak i międzynarodowej. Tym samym strategia związana z budowaniem kompetencji państwa do prowadzenia walki w dobie cyberprzestrzeni powinna określić:

- jakie są zagrożenia państwa, zarówno wewnętrze, jak i zewnętrzne?
- czy jesteśmy w stanie przeciwstawić się zidentyfikowanym zagrożeniom?
- jakie są prognozy rozwoju sytuacji, zarówno wewnętrznej, jak i zewnętrznej?
- do czego zmierzamy, co zamierzamy osiągnąć, jakie są nasze cele?
- kiedy zamierzamy to osiągnąć?
- co powinniśmy posiadać, jakie kompetencje budować, aby osiągnąć przyjęte cele?
- jakimi zasadami kierować się przy tworzeniu pożądanych kompetencji?

Odpowiedzi na powyższe pytania powinny uzmysłowić co nam zagraża, w którym kierunku zmierzać, jakie cele realizować, jakimi sposobami je realizować, czym dysponować i kiedy jest to możliwe do osiągniecia. Tym samym uzyskamy odpowiedź w aspekcie polityki

państwa, kształtu systemu bezpieczeństwa narodowego, jej najważniejszych elementów realizujących przyjęte cele działania, roli i zadań sił zbrojnych, w tym wojsk cybernetycznych, zasad którymi powinniśmy się kierować.

Następnym działem sztuki wojennej jest **sztuka operacyjna**. Jej rozwój podyktowany był zmianami w charakterze prowadzonych wojen, a przede wszystkim rozwojem armii masowych i zdolności do przerzutu wojsk. W najprostszym, klasycznym ujęciu strategia zajmowała się doprowadzeniem do bitwy i wykorzystania jej rezultatów, taktyka odpowiadała zaś za sposób jej rozegrania. I takie podejście do prowadzenia wojen funkcjonowało bardzo długo w sztuce wojennej. Dopiero długotrwałość i rozprzestrzenienie geograficzne wojen skutkowało tym, że do zwycięstwa niezbędne było stoczenie wielu bitew, toczonych jedna po drugiej jako ciąg zdarzeń lub też toczonych równocześnie w wielu miejscach, często odległych geograficznie. To zrodziło zjawisko kampanii, następnie operacji postrzeganych jako działania różnych sił, w różnym miejscu i czasie [10]. Taktyka postrzegana przez pryzmat jedności celu, czasu i miejsca przestała wystarczać do osiągnięcia zwycięstwa w wojnie. Tym samym zrodziła się potrzeba opracowania nowego podejścia do rozegrania wojny. W historii wojen możemy dostrzec pojedyncze pierwiastki nowej jakości działań, niemniej jednak dopiero rozwój armii masowych opartych na przymusowym poborze i napoleońska sztuka wojenna w podejściu do ich wykorzystania kojarzone są z rozwojem operacji, określanej w tamtych czasach jako wielka taktyka. Podejście to było rozwijane w wojnach ery ponapoleońskiej toczonych w XIX wieku w Europie i zostało ukształtowane na polach bitewnych I Wojny Światowej. Zaowocowało to powstaniem nowego działu w sztuce wojennej, *sztuki operacyjnej*, ukierunkowanego na prowadzenie operacji. W taktyce i w operacji wspólnym elementem jest jedność celu, odmienne jest zaś podejście do miejsca i czasu. Tak jak w taktyce niezbędna jest także jedność miejsca i czasu do doprowadzenia do starcia zbrojnego z przeciwnikiem, tak w operacji czas i miejsce są rozdzielone, a jego istotą jest manewr. Cytując za Stefanem Mossorem, w *walce zaś rzeczą zasadniczą jest złączenie wszystkich zasobów moralnych, fizycznych i materialnych w celu stworzenia silnego uderzenia, które musi złamać wolę i siłę przeciwnika postawionego w złych warunkach przez manewr dowódcy operacyjnego* [5]. Manewr jest tym elementem, który warunkuje miejsce starcia zbrojnego z przeciwnikiem. Jego przejawem jest zespolenie wysiłku posiadanych sił, rodzajów sił zbrojnych w odpowiednim miejscu i czasie, do wspólnego działania w prowadzonej operacji. W *walce bowiem mamy siłą walczyć o to, co operacyjny dowódca postanowił nieprzyjacielowi wydrzeć. Trzeba się strzec bezpłodnego biegania po polu bitwy, bo każda z bitew, jeżeli ma dać w wyniku nie tylko odwrót, ale klęskę nieprzyjaciela, musi być zakończona aktem siły* [5].

W sztuce operacyjnej oprócz ogólnych podstaw operacyjnych wyróżnia się także sztukę operacyjną poszczególnych rodzajów sił zbrojnych [10]: wojsk lądowych, sił powietrznych, marynarki wojennej, wojsk specjalnych, wojsk obrony terytorialnej. W tym miejscu pozwolę sobie powrócić do pytania, czy wojska cybernetyczne to rodzaj wojsk, czy też może rodzaj sił zbrojnych? Odpowiedź zarówno na pierwszy, jak i na drugi człon pytania może być twierdząca. Wojsk cybernetyczne postrzegane jako rodzaj wojsk muszą posiadać swoją taktykę walki, muszą być zdolne, zarówno do odparcia ataków, jak i do zadawania ciosów. Z drugiej strony, jako rodzaj sił zbrojnych, muszą być zdolne do prowadzenia wspólnych z innymi rodzajami wojsk operacji. Nie można bowiem współcześnie prowadzić operacji bez uwzględnienia cyberprzestrzeni i to nie tylko w wymiarze czysto militarnym, ale także w wymiarze cywilnym. Co więcej, w warunkach pokoju wojska cybernetyczne muszą być zdolne do prowadzenia ciągłego rozpoznania zasobów informacyjnych i infrastruktury krytycznej przeciwnika, rozwoju potencjału rażenia, prowadzenia kampanii informacyjnych, ukierunkowanych na realizację przyjętych w strategii, celów działania. Tym samym mamy do czynienia z pewnym dylematem poznawczym, polegającym na właściwym umiejscowieniu wojsk cybernetycznych w systemie kierowania i dowodzenia sił zbrojnych lub też nawet w systemie bezpieczeństwa narodowego. Prowadzenie operacji wymaga bowiem posiadania dowództwa wojsk cybernetycznych na poziomie operacyjnym, natomiast walka w cyberprzestrzeni wymaga posiadania taktyki wojsk cybernetycznych. Czy zatem zasadnym jest posiadanie dowództwa wojsk cybernetycznych na poziomie operacyjnym, z podporządkowanymi rodzajami wojsk, w tym z wojskami cybernetycznymi? Wydaje się, że tak. Wszak dowództwo na poziomie operacyjnym jest elementem niezbędnym do prowadzenia operacji połączonych. Rodzaje wojsk, nie tylko wojsk cybernetycznych, są niezbędne, aby ten rodzaj sił zbrojnych mógł funkcjonować. Trzeba go bowiem utrzymywać, zasilać, szkolić, chronić. A do tego niezbędne są wyspecjalizowane rodzaje wojsk. Co więcej, należy się zastanowić, czy w szeroko pojmowanych wojskach cybernetycznych nie powinno być także specjalizacji związanej z samą walką w cyberprzestrzeni (obroną i atakiem), rozpoznaniem w cyberprzestrzeni, prowadzeniem i zwalczaniem kampanii informacyjnych w cyberprzestrzeni.

Taktyka, postrzegana jest jako *metoda postepowania, umiejętność używania rozporządzalnych sił dla osiągnięcia zamierzonych celów* [8]. To także *sposób, metoda postepowania, mająca doprowadzić do osiągnięcia zamierzonego celu; działanie według obmyślonego planu* [17]. Taktyka ewoluowała wraz z rozwojem sztuki wojennej. W ujęciu czysto wojskowym taktyka definiowana jest najczęściej jako teoria i praktyka walki – teoria i praktyka działań taktycznych (bojowych) [10]. Jest niczym innym jak sztuką użycia wojsk w tym punkcie,

do którego przybędą [10]. Początkowo taktyka dotyczyła sposobów rozegrania bitwy bez rozróżnienia na rodzaje formacji, które był w niej wykorzystywana. Była to taktyka jednorodna, skupiająca się w swej istocie na umiejętności uszykowania wojsk na polu bitwy. Wraz ze zmianami na polu walki, złożonością zjawiska wojny, zwiększało się znaczenie taktyki, która wraz z pojawieniem się specjalizacji ewoluowała w stronę taktyki rodzajów wojsk, kierujących się swoimi odmiennymi sposobami prowadzenia działań bojowych. W wyniku dalszej ewolucji i potrzeby współdziałania rodzajów wojsk na polu walki pojawiła się konieczność opracowania działań wspólnych, określonych jako działania broni połączonych. Tym samym zapoczątkowany został nowy dział taktyki określany jako taktyka ogólna obejmująca swoim zasięgiem działania oddziałów i związków taktycznych, będącymi formacjami broni połączonych. Także wojska cybernetyczne, jako swoisty nowy rodzaj wojsk, powinny mieć swoją taktykę rodzajów wojsk, wpisującą się w taktykę ogólną, zgodnie z zasadą synergii.

Jaka zatem powinna być taktyka prowadzenia walki w specyficznym środowisku jakim jest cyberprzestrzeń? W taktyce występuje jedność celu, czasu i miejsca działania, a punktem wyjścia są siły i środki jakim się dysponuje [5]. Tym samym taktyka zawiera się w określeniu zadań dla sił jakim się dysponuje. Jakimi zatem siłami zdolnymi do prowadzenia walki w cyberprzestrzeni powinniśmy dysponować? Odpowiedź na powyższe pytanie powinna wynikać ze strategii budowania zdolności państwa do prowadzenia działań w cyberprzestrzeni. To przyjęta strategia powinna określić kształt wojsk cybernetycznych, ich przeznaczenie i umiejscowienie w systemie bezpieczeństwa narodowego. Taktyka wojsk cybernetycznych będzie tylko pochodną strategii, umożliwiającą realizację określonych w strategii celów funkcjonowania i rozwoju państwa (organizacji). Podkreślę jednocześnie, że nie można odnieść sukcesu bez budowania zdolności ofensywnych, spostrzegawczości, wyobraźni i odwagi.

5. Zakończenie

Kończąc rozważania pozwolę sobie na krótkie podsumowanie. Walka w cyberprzestrzeni jest tą częścią sztuki wojennej, jeżeli w ogóle nią jest, która nie doczekała się jak dotychczas jakiegokolwiek opracowania teoretycznego. Są wprawdzie doktryny, ale one nie mają nic wspólnego z teorią. Wszyscy piszą o zagrożeniach w cyberprzestrzeni, o bezpieczeństwie cyberprzestrzeni lub w cyberprzestrzeni, o wojnie w cyberprzestrzeni lub wojnie cybernetycznej, lecz tylko nieliczni próbują opisać jak taką walkę prowadzić, jakimi zasadami się kierować, jakie cele realizować i w końcu jakimi siłami walczyć. Wyrażam przekonanie, że przedstawione rozważania uświadomią czytelnikom z jak złożonym zjawiskiem mamy

do czynienia, jak dużo jest niewiadomych i jak wiele problemów do rozwiązania jeszcze pozostało.

6. Bibliografia

1. Bojarski W., Podstawy analizy i inżynierii systemów, Państwowe Wydawnictwo Naukowe, Warszawa 1984.
2. Clausewitz C., O wojnie, Wydawnictwo Test, Lublin 1995.
3. Fehler W., Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i prawne, Wydawnictwo Arte, Warszawa 2012.
4. Marchesnay M., Zarzadzanie strategiczne, Poltext, Warszawa 1994.
5. Mossor S., Sztuka wojenna w warunkach nowoczesnej wojny, Wydawnictwo Ministerstwa Obrony Narodowej, Warszawa 1986.
6. Nowakowski Z., Szafran H., Szafran R., Bezpieczeństwo w XXI wieku. Strategia bezpieczeństwa narodowego Polski i wybranych państw, Towarzystwo Naukowe Powszechne, Rzeszów 2009.
7. Nowicka J., Załoga W., Ciekanowski Z., Komunikacja strategiczna w naukach o zarządzaniu i jakości oraz w naukach o bezpieczeństwie, Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w 7Katowicach, Nr 1(14)/2018.
8. Kopaliński W., Słownik wyrazów obcych i zwrotów obcojęzycznych, Wiedza Powszechna, Warszawa 1985.
9. Kotarbiński T., Traktat o dobrej robocie, Zakład Narodowy im. Ossolińskich, Wydawnictwo Polskiej Akademii Nauk, Wrocław-Warszawa-Kraków 1965.
10. Koziej S., Teoria sztuki wojennej, Bellona, Warszawa 1993.
11. Koźmiński A., Zarzadzanie w warunkach niepewności, Państwowe Wydawnictwo Naukowe, Warszawa 2004
12. PN-I-02000:2002 Technika Informatyczna – Zabezpieczenie w systemach informatycznych – Terminologia, Polski Komitet Normalizacyjny, Warszawa 2002.
13. Polak A. (red), Sztuka wojenna, Akademia Obrony Narodowej, Warszawa 2014.
14. Polak A., Sztuka wojenna. Kontekst teoretyczny i praktyczny, Zeszyty Naukowe Akademii Obrony Narodowej nr 3/2013.
15. Skibiński F, Rozważania o sztuce wojennej, Wojskowy Instytut Historyczny, Warszawa 1972.
16. Słownik języka polskiego, t. 1., Państwowe Wydawnictwo Naukowe, Warszawa 1978.
17. Słownik wyrazów obcych, Państwowe Wydawnictwo Naukowe, Warszawa 1991.

18. Sułek M., Trzy działy prakseologii, Rocznik Naukowy Wydziału Zarzadzania w Ciechanowie Wyższej Szkoły Menadżerskiej w Warszawie, z. 1-2, t. II, Ciechanów 2008, publikacja na stronie www.mises.pl. [11.09.2019 r.]
19. Wiatr M., Między strategia a taktyką, Wydawnictwo Adam Marszałek, Toruń 1999.

ABSTRACT

MILITARY ACTION IN CYBERSPACE – CLASSIFICATION ATTEMPT

Summary: The chapter presents an attempt to classify military activities in cyberspace. The starting point was to define the purpose of these activities, aimed at the effectiveness of impact in terms of time, cost and degree of achievement of the goal. Additionally, protective and defense activities related to the broadly understood information security are presented, as well as the classification of levels of activities in cyberspace, taking as a starting point the classic divi-sion into strategic, operational and tactical activities.

Keywords: cyberspace, cyber conflict, combat theory, cyberspace security.

ROZDZIAŁ 2

ROLA ISAC W KONTEKŚCIE PROJEKTU NOWELIZACJI USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA Z DNIA 16 LUTEGO 2021 R.

dr Jarosław BIEGAŃSKI [3]

STRESZCZENIE: Niniejszy rozdział przedstawia rolę ISAC w kontekście projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa z dnia 16 lutego 2021 r. Opisano w nim genezę powstania ISAC jako centrów wymiany i analizy informacji o zagrożeniach, podatnościach i incydentach. Wskazując na potrzebę tworzenia ISAC zwrócono uwagę na fakt, że organizacje ISAC stanowić powinny ważny element systemu cyberbezpieczeństwa. Proponowane w projekcie nowelizacji ustawy ograniczenie funkcji ISAC wyłącznie do wspierania enumeratywnie wymienionych podmiotów krajowego systemu cyberbezpieczeństwa może stać się przyczyną dylematów interpretacyjnych odnoszących się do tego, jak w praktyce ośrodki ISAC będą mogły realizować swoje funkcje, w sytuacji, gdy zwróci się do nich podmiot, który nie został zakwalifikowany do krajowego systemu cyberbezpieczeństwa oraz gdy ISAC nie zostaną wyposażone w uprawnienia do przetwarzania informacji mogących stanowić tajemnice prawnie chronione.

SŁOWA KLUCZOWE: cyberbezpieczeństwo, ISAC, UKSC, NIS 2.

Różnorodność i powszechność zagrożeń występujących w cyberprzestrzeni na przełomie XX i XXI wieku wskazały na potrzebę współpracy podmiotów działających na rzecz

[3] Doradca Zarządu ZBP w Zespole Bezpieczeństwa Banków, Wyższa Szkoła Bankowa w Poznaniu, jaroslaw.bieganski@wsb.poznan.pl, ORCID: 0000-0002-4689-5909.

cyberbezpieczeństwa. Idea tworzenia ośrodków kompetencji, wspierających wymianę informacji w celu wzmacniania wspólnej odporności na zagrożenia płynące z cyberprzestrzeni, znalazła swój wyraz w inicjatywie amerykańskiego sektora prywatnego, który zareagował na prezydencką dyrektywę PDD63 z 1998 roku i zaczął się dobrowolnie samoorganizować, tworząc ośrodki wymiany informacji o incydentach, cyberzagrożeniach i podatnościach, tzw. centra ISAC[4]. Po atakach terrorystycznych z 11 września 2001 r. misja ISAC została rozszerzona o zagadnienia związane z ochroną fizyczną. Działania amerykańskich ISAC początkowo koncentrowały się na wymianie informacji wewnątrz poszczególnych sektorów gospodarki. Przykładowo powstały organizacje ISAC zrzeszające podmioty z branży lotniczej, przemysłu energetycznego, przemysłu wydobywczego, usług finansowych, ochrony zdrowia, czy branży IT. Od początku XXI wieku amerykańskie organizacje ISAC zaczęły wychodzić poza współpracę w ramach jednego sektora gospodarki, ustanawiając w roku 2003 Narodową Radę ISAC[5], promującą wymianę informacji o wspólnych, międzysektorowych zagrożeniach i podatnościach[6].

Idea tworzenia ISAC znalazła swoje odzwierciedlenie w Europie. ENISA, europejska agencja ds. cyberbezpieczeństwa, zaangażowała się w promowanie modelu współpracy międzysektorowej i transgranicznej bazującej na tworzeniu krajowych, sektorowych i paneuropejskich organizacji ISAC[7]. Także Komisja Europejska w projekcie Dyrektywy NIS 2 wzmocniła przekaz o konieczności wymiany informacji, wyjaśniając w uzasadnieniu do projektu z grudnia 2020 r., że preferowany wariant wzmocnienia cyberodporności zakłada ustanowienie jasnych mechanizmów mających na celu zwiększanie zaufania wśród państw członkowskich oraz pomiędzy instytucjami sektora publicznego i prywatnego, zachęcających do dzielenia się informacjami oraz do zapewnienia bardziej operacyjnego podejścia opartego

[4] ISAC – Information Sharing & Analysis Centre – centrum wymiany i analizy informacji.
[5] NCI – National Council of ISACs, zob. https://1d74b95c-e5fa-4920-9b2e-254ec35a1c46.filesusr.com/ugd/651d24_63716f50586e4ec99c45c4dea8f9ed66.pdf; dostęp 31.03.2021.
[6] Zob. https://www.nationalisacs.org/publications; dostęp 21.01.2021.
[7] Zob. ENISA'S OPINION PAPER ON ISAC COOPERATION, źródło: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-isac-cooperation; dostęp 21.01.2021.

na wzajemnej pomocy i wzajemnej weryfikacji[8]. Na wzajemnym zaufaniu i wymianie informacji o zagrożeniach opiera się także globalna współpraca sektora finansowego na rzecz ograniczania cyberryzyka, rozwijana w ramach działającego na świecie, w tym także w Europie, ISAC sektora finansowego: *Financial Services Information Sharing and Analysis Center* (FS-ISAC), budującego kulturę wymiany informacji i dobrych praktyk w zakresie współpracy i pomocy przy koordynacji reakcji na incydenty cyberbezpieczeństwa[9].

Idąc tym śladem także polski ustawodawca podjął działania zmierzające do sformalizowania i udzielenia publicznego wsparcia dla idei tworzenia ośrodków wymiany i analiz informacji o zagrożeniach i podatnościach związanych z funkcjonowaniem życia gospodarczego i społecznego w cyberprzestrzeni, proponując dodanie adekwatnych zapisów w dotychczas obowiązującej ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

Projekt zmiany ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne z dnia 16 lutego 2021 r. (zwany dalej projektem ustawy) stanowi, że w art. 2 po pkt 3 między innymi dodaje się pkt 3b) wprowadzający legalną definicję ISAC jako ***centrum wymiany i analizy informacji na temat podatności, cyberzagrożeń i incydentów funkcjonujące w celu wspierania podmiotów krajowego systemu cyberbezpieczeństwa***[10]. Zadania ISAC wskazano w projektowanym Rozdziale 5a w artykule 25a. 1. w otwartym katalogu. Będą to: *wymiana informacji, dobrych praktyk i doświadczeń dotyczących cyberzagrożeń, podatności oraz incydentów*. Dalej dodano przepisy odnośnie prowadzenia wykazu ISAC, wpisu do niego oraz wykreślenia. Wpis do wykazu ma odbywać się po uzyskaniu opinii organów właściwych do spraw cyberbezpieczeństwa. ISAC ma współpracować z zespołami

[8] Zob. Komisja Europejska, Uzasadnienie do projektu Dyrektywy NIS 2 z 16 grudnia 2020, s.8 źródło: https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0010.02/DOC_1&format=PDF; dostęp 2.04.2021.

[9] Zob. FS-ISAC, What we do: Resilience; źródło: https://www.fsisac.com/what-we-do/resilience; dostęp 30.11.2020.

[10] Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa z 16 lutego 2021 r.; źródło: https://legislacja.gov.pl/docs//2/12337950/12716624/12716625/dokument490917.pdf; dostęp 31.03.2021.

CSIRT poziomu krajowego[11]. Uzasadniono, że centra ISAC pozwolą na wsparcie merytoryczne personelu podmiotów krajowego systemu cyberbezpieczeństwa[12].

Z treści proponowanych w projekcie ustawy zapisów oraz ich uzasadnienia wynika, że projektodawca zaproponował utworzenie nowego rodzaju podmiotu – **ISAC**, którego funkcjonowanie dotychczas nie było uregulowane w akcie prawnym rangi ustawy. W kontekście przytoczonej powyżej propozycji stwierdzić należy, że w proponowanym brzmieniu treść przepisu nie oddaje w pełni idei tworzenia ISAC, ponieważ projekt ustawy zakłada utworzenie ISAC jedynie w celu wspierania **podmiotów krajowego systemu cyberbezpieczeństwa**. Projekt ustawy ogranicza zatem funkcje ISAC do wspierania enumeratywnie (*numerus clausus* – katalog zamknięty) wymienionych podmiotów systemu cyberbezpieczeństwa, o których mowa w art. 4 ustawy o krajowym systemie cyberbezpieczeństwa. *W* uzasadnieniu do projektu ustawy podano: *Krajowy system cyberbezpieczeństwa składa się z wielu podmiotów. Przede wszystkim są to operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, na które nałożono obowiązki związane z zapewnieniem bezpieczeństwa systemów informacyjnych, utrzymania niezakłóconego świadczenia usług, a także zgłaszania i obsługi incydentów bezpieczeństwa. Operatorzy usług kluczowych zostali podzieleni według sektorów i podsektorów, które zostały wskazane w załączniku nr 1 do ustawy. Ustawa określa 6 kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa sektorów gospodarki tj.: energii, transportu, zdrowia, bankowości i infrastruktury rynków finansowych, zaopatrzenia w wodę oraz infrastruktury cyfrowej. Dla każdego sektora ustanowiono organ właściwy do spraw cyberbezpieczeństwa (zwany dalej „organem właściwym"), który odpowiada za wyznaczanie operatorów oraz nadzór i kontrolę nad przestrzeganiem przepisów ustawy w danym sektorze. Obecnie w krajowym systemie cyberbezpieczeństwa nie znajdują się przedsiębiorcy telekomunikacyjni, ani dostawcy usług zaufania*[13].

Dalej w uzasadnieniu projektu wyjaśniono: *Pierwsze ISAC powstały w Stanach Zjednoczonych pod koniec lat dziewięćdziesiątych XX wieku. ISAC gromadzi informacje o podatnościach i cyberzagrożeniach, a następnie przekazuje te informacje oraz zestawy dobrych praktyk do podmiotów, które uczestniczą w tym systemie. Taka formuła znacząco wpływa*

[11] Zob. tamże s. 66.
[12] Zob. tamże s. 58.
[13] Tamże, s. 93.

na poprawę cyberbezpieczeństwa i jest praktykowana w państwach Unii Europejskiej. Wskazane jest, aby więcej takich organizacji powstało w Polsce. Zdaniem ENISA dla prawidłowego rozwoju cyberbezpieczeństwa niezbędna jest współpraca pomiędzy sektorem publicznym i prywatnym. Centra ISAC stanowią platformę takiej współpracy poprzez wymianę informacji na temat przyczyn, incydentów, cyberzagrożeń, jak również dzielenie się doświadczeniem, wiedzą i analizami. Akt o cyberbezpieczeństwie zachęca do tworzenia ISAC. Co więcej, jednym z obowiązków nałożonych na ENISA jest konieczność wspierania działań mających na celu wymianę informacji w ramach sektorów. Przykładem sektorowego ISAC na poziomie europejskim jest European Energy Information Sharing & Analysis Centre (EE ISAC). Został zorganizowany z inicjatywy przemysłu energetycznego. W ramach EE ISAC wymieniają informacje ***dostawcy usług, przedsiębiorstwa użyteczności publicznej, instytucje naukowe, organizacje rządowe i pozarządowe*** *(m. in. członkiem EE ISAC jest Polskie Sieci Elektroenergetyczne Spółka Akcyjna)*[14].

Zacytowane wyżej intencje ustawodawcy wskazują na sięgnięcie do amerykańskiego wzorca tworzenia ośrodków wymiany informacji i analiz tzw. *Information Sharing & Analysis Centre* (ISAC). Szukając zatem prawidłowego odniesienia dla stosowania idei ISAC warto przyjrzeć się funkcjom jakie spełniają ośrodki wymiany i analizy informacji na rynku, który powołał organizacje ISAC do życia.

Amerykański Narodowy Instytut Standardów i Technologii (NIST) wskazuje ISAC jako ważne zewnętrzne źródło informacji o zagrożeniach, które należy brać pod uwagę podczas analizy ryzyka bezpieczeństwa informacji danej organizacji[15]. Szukając dobrych praktyk wykorzystania ISAC należy sięgnąć do przykładów, którymi podzieliło się we wrześniu 2015 roku, działające przy NIST, *Computer Security Resource Center* w analizie dotyczącej studiów przypadków[16], wykonanej pod auspicjami amerykańskiej Narodowej Rady ISAC (ang. NCI - *National Council of ISACs*). Przedmiotowa analiza wskazuje na szczególną wartość ISAC w kontekście współpracy międzysektorowej, której wzmocnienie zwłaszcza w sektorach, które nie utworzyły swoich ISAC obrała sobie za cel amerykańska Narodowa Rada

[14] Tamże, s. 49-50.
[15] Zob. NIST, Guide for Conducting Risk Assessments, s. 27-28; źródło: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf; dostęp 14.12.2020.
[16] Zob. Case Studies in ISAC Information Sharing, źródło: https://csrc.nist.gov/CSRC/media/Presentations/Case-Studies-in-ISAC-Information-Sharing/images-media/day1_info-sharing_430-530.pdf; dostęp 14.12.2020.

ISAC[17]. Ta organizacja podała, że w ramach współpracy międzysektorowej szczególną wartość ma dzielenie się informacjami dotyczącymi między innymi: stron ze złośliwym oprogramowaniem, podatności oprogramowania, aktorami i celami ataków, metodami analizy i postępowania z ryzykiem, sposobami reagowania na incydenty, w tym pomoc w rozwiązywaniu sytuacji kryzysowych[18].

Biorąc powyższe pod uwagę można sformułować wniosek, że amerykańska praktyka tworzenia ISAC wyszła poza przestrzeń działania podmiotów krajowego systemu cyberbezpieczeństwa w rozumieniu projektu polskiej ustawy. Dlatego na gruncie polskiego prawa **zasadnym byłoby wskazanie możliwości objęcia współpracą w ramach ISAC także innych podmiotów niż wyłącznie skatalogowane w art. 4 ustawy o krajowym systemie cyberbezpieczeństwa.** Na potrzebę taką zwrócił uwagę Związek Banków Polskich proponując, aby ISAC wspomagał podmioty z danego sektora, sektorów lub podsektorów niezależnie od wydania decyzji o uznaniu za operatora usługi kluczowej, co zdaniem ZBP powinno zapewnić szczelność systemu[19]. *Szczególnym przypadkiem jest tutaj sektor bankowy, w którym bezpieczeństwo jednego banku zależy również od innych podmiotów – pozostałych banków, dostawców usług płatniczych, izb rozliczeniowych itd.*[20]

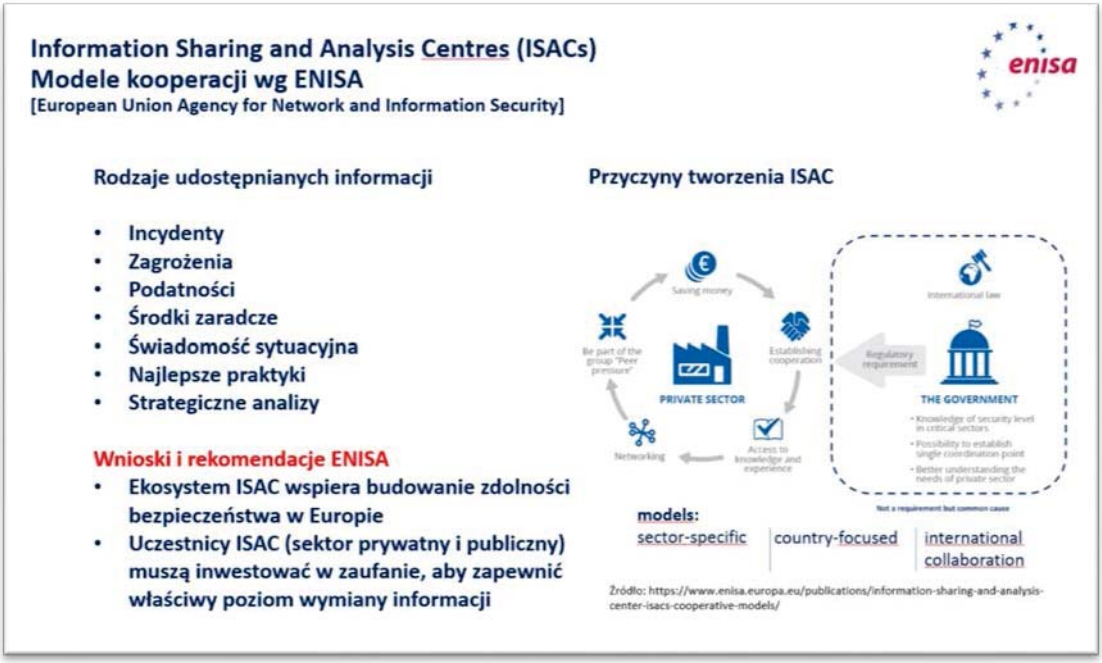
Pomimo, że legalna definicja ISAC zgodnie z jej projektowanym brzmieniem ustanowi ograniczenia działalności ISAC wyłącznie do wspierania podmiotów krajowego systemu cyberbezpieczeństwa, to w uzasadnieniu do projektu nowelizacji ustawy z lutego 2021 umieszczono wyjaśnienie, że rozdział 5a dotyczy ISAC funkcjonujących w ramach krajowego systemu cyberbezpieczeństwa. Zdaniem projektodawcy: *Nic nie stało do tej pory na przeszkodzie, aby były tworzone podmioty na wzór ISAC, na zasadach ogólnych – na przykład w formie stowarzyszeń, fundacji. Nowelizacja tego nie zmienia, daje jedynie możliwość funkcjonowania ISAC w ramach krajowego systemu cyberbezpieczeństwa*[21]. Takie wyjaśnienie nadal budzi wątpliwości co do zakresu działalności ISAC, który z jednej strony ma wspierać enumeratywnie wymienione podmioty krajowego systemu cyberbezpieczeństwa i jednocześnie z drugiej

[17] Zob. tamże, s. 11-12.
[18] Zob. tamże 11,12,18.
[19] Pismo ZBP z dnia 22.09.2020 do Ministra Cyfryzacji; plik Uwagi - ZBP.pdf; s.1, tabela s.1; źródło: https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html; dostęp 14.12.2020.
[20] Tamże s. 4.
[21] Projekt nowelizacji ustawy, tamże s. 66.

strony chciałby pozostać centrum wymiany informacji o zagrożeniach, podatnościach i incydentach dla innych podmiotów, które nie zostały zaliczone do krajowego systemu cyberbepieczeństwa (np. dla ISAC sektora bankowego w grupie podmiotów wymagających wsparcia poza krajowym systemem cyberbezpieczeństwa mogą znaleźć się banki spółdzielcze). Stawia to przed ISAC praktyczne wyzwania, jak rozdzielić wsparcie dla podmiotów krajowego systemu cyberbezpieczeństwa od innej aktywności ISAC, która nie będzie elementem krajowego systemu cyberbezpieczeństwa. Rozwiązaniem problemu związanego z interpretacją kogo ISAC może wspierać mogłoby być uzupełnienie definicji ISAC o zwrot „w szczególności", dający możliwość zastosowania katalogu otwartego wspieranych podmiotów, w takim przypadku ustawowa definicja ISAC mogłaby przyjąć postać: ISAC - centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów funkcjonujące w **szczególności** w celu wspierania, podmiotów krajowego systemu cyberbezpieczeństwa. Takie rozwiązanie w bardziej trafny sposób oddałoby intencję ustawodawcy wyrażoną w uzasadnieniu w postaci zdania: *Zostanie dodany nowy rodzaj podmiotu – ISAC – który umożliwi nawet niewielkim a wyspecjalizowanym podmiotom na dołączenie się do krajowego systemu cyberbezpieczeństwa*[22].

Logiczną konsekwencją idei tworzenia i współpracy wielu ISAC powinno być także formalne nadanie organizacjom ISAC uprawnienia do przetwarzania informacji prawnie chronionych. Brak takiej ustawowej legitymacji w analizowanym projekcie nowelizacji ustawy może znacząco ograniczyć funkcjonalność i skuteczność ISAC w zakresie wymiany informacji o zagrożeniach i incydentach, w szczególności, gdy incydent może dotyczyć wielu ISAC z różnych sektorów. Przykładowo funkcjonalność ISAC ograniczy sytuacja, kiedy konieczna stanie się wymiana informacji z sektora medycznego, finansowego i transportu w przypadku hipotetycznego incydentu zagrożenia życia spowodowanego przez terrorystę, który dokonał zakupu biletu lotniczego z wykorzystaniem karty płatniczej wydanej na osobę, której tożsamość została skradziona w wyniku włamania do bazy pacjentów szpitala.

[22] Tamże s. 97.



Rys. 1. Modele kooperacji ISAC wg ENISA.Źródło: opracowanie własne na podstawie ENISA, Information Sharing and Analysis Center (ISACs) - Cooperative models.

Na szerszy kontekst działalności ISAC zwróciła także uwagę w swojej analizie modelów kooperacji Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)[23] (zob. rys.1). ENISA wskazała, że specyfika europejska tworzenia ISAC różni się od amerykańskiej. W raporcie ENISA wyjaśniła, że wiąże się to z różnicami kulturowymi - o ile w USA biznes powinien sam o siebie zadbać, o tyle w Europie oczekuje się zaangażowania państwa w ochronę cyberprzestrzeni i prowadzonej tam działalności gospodarczej[24]. Według analizy dokonanej przez ENISA europejskie ISAC koncentrują się na budowaniu partnerstwa i zaufania między członkami. Są one bardzo ukierunkowane na branżę, ale istnieje również mocne oczekiwanie na wsparcie ze strony sektora publicznego - nie w zakresie finansowania, ale raczej ułatwiania

[23] Zob. ENISA, Information Sharing and Analysis Center (ISACs) - Cooperative models, źródło: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/; dostęp 17.12.2020.
[24] Zob. tamże s. 16.

funkcji (sekretariat) i oferowania specjalistycznej wiedzy (walka z cyberprzestępczością, dzielenie się informacjami istotnymi dla branży). Udział organów rządowych zapewnia ISAC większą formalność, potwierdza poszanowanie potrzeb sektora prywatnego przez sektor publiczny i wspiera go w stawianiu czoła nowym wyzwaniom regulacyjnym (np. implementacja wymagań dyrektywy NIS, czy też pomoc we wdrożeniu RODO)[25]. W konkluzji raportu ENISA podkreśliła, że ekosystem ISAC wspiera budowanie zdolności bezpieczeństwa w Europie oraz, że uczestnicy ISAC (sektor prywatny i publiczny) muszą inwestować w **zaufanie**, aby zapewnić właściwy poziom wymiany informacji. Ponadto ENISA podała, że sektor prywatny w badaniu opinii opowiedział się za budowaniem partnerstw transgranicznych (międzynarodowe ISAC) w celu wymiany informacji o zagrożeniach w całej Europie[26].

Podsumowanie

Konkludując analizę dotyczącą zasadności i funkcjonalności proponowanych przepisów nowelizujących ustawę o krajowym systemie cyberbezpieczeństwa odnośnie sformalizowania istnienia **ISAC** jako centrów wymiany i analiz informacji o incydentach, zagrożeniach i podatnościach należy wziąć pod uwagę kontekst istnienia ISAC jako ważnego elementu systemu cyberbezpieczeństwa. Z tego kontekstu wynika **potrzeba tworzenia ISAC jako ośrodków kompetencji wspierających cały system cyberbezpieczeństwa**, bez ograniczania aktywności ISAC jedynie do wspierania podmiotów wyliczonych w zamkniętym katalogu, o którym mowa w art. 4 projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.

W uzupełnieniu należy podkreślić, że istotne dla prawidłowego wypełniania swoich ról przez sektorowe, krajowe i międzynarodowe organizacje ISAC będzie zapewnienie organizacjom ISAC adekwatnych uprawnień dla przetwarzania informacji mogących stanowić tajemnicę prawnie chronioną. Dlatego formalnemu usankcjonowaniu istnienia organizacji ISAC powinno towarzyszyć **utworzenie legalnych mechanizmów dostępu oraz uprawnienia do przetwarzania informacji mogących stanowić tajemnicę prawnie chronioną** i to zarówno w ramach jednego sektora, jak również pomiędzy organizacjami ISAC różnych sektorów, w tym także w ramach współpracy międzynarodowej.

---

[25] Zob. tamże s. 16.
[26] Zob. tamże s. 38.

Literatura

1. Case Studies in ISAC Information Sharing, https://csrc.nist.gov/CSRC/media/Presentations/Case-Studies-in-ISAC-Information-Sharing/images-media/day1_info-sharing_430-530.pdf
2. ENISA's opinion paper on ISAC cooperation, https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisas-opinion-paper-on-isac-cooperation
3. FS-ISAC, What we do: Resilience, https://www.fsisac.com/what-we-do/resilience
4. https://www.nationalisacs.org/publications
5. Information Sharing and Analysis Center (ISACs) - Cooperative models, ENISA, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/
6. National Council of ISACs, https://1d74b95c-e5fa-4920-9b2e-254ec35a1c46.filesusr.com/ugd/651d24_63716f50586e4ec99c45c4dea8f9ed66.pdf
7. NIST, Guide for Conducting Risk Assessments, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
8. Pismo ZBP z dnia 22.09.2020 do Ministra Cyfryzacji; https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html
9. Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa z 16 lutego 2021 r., https://legislacja.gov.pl/docs//2/12337950/12716624/12716625/dokument490917.pdf
10. Uzasadnienie do projektu Dyrektywy NIS 2 z 16 grudnia 2020, Komisja Europejska, https://eur-lex.europa.eu/resource.html?uri=cellar:be0b5038-3fa8-11eb-b27b-01aa75ed71a1.0010.02/DOC_1&format=PDF

ABSTRACT

THE ISAC ROLE IN THE CONTEXT OF THE DRAFT AMENDMENT TO THE NATIONAL CYBER SECURITY SYSTEM ACT OF FEBRUARY 16, 2021.

Summary: This chapter deals with the role of ISAC in the context of the draft amendment to the Polish act on the national cybersecurity system of February 16, 2021. The genesis of ISAC as Information Sharing & Analysis Centre on threats, vulnerabilities and incidents is described. While pointing to the need to establish ISAC, attention was drawn to the fact that

ISAC organizations should constitute an important element of the cybersecurity system. The limitation of the ISAC functions proposed in the draft amendment to the act only to support the enumerated entities of the national cybersecurity system may cause interpretation dilemmas how in practice ISAC centres will be able to perform their functions if they are approached by an entity that does not has been classified for the national cybersecurity system and when ISAC is not provided with the power to process information that may constitute legally protected secrets.

Keywords: cybersecurity, ISAC, Polish Act on the Cybersecurity System (UKSC), NIS 2.

ROZDZIAŁ 3

ZARZĄDZANIE OCHRONĄ INFORMACJI STERUJĄCEJ W SIECIACH I SYSTEMACH PRZEMYSŁOWYCH

dr inż. Krzysztof LIDERMAN [27]

STRESZCZENIE: W rozdziale przedstawiono zagadnienia bezpieczeństwa sieci i systemów przemysłowych związane z ochroną danych produkcyjnych oraz informacji sterującej (nie tylko) procesami produkcyjnymi. Po zwięzłym przeglądzie typów sieci i systemów przemysłowych, ze szczególnym zaakcentowaniem właściwości systemów czasu rzeczywistego, krótko scharakteryzowano podstawowe dla tego obszaru problemowego normy i standardy: IEC 61508, IEC 62443, NIST SP 800-82 i NIST 800-53. Przedstawiono także zbiory „dobrych praktyk" wskazanych przez NERC oraz Bundesamt für Sichercheit in der Informationstechnik. Na tej podstawie opracowano zamieszczony na końcu rozdziału zbiór dobrych praktyk dotyczących zarządzania ochroną informacji sterującej w sieciach i systemach przemysłowych.

SŁOWA KLUCZOWE: systemy i sieci przemysłowe, bezpieczeństwo przemysłowych sieci sterowania, SCADA, IEC 61508, IEC 62443, NIST SP 800-82.

[27] Wojskowa Akademia Techniczna, Wydział Cybernetyki, Instytut Teleinformatyki i Cyberbezpieczeństwa, krzysztof.liderman@wat.edu.pl, ORCID: 0000-0002-0004-5095.

1. Wstęp

Eksploatowane we współczesnych organizacjach i, ujmując problem szerzej, infrastrukturze państwowej systemy: transportowe, komunikacyjne, magazynowe i produkcyjne, muszą być *nadzorowane* oraz w części przypadków, dotyczy to głównie systemów produkcji, *sterowane*. Zadania te są realizowane za pomocą przemysłowych systemów sterowania, na które składają się, m.in. sieci SCADA (ang. *Supervisory Control And Data Acquisition*), DCS (ang. *Distributed Control Systems*) oraz ich elementy składowe w postaci sterowników programowalnych PLC (ang. *Programmable Logic Controllers*).

Przemysłowe systemy sterowania (ang. *Industrial Control System* – ICS)[28] rozwijały się w zasadzie oddzielnie od teleinformatycznych (biurowych) sieci komputerowych. To oddzielenie, brak połączeń pomiędzy różnymi ICS, stosowanie specjalizowanego sprzętu i protokołów, wydzielonych kanałów komunikacyjnych oraz zwykle dobra ochrona fizyczna centrów sterowania powodowało, że problemy nękające biurowe sieci informatyczne związane z działaniami różnego rodzaju intruzów, możliwościami propagacji niekorzystnych efektów pomiędzy różnymi, połączonymi sieciami, podatność na ataki typu Denial of Services itp. nie dotyczyły praktycznie sieci przemysłowych.

Jednak od lat 90-tych XX wieku zaczął się zarysowywać trend[29] łączenia wydzielonych dotąd ICS z sieciami biurowymi oraz stosowanie do ICS rozwiązań z „klasycznych" sieci biurowych (komercyjnych systemów operacyjnych i sprzętu komputerowego) oraz wykorzystanie Internetu (protokołu IP) jako medium komunikacyjnego. Wymienione fakty złożyły się na nowy jakościowo obraz współczesnych sieci przemysłowych – pojawiły się w nich nowe problemy z zapewnianiem bezpieczeństwa. Że są to zagadnienia istotne dla żywotnych interesów, nie tylko poszczególnych firm czy organizacji, ale także państwa, świadczą już wczesne publikacje o tej tematyce i podejmowane działania:

– opublikowane po raz pierwszy we wrześniu 2007 roku rekomendacje NIST (*National Institute of Standards and Technology*) [30],
– przyjęcie przez NERC (*North American Electric Reliability Corporation*) w 2008 roku ośmiu standardów z zakresu „cybersecurity" i ochrony infrastruktury krytycznej (patrz też rozdział 4.3 oraz przypisy dolne z linkami w tym rozdziale);

---

[28] W literaturze anglojęzycznej jest też często używane określenie *Operational Technology* (OT).

[29] Głównie pod wpływem czynników ekonomicznych i nowych koncepcji zarządzania biznesem, w których kadra zarządzająca w celu podwyższenia efektywności i konkurencyjności swoich organizacji korzysta z danych na temat produkcji dostępnych w systemach automatyki.

– powołanie w USA, w ramach U.S. Department of Homeland Security, przemysłowego zespołu reagowania (ICS-CERT − *Industrial Control Systems Cyber Emergency Response Team*)[30]. Obecnie na swoich stronach internetowych[31] ICS-CERT prezentuje nie tylko specyfikacje aktualnych zagrożeń i podatności wykrytych w systemach przemysłowych, ale także obszernie opisane zalecane praktyki zabezpieczania takich systemów [39].

Najnowsze dane statystyczne pokazują[32], że sieci przemysłowe i przemysłowe systemy sterowania w szczególności, mogą być stosunkowo łatwym celem dla intruzów, ponieważ:

- 40% instalacji przemysłowych ma co najmniej jedno bezpośrednie połączenie z Internetem;
- w 53% instalacji przemysłowych używa się przestarzałych, już nie wspieranych przez producenta systemów Windows, takich jak Windows XP;
- w 69% instalacji przemysłowych używa się nieszyfrowanych haseł do dostępu do ICS;
- 57% instalacji przemysłowych nie ma zainstalowanego oprogramowania antywirusowego z funkcją automatycznej aktualizacji baz sygnatur;
- 16% instalacji przemysłowych ma co najmniej jeden bezprzewodowy punkt dostępowy;
- 84% instalacji przemysłowych ma co najmniej jedno urządzenie z dostępem zdalnym.

Zagadnienia bezpieczeństwa ICS związane z przesyłaniem sygnałów sterujących i danych produkcyjnych, w zasadzie od początku ich zaistnienia, są dowiązywane do problemów bezpieczeństwa infrastruktury krytycznej[33], a ostatnio także do modnej tematyki łańcucha dostaw [28]. Ma to odzwierciedlenie w tworzonych rozwiązaniach prawnych, publikacjach naukowych, szkoleniach itp. Przykład takiego podejścia daje chociażby ENISA (*European Union Agency for Network and Information Security*). ENISA w 2014 roku ustanowiła grupę zainteresowanych stron dla problematyki sieci przemysłowych (*ICS Stakeholder Group*). Jej celem jest dostarczenie użytkownikom i ekspertom od ICS/SCADA platformy wymiany poglądów oraz możliwości opracowywania i rozpowszechniania nowych idei podnoszących poziom

[30] https://www.us-cert.gov/control_systems/ics-cert/
[31] https://www.us-cert.gov/ics/Recommended-Practices
[32] Patrz np. raport firmy CyberX z za rok 2019 dostępny pod: https://cyberx-labs.com/resources/risk-report-2019/ (dostęp 22.05.2020). Dane opracowano na podstawie badania ponad 850 podmiotów z całego świata.
[33] Patrz np. standardy NERC-CIP (CIP − *Critical Infrastructure Protection*).

bezpieczeństwa przemysłowego w UE[34]. Przykłady takich opracowań eksperckich to [9] i [10]. Pierwsze z nich dotyczy wyzwań i rekomendacji związanych z Industry 4.0 Cybersecurity. Drugie z kolei, oprócz przeglądu publikacji i przedsięwzięć ENISY (do roku 2015) w dziedzinie ICS, zawiera wyniki oceny[35] ośmiu krajów UE (w tym Polski) pod względem dojrzałości wdrożonych w infrastrukturze krytycznej państwa rozwiązań z zakresu bezpieczeństwa przemysłowego.

W artykule przedstawiono kolejno:

- typy sieci przemysłowych,
- systemy czasu rzeczywistego jako szczególny przypadek systemów przemysłowych, szczególnie wrażliwych ze względu na konieczność zachowania reżimów czasowych na wszelkie zakłócenia w nadsyłaniu sygnałów sterujących,
- ataki na sieci i systemy przemysłowe, jako jeden ze sposobów realizacji zagrożenia,
- autorski przegląd norm, standardów i zaleceń (dobrych praktyk) dla systemów przemysłowych,
- zsyntetyzowany opis dobrych praktyk dotyczących, zgodnie z tytułem artykułu, zarządzania ochroną informacji sterującej w systemach przemysłowych.

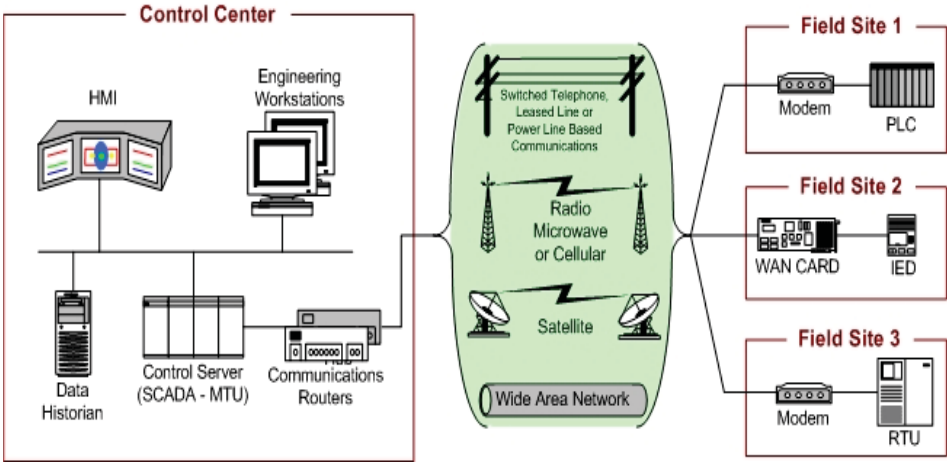
2. Przegląd typów sieci przemysłowych

Termin SCADA (patrz np. [12], [26]) oznacza rozproszony na rozległym geograficznie terenie system elementów wykonawczych i monitorujących komunikujących się z centrami dyspozycyjnymi przez rozległe sieci łączności (rys.1). Przykładami takich sieci są systemy nadzoru i sterowania ruchu kolejowego, systemy nadzoru i sterowania przesyłem mocy w sieciach energetycznych itp.

---

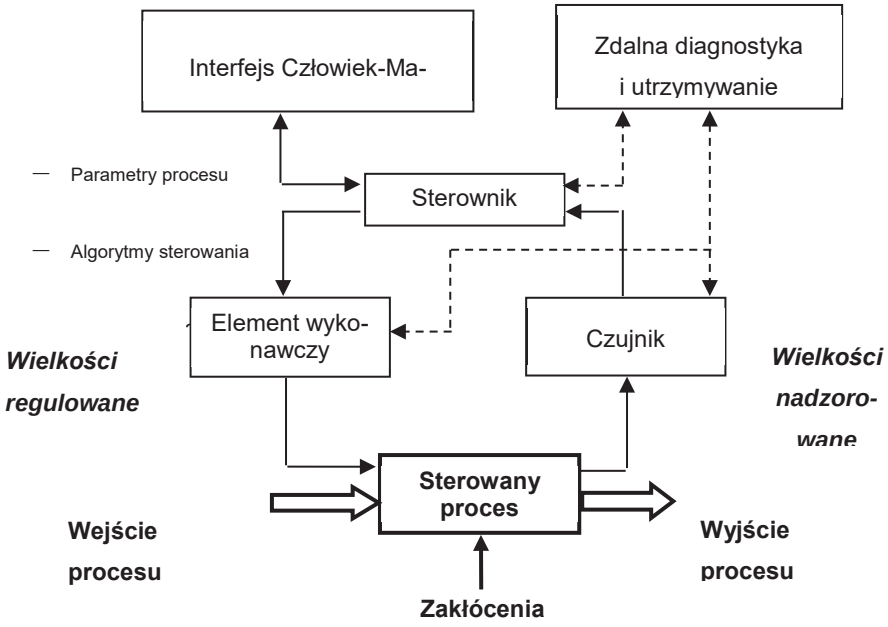
[34] *„Terms of reference for an ENISA ICS Security Stakeholder Group”* − https://resilience.enisa.europa.eu/ics-security/EICSSGTermsofReference.pdf

[35] Ocena bazowała na dziewięciu kryteriach, przydzielonych (po trzy) do trzech grup: prawo lokalne, wsparcie operatorów usług krytycznych przez państwo, lokalne warunki eksploatacji i rozwoju systemów ICS-SCADA.



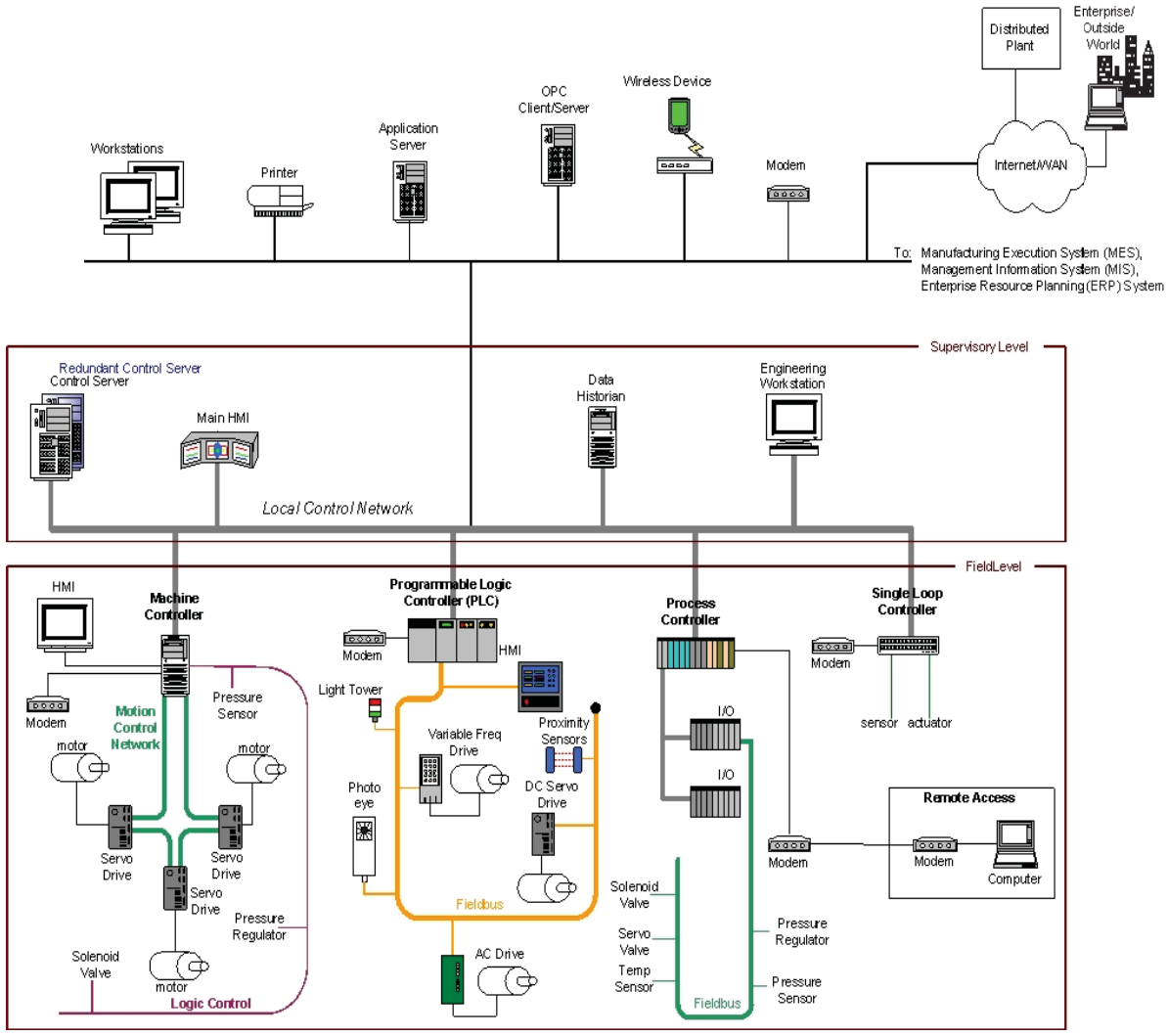
Rys.1. Schemat ogólny sieci SCADA (za [26]).

Podstawowe elementy i operacje związane z sieciami typu SCADA i ogólnie, sieciami przemysłowymi służącymi do sterowania procesami, pokazane są na rys.2.



Rys. 2. Schemat podstawowych operacji i elementów przemysłowych sieci sterowania (za [26]).

Termin *rozproszony system sterowania* zwykle odnosi się do systemu komputerowego, który pełni rolę nadrzędną w stosunku do sterowników PLC i innych urządzeń (rys.3). Zwykle to sterowniki PLC połączone są bezpośrednio z urządzeniami wykonawczymi (zawory, pompy, itp.) i pomiarowymi (czujniki temperatury, poziomu itp.) i zbierają aktualne dane z obiektu oraz wykonują automatyczne algorytmy sterowania i regulacji. Za pośrednictwem sterowników PLC dane trafiają do systemu komputerowego i tam są archiwizowane oraz przetwarzane na formę bardziej przyjazną dla użytkownika. Syntetyczne ujęcie różnic pomiędzy „klasycznymi" systemami teleinformatycznymi a systemami przemysłowymi jest przedstawione w tabeli 1.



Rys. 3. Przykład implementacji rozproszonego przemysłowego systemu sterowania (za [26]).

Tab.1. Specyfikacja różnic pomiędzy sieciami informatycznymi a systemami przemysłowymi (za [26]).

Kategoria	Sieć informatyczna	System przemysłowy
Wymagania wydajnościowe	Nie działa w czasie rzeczywistym Wymagana wysoka przepustowość Duże opóźnienia i zniekształcenia odpowiedzi systemu są akceptowalne	Działa w czasie rzeczywistym, odpowiedź systemu jest silnie zależna od czasu Niewielka przepustowość jest akceptowalna Opóźnienia i/lub zniekształcenia (fluktuacje) odpowiedzi systemu nie są akceptowalne
Wymagania na dostępność	Operacja przeładowania systemu jest akceptowalna Braki w dostępności często są tolerowane (zależą od konkretnych wymagań operacyjnych na system)	Operacja przeładowania systemu może być nie do zaakceptowania ze względu na wymaganą dostępność systemu Wymagania na dostępność powodują konieczność stosowania redundancji Wyłączenia muszą być planowane i umieszczane z odpowiednim wyprzedzeniem w harmonogramie Wysoka dostępność wymaga dokładnego testowania przed wdrożeniem systemu

Kategoria	Sieć informatyczna	System przemysłowy
Wymagania na zarządzanie ryzykiem	Tajność i integralność danych jest najważniejsza Odporność na błędy jest mniej ważna – chwilowy przestój jest akceptowalny Głównym skutkiem ryzyka (*risk impact*) jest opóźnienie operacji biznesowych	Najważniejsze jest bezpieczeństwo ludzi, wymagające właściwej ochrony procesów Odporność na błędy jest bardzo ważna – nawet chwilowy przestój może być nieakceptowany Głównym skutkiem ryzyka est powstanie niezgodności z przepisami, szkody w środowisku, utrata życia, wyposażenia lub możliwości produkcji i produktów
Cechy architektury	Podstawowy cel projektu architektury to ochrona zasobów IT i informacji w nich przechowywanej (lub pomiędzy nimi przesyłanej) Silna ochrona centralnego serwera	Podstawowy cel projektu architektury to ochrona urządzeń brzegowych (polowych, np. elementów wykonawczych, czujników i/lub sterowników) Ochrona serwera centralnego drugoplanowa Silna ochrona fizyczna dostępu do elementów ICS

Kategoria	Sieć informatyczna	System przemysłowy
Oddziaływanie na środowisko	Typowe systemy IT nie wchodzą w interakcje z otaczającym je środowiskiem	Typowe systemy ICS oddziałują poprzez elementy wykonawcze na otaczające je środowisko, a za pomocą czujników zbierają informacje z tego środowiska Wszystkie funkcje „bezpieczeństwa" zintegrowane z ICS muszą być przetestowane (zwykle off-line, na porównywalnych systemach) w celu zapewnienia, że nie zostaną zakłócone normalne operacje ICS
Krytyczne czasowo interakcje	Czas odpowiedzi na działania użytkownika (np. żądanie dostępu) najczęściej nie jest krytyczny	Czas odpowiedzi na sygnały z otoczenia zwykle jest krytyczny Działania użytkownika (komunikacja człowiek-maszyna) podlegają priorytetyzacji – nie powinny wpływać ujemnie na realizację podstawowych funkcji ICS
Operacje w systemie	System jest projektowany do użytku z typowymi systemami operacyjnymi Aktualizacje są wgrywane bezpośrednio z zastosowaniem zautomatyzowanych narzędzi wdrożeniowych	Używane są różne, najczęściej firmowe, systemy operacyjne bez wbudowanych właściwości odporności na ataki wykorzystujące luki lub błędy w oprogramowaniu Zmiany w oprogramowaniu muszą być przetestowane i wdrażane stopniowo w celu uniknięcia naruszenia integralności systemu Eksploatacja ICS wymaga specyficznej wiedzy, różnej od wiedzy typowego administratora IT

Kategoria	Sieć informatyczna	System przemysłowy
Ograniczenia na zasoby	„Klasyczne" systemy informatyczne mają zwykle nadmiar resursów, co pozwala zastosować dodatkowe aplikacje, np. związane z bezpieczeństwem	ICS są projektowane w celu obsługi konkretnych procesów przemysłowych i mogą nie posiadać wystarczającej ilości pamięci i mocy obliczeniowej do obsługi dodatkowych zadań z dziedziny bezpieczeństwa
Komunikacja	Używane są standardowe protokoły komunikacyjne Głównie sieci kablowe z dołączonymi czasami sieciami bezprzewodowymi	Używane są najczęściej firmowe i standardowe protokoły komunikacyjne Wykorzystywane są specjalizowane środki łączności przewodowej i bezprzewodowej (radiowe i satelitarne)
Zarządzanie zmianami	Zmiany w oprogramowaniu są wykonywane w odpowiednim czasie z zachowaniem zasad i procedur polityki bezpieczeństwa. Procedury są często zautomatyzowane	Zmiany w oprogramowaniu muszą być wykonywane bardzo ostrożnie, zwykle przez personel producenta oprogramowania, ponieważ mogą być wtedy wymagane zmiany także w algorytmach sterowania, sprzęcie lub pozostałym oprogramowaniu Wyłączenia ICS muszą być zaplanowane
Wsparcie i usługi	Może być realizowane przez różnych dostawców	Wsparcie najczęściej tylko przez jednego dostawcę
Czas życia elementów systemu	3-5 lat	15-20 lat
Dostęp do elementów systemu	Komponenty są zwykle zlokalizowane na niewielkim obszarze i jest do nich łatwy dostęp	Komponenty są izolowane, rozproszone na dużym obszarze i zwykle trudno jest się do nich (fizycznie) dostać

3. Systemy czasu rzeczywistego

W specyfikacjach systemów sterowania używane są często określenia: „czasu rzeczywistego" (ang. *real-time systems*) oraz „systemy wbudowane" (ang. *embedded systems*), wskazujące dokładniej typ systemu sterowania. Zwykle określa się systemy czasu rzeczywistego jako „*... systemy wykonujące wszystkie swoje zadania przy zachowaniu określonych wymagań czasowych"* (wymagania te mogą dotyczyć obsługi zdarzeń o dużej częstotliwości napływania do systemu, określonego czasu reakcji na zdarzenie, generowania sygnałów sterujących z określoną częstotliwością itp.). Można spotkać się również z definicją, że *„... są to systemy reagujące w przewidywalny sposób na nieprzewidywalne wymuszenia zewnętrzne".* Zgodnie z definicją IEEE/ANSI Std 729: „ … *komputerowym systemem czasu rzeczywistego nazywamy system komputerowy, w którym obliczenia są wykonywane współbieżnie z procesem zewnętrznym (otoczenia) w celu sterowania, nadzorowania lub terminowego reagowania na zdarzenia występujące w tym procesie (otoczeniu)*". Jeżeli oprogramowanie systemu sterowania jest zapisane w pamięci stałej stanowiącej część urządzenia sterującego (tzn. jego zmiana wiąże się z wymianą bądź przeprogramowaniem pamięci PROM), to o takim systemie sterowania mówi się że jest „wbudowany"[36].

Z przytoczonych definicji wynika, że w analizie i projektowaniu systemów czasu rzeczywistego należy uwzględnić jego trzy podstawowe elementy:

- otoczenie wysyłające i odbierające dane/sygnały do/z systemu komputerowego;
- system komputerowy;
- czas.

[36] W przypadku instalacji systemów wbudowanych na platformach pływających, latających lub jeżdżących. używa się często określenia „systemy pokładowe".

Czynnik czasu może występować jako:

- jakościowy – tzn. jeżeli pewne zdarzenie wystąpi przed innym, to odpowiedź systemu może być inna niż w przypadku, gdy takie zdarzenia wystąpią w innym porządku;
- ilościowy – tzn. reakcja systemu zależy od czasu (momentu lub przedziału czasowego) wyrażonego ilościowo (por. np. pojedyncze i podwójne „kliknięcie" myszką w systemach okienkowych).

Ze względu na dokładność spełnienia wymagania czasu reakcji systemu, wyróżnia się trzy klasy systemów czasu rzeczywistego:

- **systemy o silnych** (twardych) **wymaganiach czasowych** (ang. *Hard Real-Time Systems*) – odpowiedź systemu musi być przesłana do otoczenia dokładnie w danym momencie czasowym (przykład: stymulatory serca).
- **systemy o słabych** (miękkich) **wymaganiach czasowych** (ang. *Soft Real-Time Systems*) – odpowiedź systemu może być przesłana w ciągu pewnego przedziału czasu. Zbyt późne dostarczenie odpowiedzi nie powoduje katastrofy, ale zwykle wpływa niekorzystnie na ocenę systemu (przykład: system rezerwacji miejsc).
- **systemy o solidnych wymaganiach czasowych** (ang. *Firm Real-Time Systems*) – odpowiedź systemu może być przesłana w ciągu pewnego przedziału czasu (miękko), ale definiuje się (twardo) czas graniczny, którego nie można przekroczyć, bo może to doprowadzić do katastrofy (przykład: większość systemów sterowania).

Przedstawione rozważania i definicje pozwalają sformułować charakterystyczne cechy komputerowych systemów czasu rzeczywistego [6]. Należą do nich:

- ciągłość działania – system powinien pracować bez przerw od momentu jego uruchomienia do wycofania z eksploatacji, natomiast może znajdować się w stanach oczekiwania na wystąpienie określonych zdarzeń. Konsekwencją jest trudność w wyodrębnieniu stanu początkowego procesu obliczeń w takim systemie;
- zależność od otoczenia (zdarzeń i danych generowanych przez proces zewnętrzny) – struktura otoczenia jest zwykle skomplikowana lecz statyczna, co istotnie ogranicza konieczność stosowania struktur dynamicznych (rekurencji) i ułatwia analizę systemu;
- współbieżność – w otoczeniu systemu przebiega zwykle wiele współbieżnych procesów generujących sygnały zdarzeń lub wymagających obsługi przez system komputerowy, co narzuca współbieżną strukturę takiego systemu;
- przewidywalność – pomimo zachodzących w systemie komputerowym wielu procesów współbieżnych, na zewnątrz system taki musi się zachowywać deterministycznie, tj. Musi reagować na zdarzenia według założonych wymagań;

- terminowość – reakcje na zdarzenia w otoczeniu (odpowiedzi systemu) powinny być obliczane zgodnie z zaprojektowanymi algorytmami i dostarczane do otoczenia w odpowiednich momentach czasowych. Brak możliwości (zwykle) zatrzymania procesu zewnętrznego, stawia dodatkowe wymagania co do momentu przekazania odpowiedzi.

4. Ataki na sieci i systemy przemysłowe

Podstawowy zbiór zagrożeń dla poprawnego działania sieci i systemów teleinformatycznych oraz sieci i systemów przemysłowych obejmuje:

1. Zagrożenia środowiskowe, tj. oddziaływanie:
   - ognia (np. pożary instalacji przemysłowych wywołanych uderzeniem pioruna),
   - wody (np. wylewy rzek powodujące podtopienia obiektów z infrastrukturą teleinformatyczną i przemysłową),
   - czynników mechanicznych (np. trzęsienia ziemi lub huragany niszczące infrastrukturę telekomunikacyjną),
   - czynników biologicznych (np. wirusów, powodujących braki w personelu obsługującym sieci i systemy teleinformatyczne i przemysłowe), itp.
2. **Zagrożenia celowymi** lub błędnymi **działaniami człowieka.**
3. Tzw. „siły wyższe" inne niż zagrożenia środowiskowe (np. ustanowienie złych przepisów prawa przez ustawodawcę).

Wspomniane w tytule rozdziału „ataki" to forma realizacji zagrożenia celowymi działaniami człowieka. Cennym źródłem wiedzy o możliwościach ataków na zasoby informacyjne oraz sieci i systemy teleinformatyczne jest strona https://attack.mitre.org/[37]. Zawiera ona podstronę https://collaborate.mitre.org/attackics/index.php/Main_Page[38] z tabelą podsumowującą **ataki na sieci i systemy przemysłowe** (jej fragment zamieszczony jest na rys. 4). Na kolejnych podstronach są szczegółowe opisy:

- 81 technik ataków na systemy ICS;
- 17 narzędzi programowych używanych do ataków na systemy ICS (strona aktualizowana 02.01.2020);
- 10 ujawnionych grup atakujących systemy ICS (strona aktualizowana 02.01.2020).

[37] Dostęp 16.05.2020.
[38] Dostęp 16.05.2020; strona aktualizowana 04.03.2020.

The MITRE ATT&CK for ICS Matrix is an overview of the tactics and techniques described in the ATT&CK for ICS knowledge base. It visually aligns individual techniques under the tactics in which they can be applied. Some techniques span more than one tactic because they can be used for different purposes.

Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/ Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View

Rys. 4. Fragment tabeli podsumowującej ataki na systemy ICS. Źródło: https://collaborate.mitre.org/attackics/index.php/Main_Page.

Należy podkreślić, że opisywany framework (bo tak jest traktowany MITRE ATT&CK), dotyczy jedynie sposobów realizacji (w formie ataków) jednego typu zagrożenia – celowych działań ludzi.

Również w dodatku C (*Threat Sources, Vulnerabilities, and Incidents*) standardu NIST SP 800-82 rev.2 zamieszczony jest opis 16 incydentów dotyczących ICS (w tym 8 ataków). Opis jest doprowadzony do roku 2013.

Dane statystyczne pokazują także [2], jak grupują się incydenty bezpieczeństwa dla ICS związane z działaniami ludzi (dane na rok 2019). Wyróżnia się incydenty związane z[39]:

1. dostępem fizycznym (np. poprzez USB lub bezpośredni fizyczny dostęp do urządzenia, w szczególności do jego panelu sterującego) – 56,3%,
2. dostępem zdalnym (obejście zabezpieczeń wbudowanych w architekturę ICS) – 40,6%,
3. zaufanym dostępem zdalnym (dostęp zaufanego podmiotu bez naruszenia zabezpieczeń technicznych) – 37,5%,
4. działaniami serwisowymi i konsultacjami (skutki: nierozpoznane zmiany w konfiguracji) – 34,4%,
5. łańcuchem dostaw (np. oprogramowanie lub sprzęt niezgodne ze specyfikacjami) – 18,8%.

Jak już wspomniano we Wstępie, problematyka bezpieczeństwa sieci przemysłowych jest zwykle lokowana w obszarze bezpieczeństwa infrastruktury krytycznej. Oznacza to, że:

1. Reakcja „pozatechniczna" na incydenty z zakresu bezpieczeństwa, w szczególności ściganie sprawców takich incydentów, będzie inne niż w przypadku incydentów w klasycznych sieciach teleinformatycznych, gdzie najczęściej dochodzi do realizowanych w celach komercyjnych oszustw, nieuprawnionego przejęcia zasobów informacyjnych czy blokowania usług. Ściganie sprawców takich incydentów jest realizowane przez policję, podczas gdy ściganie sprawców incydentów w infrastrukturze krytycznej powinno być domeną odpowiednich służb ochrony państwa (co jednak nie wyklucza współdziałania z policją).
2. Sprawcami incydentów w sieciach i systemach przemysłowych zwykle będą zorganizowane grupy działające w strukturach militarnych obcego państwa (w mass mediach określane mianem „wojska cybernetycznego" ☺) lub grupy nieformalne, przez obce państwo do takich działań wynajęte. Natomiast sprawcami incydentów w klasycznych sieciach te-

[39] Podane na końcu każdego punktu wartości procentowe informują, jaki procent respondentów badania prowadzonego przez SANS wskazał na daną grupę.

leinformatycznych są zwykle pojedyncze osoby lub grupy przestępcze działające dla osiągnięcia doraźnych korzyści materialnych bądź wyrządzenia doraźnych szkód z powodów osobistych.

3. Sprawcami incydentów zarówno w obszarze infrastruktury krytycznej, jak i klasycznych sieci teleinformatycznych mogą być też pojedyncze osoby lub grupy nieformalne połączone jakimś celem ideowym: obronie życia poczętego, niedopuszczenia do budowy instalacji nuklearnych, obronie praw zwierząt itp.[40]

5. Normy, standardy i zbiory „dobrych praktyk" dotyczące bezpieczeństwa sieci przemysłowych

Zamieszczona w [2] tabela nr 8: *Top 10 Regulations, Standards, Best Practices Used* przedstawia następujący ranking (z prawej strony % respondentów którzy wskazali dany standard, regulację lub zbiór dobrych praktyk):

1.	NIST CSF (Cyber Security Framework)	38,1%
2.	ISO 27000 series	32,0%
3.	**NIST 800-53**	31,4%
4.	**NIST 800-82**	30,9%
5.	**ISA/IEC 62443**	30,4%
6.	CIS Critical Security Controls	29,9%
7.	**NERC CIP**	23,7%
8.	GDPR	15,5%
9.	C2M2 (Cybersecurity Capability Maturity Model)	10,3%
10.	NIS Directive (EU)	8,3%

Badaniem objęto 338 respondentów, przy czym większość (70%) pochodziła z USA i Kanady i ten fakt należy mieć na uwadze przy dyskusji popularności konkretnych regulacji, standardów czy zbiorów dobrych praktyk. Warto też zauważyć, że do jednego worka wrzucono opracowania o różnych profilach:

- NIST CSF [41] jest opracowaną przez organ standaryzacyjny USA, w odpowiedzi na regulacje prawne administracji rządowej, ogólną metodyką zabezpieczania infrastruktury

[40] W [2], np. w tab.2 na stronie 8, można znaleźć bardziej detaliczne rozróżnienie sprawców incydentów.

krytycznej państwa w zakresie „cybersecurity". W jej ramach ICS są jednym z zabezpieczanych elementów[41].

- Seria norm ISO 27000 dotyczy bezpieczeństwa informacji w systemach informacyjnych, w tym budowania systemów zarządzania bezpieczeństwem informacji (SZBI). Nie dotyczy bezpośrednio ICS.
- NIST 800-53 [27] jest standardem zawierającym zbiór zalecanych przez NIST zabezpieczeń i metodykę ich wdrożenia w systemach informacyjnych. Do ICS standard ten stosuje się przez dodatkowe uregulowania (NIST 800-82 [30]).
- CIS Critical Security Controls są zbiorem 20 dobrych praktyk zabezpieczania systemów informatycznych przed atakami (tylko!). Nie odnosi się bezpośrednio do ICS – sposób zastosowania tych zaleceń do ICS jest podany w [40][42].
- NIS Directive (EU) jest dyrektywą europejską mającą na celu usprawnienie współpracy (przede wszystkim międzynarodowej) w zakresie incydentów dotyczących infrastruktury krytycznej. Nie odnosi się bezpośrednio do ICS.
- GDPR (*General Data Protection Regulation*) czyli po polsku RODO, dotyczy tylko jednej kategorii informacji – danych osobowych, które w systemach ICS mają marginalne znaczenie.
- **Tylko ISA/IEC 62443, NIST 800-82, NERC CIP dotyczą w całości i bezpośrednio ICS** (przy czym ten ostatni zbiór standardów jest ukierunkowany na ICS w elektroenergetyce).

W tym rozdziale przedstawiono, według autorskiego wyboru, krótkie charakterystyki norm, standardów i „dobrych praktyk" dotyczących bezpieczeństwa sieci przemysłowych. Wybrano:

- siedmioczęściową normę PN-EN 61508:2020 *Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem*;
- serię norm IEC 62443;
- standardy North American Electric Reliability Corporation (NERC);

---

[41] W oryginalnej publikacji [41] zapisano: (…) *The Framework offers a flexible way to address cybersecurity, including cybersecurity's effect on physical, cyber, and people dimensions. It is applicable to organizations relying on technology, whether their cybersecurity focus is primarily on* information technology (IT), industrial control systems (ICS), cyber-physical systems (CPS), *or connected devices more generally, including the* Internet of Things (IoT).

[42] Patrz też podrozdział 5 tego rozdziału.

- standard NIST SP 800-82: *Guide to Industrial Control Systems (ICS) Security* oraz standard NIST SP 800-53*: Security and Privacy Controls for Federal Information Systems and Organizations*;
- zbiór dobrych praktyk zawarty w kompendium wydanym przez niemiecki *Bundesamt für Sichercheit in der Informationstechnik* (https://www.bsi.bund.de) [12].

5.1. Norma PN-EN 61508: 2010 Bezpieczeństwo funkcjonalne elektrycznych/ elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem

Jest to siedmioczęściowa norma [36]-[42] mająca za podstawę normę EN 61508. Odnosi się do systemów związanych z bezpieczeństwem, które składają się z elementów elektrycznych albo elektronicznych lub systemów elektrycznych albo systemów elektronicznych jak również programowalnych systemów elektronicznych (PES). Ma status normy podstawowej, może być stosowana jako wyłączny dokument, może też być normą podstawową lub ramową dla opracowania norm sektorowych.

Norma EN 61508 zakłada oparte na ryzyku podejście do bezpieczeństwa funkcjonalnego złożonych systemów bezpieczeństwa. Główną zasadą jest zarządzanie i analiza ryzyka jako funkcji następstwa wydarzenia i prawdopodobieństwa wystąpienia tego wydarzenia. Norma odnosi się do pełnego cyklu życia systemu z punktu widzenia wykonawcy i użytkownika końcowego. Wiarygodność systemu jako układu bezpieczeństwa wyraża się poziomem integralności bezpieczeństwa SIL (*Safety Integrity Level*), który zależy od prawdopodobieństwa wystąpienia błędu wewnętrznego w czasie pracy systemu. Prawdopodobieństwo, że elementy zabezpieczające prawidłowo wykonają wymagane funkcje jest nazywane integralnością zabezpieczeń (ang. *safety integrity*). W normie wskazano cztery poziomy integralności zabezpieczeń, określone przez prawdopodobieństwa awarii (tab. 2).

Tab. 2. Poziomy integralności zabezpieczeń.

Poziom integralności (*SIL*)	**Praca start-stopowa: p-stwo błędu**	**Praca ciągła: p-stwo błędu w ciągu godziny**
4	10^{-5} do. 10^{-4}	10^{-9} do 10^{-8}
3	10^{-4} do 10^{-3}	10^{-8} do 10^{-7}
2	10^{-3} do 10^{-2}	10^{-7} do 10^{-6}
1	10^{-2} do 10^{-1}	10^{-6} do 10^{-5}

Analiza bezpieczeństwa dla systemów sterowania jest procesem, w ramach którego oceniany jest poziom ryzyka związanego z systemem i identyfikowane są mechanizmy występowania wypadków. Zdarzenia prowadzące w sposób bezpośredni do wypadku nazywane są *stanami hazardowymi* lub *hazardami*. Analiza bezpieczeństwa jest częścią cyklu życia bezpieczeństwa – według standardu IEC 61508, wykonywana jest w ramach kolejnych etapów cyklu życia systemu:

- podczas budowy systemu – w celu identyfikacji zagrożeń i dobrania właściwych środków projektowania i realizacji;
- podczas eksploatacji systemu – w celu sprawdzenia i/lub poprawienia stanu bezpieczeństwa systemu;
- podczas oceny systemu przez niezależną instytucję certyfikującą, dla sprawdzenia stopnia bezpieczeństwa i zaakceptowania (lub odrzucenia) systemu do użytkowania.

W normie przedstawiono m.in. ogólne zasady zabezpieczania urządzeń z programowalnymi układami elektronicznymi, w tym połączonych za pomocą sieci. Metody oceny bezpieczeństwa dla systemów ICS uwzględniające wymagane poziomy SIL są przedstawione w tabeli 3.

Tab. 3. Metody oceny bezpieczeństwa a poziomy integralności.

	Metoda lub technika	**SIL 1**	**SIL 2**	**SIL 3**	**SIL 4**
1	Kwestionariusze ocen	R	R	R	R
2	Tablice decyzyjne i tablice prawdy	R	R	R	R
3	Miary złożoności programów	R	R	R	R
4	Diagramy przyczynowo-skutkowe (CCD)	R	R	R	R
4a	Analiza drzewa zdarzeń (ETA)	R	R	R	R
5	Analiza drzewa błędów (FTA)	R	R	WR	WR
6	Analiza rodzajów i skutków uszkodzeń (FMEA)	R	R	WR	WR
7	Analiza hazardu i gotowości systemu (HAZOP)	R	R	WR	WR
8	Modele Markowa	R	R	R	WR
9	Schematy blokowe niezawodności	R	R	R	R
10	Symulacja (Monte-Carlo)	R	R	R	R

R- rekomendowane, WR - wysoce rekomendowane

Podstawowe zadanie dla sieciowego systemu bezpieczeństwa nie polega na wyeliminowaniu możliwości awarii układu, lecz na spowodowaniu, że w wypadku awarii odpowiednie urządzenia przełączone zostaną w tzw. stan bezpieczny. Dla większości zastosowań przemysłowych zalecany jest SIL3, co oznacza, że w trakcie pracy w pełni obciążonego systemu niezauważony lub źle zidentyfikowany błąd może pojawić się raz na 150 lat ciągłej pracy.

5.2. Seria norm IEC 62443

W odróżnieniu od starszych norm, takich jak np. [32]-[38], mająca za podstawę serię standardów ISA99 norma ISA/IEC 62443, jest normą kilkuelementową (patrz rys. 5)[43]. Jej elementy układają się w następujące cztery „serie":

- Seria 1 zawiera wyjaśnienie używanych terminów, koncepcji oraz proponowane miary „bezpieczeństwa".
- Seria 2 dotyczy bezpieczeństwa czynności operacyjnych i eksploatacji.
- Seria 3 zawiera proponowane poziomy ochrony IACS (*Industrial Automation and Control Systems*) oraz standaryzuje realizację zadań bezpieczeństwa OEM i integracji elementów przygotowywanych na zamówienie klienta.
- Seria 4 dotyczy „bezpiecznego" cyklu życia produktów takich jak przełączniki, sterowniki, zapory sieciowe itp. oraz technicznych wymagań bezpieczeństwa dla tych produktów.

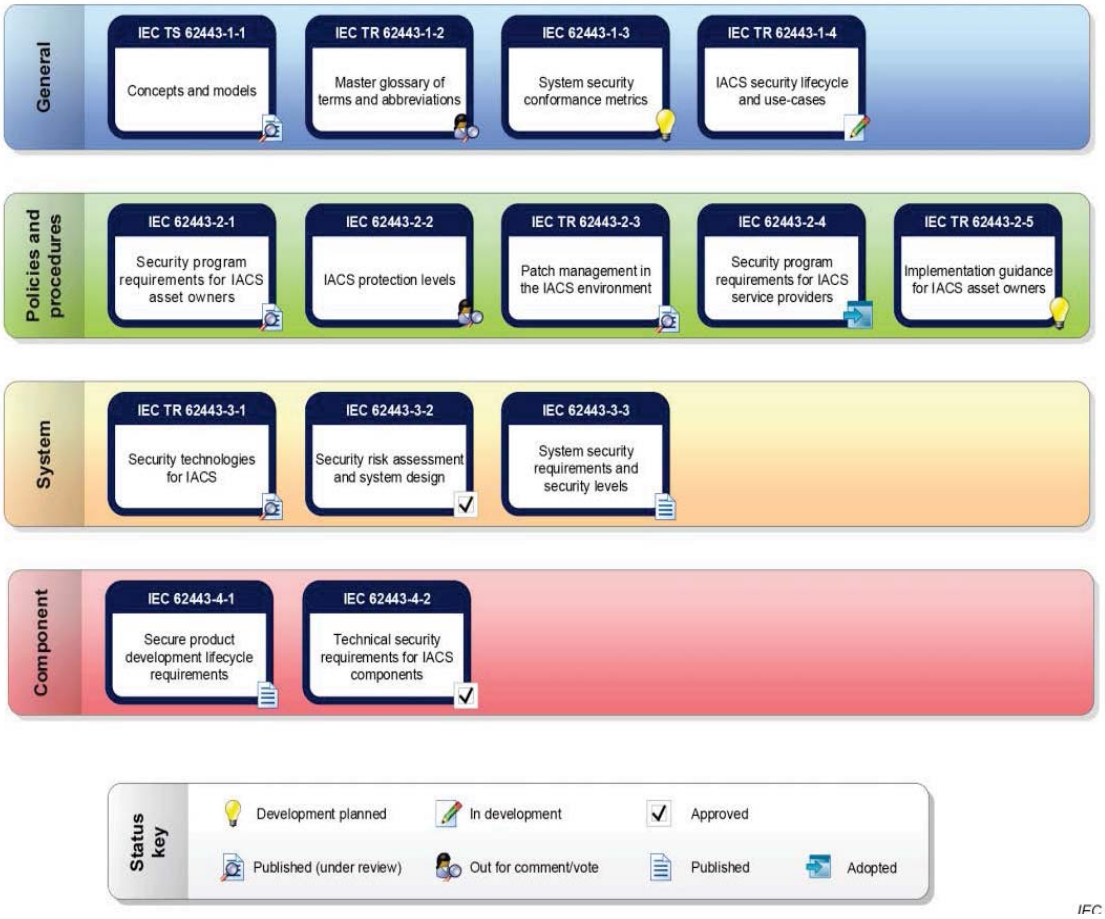
Polski Komitet Normalizacyjny wydał dotychczas (stan na maj 2020) następujące normy polskie serii IEC 62443[44]:

1. PN-EN IEC 62443-4-1:2018-06-wersja angielska: Bezpieczeństwo w systemach sterowania i automatyki przemysłowej − Część 4-1: *Wymagania cyklu rozwoju dotyczące tworzenia bezpiecznego produktu.*

W tej części normy podano wymagania dla bezpiecznego procesu wytwarzania produktów wykorzystywanych w systemach sterowania i automatyki przemysłowej. Zdefiniowano bezpieczny proces tworzenia i rozwoju (SDL) oraz podano definicje wymagań bezpieczeństwa, bezpiecznego projektowania i bezpiecznego wdrożenia (wraz z wytycznymi dla procesów: kodowania, weryfikacji i walidacji, obsługi błędów i wprowadzania poprawek oraz wycofania produktu z użycia). Te wymagania mogą być stosowane do nowych lub istniejących projektów rozwojowych, obsługi i utylizacji sprzętu, programów lub oprogramowania produktów

[43] Ułatwia to np. jej aktualizację.
[44] Ale jak widać, nie przetłumaczono tych norm (oprócz tytułów) na język polski.

nowych lub istniejących. Wymagania te dotyczą projektantów i serwisantów produktów, nie dotyczą użytkowników produktów. Pełny wykaz wymagań jest w załączniku B normy.



Rys.5. Stan procesu wydawniczego norm serii 62443 na koniec roku 2019 (za IEC 62443-4-2:2019).

2. PN-EN IEC 62443-4-2:2019-08-wersja angielska: Bezpieczeństwo w systemach sterowania i automatyki przemysłowej − Część 4-2: *Wymagania techniczne bezpieczeństwa dla komponentów IACS*.

W tej części normy zamieszczono techniczne wymagania bezpieczeństwa dla komponentów systemów sterowania powiązane z siedmioma podstawowymi wymaganiami FR (*Foundational Requirement*)) opisanymi w IEC TS 62443-1-1[45].
Te wymagania są podstawą określania stopnia bezpieczeństwa systemu za pomocą tzw. poziomów bezpieczeństwa (SL – *Security Level*)[46]. Celem tej normy jest definicja przy użyciu kryteriów FR 1-7 bezpieczeństwa systemu sterowania na poziomie komponentu systemu sterowania (SL-C). Poziom bezpieczeństwa (SL-T) oraz poziom bezpieczeństwa osiągnięty (SL-A), nie są objęte zakresem tej normy.
3. PN-EN IEC 62443-3-3:2020-01-wersja angielska: Przemysłowe sieci komunikacyjne − Bezpieczeństwo sieci i systemów − Część 3-3: *Wymagania dla systemu bezpieczeństwa i poziomów bezpieczeństwa*[47]

W tej części normy zamieszczono techniczne wymagania bezpieczeństwa dla systemów sterowania przy użyciu kryteriów FR 1-7.
4. PN-EN IEC 62443-2-4:2019-12-wersja angielska: Bezpieczeństwo w automatyce przemysłowej i systemach sterowania − Część 2-4: *Wymagania dla programu bezpieczeństwa dla dostawców usług IACS*

W tej normie określono wymagania bezpieczeństwa dla dostawców usług dla IACS, które to usługi mogą świadczyć, np. podczas konserwacji systemów automatyki. Całość wymagań bezpieczeństwa spełnianych przez dostawcę usługi dla IACS, jest nazywana *Programem Bezpieczeństwa*.

Systemy, urządzenia i procesy sieci przemysłowych mogą podlegać certyfikacji na zgodność z zaleceniami odpowiednich części normy IEC 62443. „*IEC 62443 Cybersecurity Certification Programs*" jest prowadzony w czterech zakresach [3]:

---

[45] Zawierającymi wymagania dla kompatybilności poziomów bezpieczeństwa SL-C (*Security Level-Control*).
[46] Dobre wyjaśnienie praktycznego zastosowania idei poziomów bezpieczeństwa jest zaprezentowane w [1].
[47] W oryginale: *system security requirements and security levels*. Czyli poprawnie powinno być: *wymagania na bezpieczeństwo systemu i poziomy bezpieczeństwa*.

1. Certyfikacji procesów – oceniane są procesy projektowania, integracji i testowania urządzeń i sieci ICS.
2. Certyfikacji urządzeń – oceniane są urządzenia, takie jak PLC, bramy sieciowe, zapory sieciowe, DCS.
3. Certyfikacji systemów – oceniane są złożone systemy zawierające różne urządzenia i sieci.
4. Certyfikacji osób:
   - certyfikat 1: *ISA/IEC 62443 Cybersecurity Fundamentals Specialist*;
   - certyfikat 2: *ISA/IEC 62443 Cybersecurity Risk Assessment Specialist*;
   - certyfikat 3: *ISA/IEC 62443 Cybersecurity Design Specialist*;
   - certyfikat 4: *ISA/IEC 62443 Cybersecurity Maintenance Specialist*.

   Uzyskanie certyfikatów 1-4 uprawnia do tytułu *ISA/IEC 62443 Cybersecurity Expert*.

5.3. Standardy North American Electric Reliability Corporation (NERC)

Podstawowy zbiór standardów z zakresu „cybersecurity" wydanych przez NERC[48] (stan na maj 2020) zawiera:

- CIP-001, Reporting.
- CIP-002, Cyber Security – BES Cyber System Categorization.
- CIP-003, Cyber Security – Security Management Controls.
- CIP-004, Cyber Security – Personnel & Training.
- CIP-005, Cyber Security – Electronic Security Perimeter(s).
- CIP-006, Cyber Security – Physical Security Perimeter(s).
- CIP-007, Cyber Security – Systems Security Management.
- CIP-008, Cyber Security – Incident Reporting and Response Planning.
- CIP-009, Cyber Security – Recovery Plans for BES Cyber Systems.
- CIP-010, Cyber Security – Config. Change Management and Vulnerability Assessments.
- CIP-011, Cyber Security – Information Protection.
- CIP-012, Cyber Security – Communication.
- CIP-013, Cyber Security – Supply Chain Risk Management.
- CIP-014, Cyber Security – Physical Security.

[48] Warta polecenia jest strona http://www.nerc.com/ oraz strona zawierająca, m.in. tabelę z odsyłaczami do wszystkich standardów CIP w PDF: https://blog.rsisecurity.com/what-is-nerc-cip-compliance/#more-3535.

Grupa robocza ds. bezpieczeństwa systemów sterowania przy NERC i komitecie ochrony infrastruktury strategicznej, już w 2006 roku opracowała dokument pt. *„Dziesięć najistotniejszych podatności przemysłowych systemów sterowania i sposoby ich łagodzenia”* [25]. Wymienione tam podatności to:

1. Nieodpowiednia polityka, strategie, procedury i mentalność użytkowników w zakresie bezpieczeństwa systemów sterowania[49].
2. Projekt połączonych sieci (teleinformatycznych i przemysłowych) ze zbyt ogólnym ustaleniem poziomów ochrony.
3. Możliwość zdalnego dostępu do sieci sterowania z pominięciem odpowiednich procedur ochronnych.
4. Oddzielne mechanizmy powiadamiania o zdarzeniach i administrowania w sieci sterowania i teleinformatycznej[50].
5. Niewłaściwie zabezpieczona komunikacja bezprzewodowa.
6. Brak prostych narzędzi do wykrycia/raportowania nietypowych zdarzeń i działań w sieciach sterowania.
7. Korzystanie ze współdzielonych (powszechnie dostępnych) kanałów komunikacyjnych do sterowania i zarządzania siecią sterowania.
8. Instalowanie niepotrzebnego, niezwiązanego ze sterowaniem, oprogramowania (np. gier).
9. Niewłaściwie analizowane i nadzorowane oprogramowanie w sieciach sterowania.
10. Nieautoryzowane działania i zmiany w sieci sterowania.

W ramach prac mających na celu zidentyfikowanie i klasyfikację podatności w sieciach SCADA oraz możliwości ich minimalizowania, US Department of Energy przy współudziale NERC opublikował, m.in. dokument [8]. Jego część dotycząca działań zarządczych, mających na celu ustanowienia efektywnego programu „cyberbezpieczeństwa” jest zaprezentowana w rozdz. 5.3.

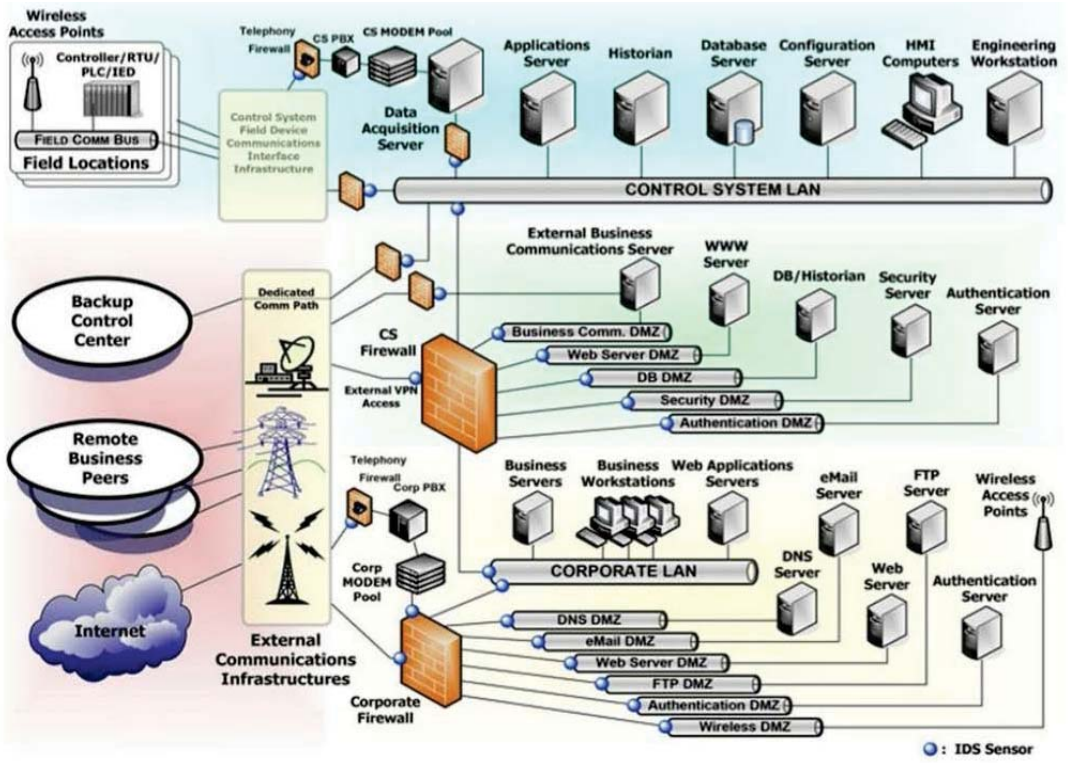
5.4. Zalecenia NIST: standard SP 800-82 i SP 800-53

[49] Pracownicy IT „widzą bezpieczeństwo” przez pryzmat informacji, ci od systemów przemysłowych – urządzeń. Różnice dotyczą także specjalistycznego języka tych dwóch grup zawodowych, w szczególności interpretacji takich pojęć jak bezpieczeństwo, wiarygodność, dyspozycyjność itp.

[50] ICS są wyposażone w funkcje generowania alarmów, ale dotyczą one zdarzeń pojawiających się w procesie produkcyjnym (np. brak produktu na taśmie produkcyjnej) a nie zdarzeń związanych np. z brakiem integralności informacji sterującej.

Konsekwencje wynikające z łączenia przemysłowych sieci sterowania z biurowymi sieciami teleinformatycznymi oraz wykorzystanie Internetu jako medium do przesyłania informacji w ramach sieci SCADA, zostały dostrzeżone także przez organizacje takie jak NIST. Efektem było opublikowanie we wrześniu 2007 roku rekomendacji NIST Special Publication 800-82: *Guide to Industrial Control Systems (ICS) Security*[51] [30]. Najistotniejszym rozdziałem w tej publikacji był rozdział 6, w którym zawarto zalecenia jak zastosować do ICS organizacyjne, operacyjne i techniczne przedsięwzięcia z zakresu bezpieczeństwa, obecnie opisane w NIST Special Publication 800-53: *Recommended Security Controls for Federal Information Systems* [27].

Rys.6. ICS defense-in-depth architecture strategy – ilustracja koncepcji opisanej w [50], zabezpiecze-



nia systemów ICS według strategii „w głąb" (za [30]).

[51] Aktualna (maj 2020) wersja jest z maja 2015 roku.

Najnowsze wydanie SP 800-82 rev.2 w szczegółach odwołuje się do standardu ISA 62443 oraz opracowań zespołów standaryzujących (USA) i zespołów US-CERT. Przykładem może być rekomendowana architektura zabezpieczania systemów przemysłowych pokazana na rys. 6.

W [27] jest wyspecyfikowanych 18 obszarów działań (nazywanych rodzinami). W poprzednich wersjach tego standardu rodzin było 17 – rodzinę Program Management (PM), opisaną bardziej szczegółowo w dalszej części tego artykułu, dodano dopiero w wersji 4. Dla każdej rodziny są podane zabezpieczenia niezbędne, zdaniem autorów standardu, do osiągnięcia określonego poziomu ochrony: niski (low), średni (moderate), wysoki (high).

5.5. Kompendium niemieckiego urzędu ds. bezpieczeństwa informacyjnego

Niemiecki urząd ds. bezpieczeństwa informacyjnego (*Bundesamt für Sichercheit in der Informationstechnik*; https://www.bsi.bund.de) wydał Kompendium [12] w którym w rozdziale 5 opisano 73 najlepsze praktyki w zakresie zapewniania bezpieczeństwa ICS rekomendowane przez ww. urząd. Te praktyki przyporządkowano do pięciu następujących grup:

1. Podstawowe przedsięwzięcia (ang. *first steps*; praktyki 1-6; rozdz.5.2).
2. Procesy i zasady bezpieczeństwa (ang. *security-specific processes /policies*; praktyki 7-18; rozdz.5.3).
3. Wybór (zakup) systemów i ich komponentów oraz związanych z nimi dostarczycieli usług serwisowych i integratorów (ang. *selection of the used systems and components as well as of the assigned service providers and integrators*; praktyki 19-30; rozdz.5.4).
4. Bezpieczeństwo konstrukcyjne i fizyczne (ang. *constructional and physical securing*; praktyka 31; rozdz.5.5).
5. Przedsięwzięcia techniczne (ang.*technical measures*; praktyki 32-73; rozdz.5.6).

6. Opis dobrych praktyk dotyczących zarządzania ochroną informacji sterującej w systemach przemysłowych – wybór autorski

Każdy z przedstawionych w poprzednim rozdziale zbiorów dobrych praktyk, norma czy standard, zawierają także zalecenia dotyczące przedsięwzięć organizacyjnych mających na celu zapewnienie poprawnego działania zabezpieczeń technicznych i fizycznych oraz ich właściwego doboru i zakupu. Zwykle w literaturze te zalecenia prezentuje się jako *zalecenia organizacyjne mające na celu wdrożenie efektywnego programu cyberbezpieczeństwa"*. Dalej są krótko zaprezentowane rekomendacje z tego zakresu wskazane przez NIST (SP 800-53), SANS (CIS-ICS), NERC (CIP) oraz niemiecki BSI (Kompendium).

6.1. Zalecenia organizacyjne NIST

Jedna z 18 rodzin z NIST SP 800-53 – Program Management (PM)[52] – zawiera zbiór „zabezpieczeń" (dokładniej: zalecanych rozwiązań organizacyjnych) wspomagających zabezpieczenia techniczne (informatyczne i fizyczne). Te zalecenia nie są przyporządkowane do żadnego z poziomów zabezpieczeń (*baselines*), są niezależne od prognozowanych szkodliwych skutków zrealizowanych zagrożeń i powinny być zaimplementowane dla całości organizacji biznesowej (np. firmy produkcyjnej) wspierając jej program bezpieczeństwa.

Zalecenia (*control*) tej rodziny są następujące:

- PM-1 (*Information Security Program Plan*) – należy opracować i rozpowszechnić w całej organizacji Plan Bezpieczeństwa Informacyjnego (PBI). Plan musi być zatwierdzony przez kierownictwo, aktualizowany i chroniony przed nieautoryzowanymi zmianami.
- PM-2 (*Senior Information Security Officer*) – należy utworzyć stanowisko dla specjalisty odpowiedzialnego za bezpieczeństwo informacyjne (w oryginale – *senior information security officer*) który będzie dysponował zasobami niezbędnymi do koordynowania, opracowania, wdrożenia i utrzymywania PBI w całej organizacji.
- PM-3 (*Information Security Resources*) – kierownictwo musi zapewnić niezbędne środki finansowe do wdrożenia PBI i realizacji wynikających z Planu zaleceń.
- PM-4 (*Plan of Action and Milestones Process*) – kierownictwo musi zapewnić odpowiedni nadzór nad realizacją Planu, w szczególności zadbać o terminową realizację wynikających z niego zadań, właściwe ich raportowane oraz uwzględnienie wynikających z niego działań w zarządzaniu ryzykiem biznesowym.
- PM-5 (*Information System Inventory*) – zalecenie wprowadzone w celu spełnienia wymagań FISMA (*Federal Information Security Management Act*).
- PM-6 (*Information Security Measures of Performance*) – dla organizacji powinny zostać opracowane, monitorowane i raportowane wartości wskaźników szacowania skuteczności zabezpieczeń.
- PM-7 (*Enterprise Architecture*) – dla organizacji powinna być opracowana „architektura przedsiębiorstwa" uwzględniająca bezpieczeństwo informacji oraz rezultaty analizy ryzyka dla operacji, zasobów i pracowników organizacji oraz wpływ na inne organizacje i państwo.

[52] Szczegóły – patrz appendix G tego standardu.

- PM-8 (*Critical Infrastructure Plan*) – kierownictwo organizacji musi uwzględnić zagadnienia bezpieczeństwa informacji podczas opracowywania, dokumentowania i uaktualniania planów ochrony infrastruktury krytycznej i kluczowych zasobów.
- PM-9 (*Risk Management Strategy*) – kierownictwo organizacji powinno opracować zrozumiałą strategię zarządzania ryzykiem dla operacji, zasobów i pracowników organizacji oraz innych organizacji i państwa zaangażowanych w ww. operacje, i stosować tę strategię do systemów informacyjnych organizacji. Strategia zarządzania ryzykiem powinna być zaimplementowana w spójny sposób w całej organizacji, powinna być regularnie przeglądana i aktualizowana a wymagane zmiany organizacyjne, wynikające z realizacji procesu zarządzania ryzykiem, powinny być uwzględnione przez kierownictwo organizacji.
- PM-10 (*Security Authorization Process*) – kierownictwo organizacji zarządza (tj. dokumentuje, śledzi, raportuje) poprzez proces „autoryzacji bezpieczeństwa", stan bezpieczeństwa eksploatowanych systemów informacyjnych oraz środowiska pracy tych systemów. W tym celu wybrani pracownicy muszą mieć przydzielone odpowiednie role i zakresy odpowiedzialności związane z procesem zarządzania ryzykiem, a sam proces „autoryzacji bezpieczeństwa" powinien być w pełni zintegrowany z realizowanym w organizacji programem zarządzania ryzykiem.
- PM-11 (*Mission/Business Process Definition*) – kierownictwo organizacji powinno zdefiniować misję (biznesową) z uwzględnieniem bezpieczeństwa informacji i wpływu wyników analizy ryzyka na operacje, zasoby i pracowników organizacji oraz wpływu na inne organizacje i państwo.
- PM-12 (*Insider Threat Program*) – w organizacji powinien być wdrożony program przeciwdziałania incydentom wywołanym przez osobę będącą członkiem organizacji (działającą wewnątrz organizacji z uprawnieniami jej legalnego pracownika), który to program powinien obejmować multidyscyplinarny zespół obsługi takich incydentów.
- PM-13 (*Information Security Workforce*) – kierownictwo organizacji powinna ustanowić program rozwoju i doskonalenia kwalifikacji przez personel przydzielony do zapewniania bezpieczeństwa jej zasobów informacyjnych.
- PM-14 (*Testing, Training, and Monitoring*) – kierownictwo organizacji powinno wdrożyć proces zapewniający, że plany przeprowadzania testów, treningów i monitorowania są opracowane i wykonywane zgodnie z harmonogramem oraz przeglądane pod kątem ich spójności ze strategią zarządzania ryzykiem organizacji i priorytetami organizacji w zakresie działań minimalizujących ryzyko.

- PM-15 (*Contacts with Security Groups and Associations*) – kierownictwo organizacji powinno ustanowić i zinstytucjonalizować kontakty z wybranymi grupami i stowarzyszeniami ze społeczności zajmujących się bezpieczeństwem informacyjnym w celu ułatwienia szkolenia i treningu własnego personelu, „bycia na bieżąco" z rekomendowanymi praktykami, technikami i technologiami oraz dzielenia się informacjami o zagrożeniach, podatnościach i incydentach.
- PM-16 (*Threat Awareness Program*) – kierownictwo organizacji powinno wdrożyć program świadomości zagrożeń, który obejmowałby m.in. wymianę informacji na temat bezpieczeństwa informacji przez wszystkich pracowników, w całej organizacji.

6.2. Zalecenia organizacyjne SANS

W 2008 roku, administracja rządu USA (w tym, m.in. National Security Agency oraz SANS Institute) w porozumieniu z członkami organizacji biznesowych opracowała zbiór zaleceń o nazwie *Consensus Audit Gudelines* (CAG). Zalecenia te zostały udostępnione publicznie przez instytut SANS w 2009 roku pod adresem *www.sans.org*.

Przedstawiony w dokumencie CAG zbiór 20 zalecanych przedsięwzięć z zakresu ochrony przed działaniami intruzów (ang. *Critical Controls*) został uznany przez SANS jako **minimalny, ale łatwy do szybkiego wdrożenia, standard zabezpieczenia systemów i sieci komputerowych przed cyberatakami**. Najnowsza wersja CAG[53] to wersja 7.1. Od wersji 6.0 zmieniła się nazwa dokumentu/projektu na *The CIS Critical Security Controls for Effective Cyber Defense*[54]. Publikacja [40] jest poradnikiem jak zalecenia CIS przystosować do wdrożenia w sieciach i systemach przemysłowych.

Zalecenia dotyczące organizacji zabezpieczania ICS przed atakami to zalecenia 17-20:

- CIS Control 17 – wdrożenie podnoszenia świadomości personelu w zakresie bezpieczeństwa OT i programu treningów (*Implement a Security Awareness and Training Program*).
- CIS Control 18 – zapewnienie bezpiecznego użytkowania bezpiecznych aplikacji (*Application Software Security*).
- CIS Control 19 – zapewnienie obsługi incydentów (*Incident Response and Management*).

---

[53] W czasie przygotowywania niniejszego opracowania, tj. maj 2020 roku. Dostępna pod: https://learn.cisecurity.org/cis-controls-download. CAG jest też krótko opisany w rozdz. 6.1.3 w [4].

[54] CIS − *Center for Internet Security, Inc.*

- CIS Control 20 – wykonywanie testów penetracyjnych i ćwiczeń zespołowych (*Penetration Tests and Red Team Exercises*).

6.3. Zalecenia organizacyjne NERC

Spośród wymienionych w rozdz.4.3 czternastu standardów NERC-CIP, dwa z nich mają istotne znaczenie dla zarządzania bezpieczeństwem systemów sterujących i sieci przemysłowych (w szczególności elektroenergetycznych):

- CIP-003, Cyber Security – Security Management Controls.
- CIP-004, Cyber Security – Personnel & Training.

W ramach prac mających na celu zidentyfikowanie i klasyfikację podatności w sieciach SCADA oraz możliwości ich minimalizowania, US Department of Energy przy współudziale NERC opublikował, m.in. dokument [8]. Jego część dotycząca działań zarządczych, mających na celu ustanowienia efektywnego programu „cyberbezpieczeństwa" zawiera dziesięć następujących zaleceń:

1. Jasne zdefiniowanie w zakresie bezpieczeństwa ról, odpowiedzialności i uprawnień dla menedżerów, administratorów systemowych i użytkowników.
2. Udokumentowanie architektury systemu i zidentyfikowanie systemów pełniących kluczowe funkcje lub przetwarzających/zawierających wrażliwe informacje, które wymagają dodatkowego poziomu ochrony.
3. Ustanowienie dobrze zdefiniowanego, ciągłego procesu zarządzania ryzykiem.
4. Ustanowienie strategii ochrony sieci z wykorzystaniem zasady „ochrony w głąb".
5. Jasne zdefiniowanie wymagań w zakresie „cyberbezpieczeństwa".
6. Ustanowienie efektywnego procesu zarządzania konfiguracją.
7. Wprowadzenie rutynowego procesu samooceny (w zakresie ryzyka lub bezpieczeństwa).
8. Opracowanie i wdrożenie planu odtwarzania systemu i wykonywania kopii bezpieczeństwa systemu.
9. Określenie przez wyższe kierownictwo oczekiwań co do zasad bezpieczeństwa i rozliczanie przestrzegania tych zasad przez pracowników.
10. Ustanowienie polityki (bezpieczeństwa) i przeprowadzanie treningów w celu zminimalizowania prawdopodobieństwa, że personel przypadkowo ujawni wrażliwe informacje odnoszące się do projektu systemu SCADA, realizowanych w nim operacji lub przyjętych zasad bezpieczeństwa.

W dokumencie [29] przedstawiono dziesięć najistotniejszych podatności ICS (patrz rozdz.4.3). Spośród wymienionych tam podatności, trzy dotyczą bezpośrednio działań organizacyjno-zarządczych:

1. Nieodpowiednia polityka, strategie, procedury i mentalność użytkowników w zakresie bezpieczeństwa systemów sterowania.
2. Niewłaściwie analizowane i nadzorowane oprogramowanie w sieciach sterowania.
3. Nieautoryzowane działania i zmiany w sieci sterowania.

Zalecenia mające na celu zminimalizowanie tych podatności, są zatem następujące:

1. Opracować i wdrożyć politykę, strategię i procedury odpowiednie dla zapewnienia bezpieczeństwa systemów sterownia.
2. Wdrożyć program podnoszenia świadomości personelu i użytkowników w zakresie bezpieczeństwa systemów sterowania.
3. Zapewnić poprawne analizowanie i nadzorowanie oprogramowania eksploatowanego w sieciach sterowania.
4. Opracować i wdrożyć procedury przeciwdziałania nieautoryzowanym czynnościom i zmianom w sieciach sterowania.

6.4. Zalecenia organizacyjne Bundesamt für Sichercheit in der Informationstechnik

W [12] jest Tabela 7: *Comparison of the best practices with IEC 62443, VDI/VDE*[55] *2182, NERC CIP*[56] *and DHS*[57] *Best Practices*. Zawiera ona 73 zalecenia, które mogą być podstawą do opracowania listy sprawdzeń do wspomagania audytu bezpieczeństwa sieci przemysłowych. Zalecenia te są w tej tabeli mapowane na zalecenia norm i standardów wymienionych w tytule tabeli.

Zamieszczona dalej w tym artykule tabela 4 to autorski wariant ww. tabeli dla sześciu praktyk wskazanych jako podstawowe dla skutecznego zarządzania bezpieczeństwem informacji sterującej w sieciach i systemach przemysłowych. Bardzo istotne z technicznej perspektywy jest zalecenie 4, które informuje, że struktura sieci powinna być udokumentowana w planie fizycznym i planie logicznym sieci. Plan logiczny sieci nie powinien opisywać jej budowy fizycznej, tylko koncentrować się na jej strukturze i strefach bezpieczeństwa. Z kolei plan fizyczny sieci powinien pokazywać lokalizacje fizycznych elementów ICS, takich jak okablowanie, budynki i bezprzewodowe punkty dostępowe. Oprócz tego, taki plan powinien zawierać co najmniej:

- adresy sieciowe IP i maski, np. 192.168.1.0/24,

[55] Verein Deutscher Ingenieure/Verband der Elektrotechnik Elektronik Informationstechnik.
[56] North American Electric Reliability Corporation Common Industrial Protocol.
[57] Department of Homeland Security.

- adresy sieciowe wszystkich interfejsów połączonych sieci, np. 192.168.1.52,
- adresy MAC,
- nazwy komputerów i ich funkcje w sieci,
- (jeżeli występują) nazwy DNS,
- (jeżeli występuje) FQDN (FullyQualifiedDomainName)

Dokumentacja techniczna, w tym plany różne, powinny mieć właściciela i być regularnie przeglądane i uaktualniane od początku cyklu życia systemu.

Tab. 4. Zalecane przez Bundesamt für Sichercheit in der Informationstechnik praktyki w zakresie zarządzania bezpieczeństwem ICS.

Lp.	**Zalecane praktyki** (ICS Security Compendium v. 1.23)	**Odpowiednik w normie IEC 62443**	**Komentarze**
1	Właściciele zasobów powinni ustanowić organizację zarządzania i kontrolowania ról i odpowiedzialności w zakresie bezpieczeństwa elementów ICS.	2-1 chapter A.3.2.3 2-1 chapter 4.3.2.3 2-1 chapter 4.3.2.3	Dotyczy wszystkich aktorów mających styczność z elementami ICS, np. dostawców produktów.
2	Zadbać o właściwe wytwarzanie i zarządzanie dokumentacją ICS	2-1 chapter A.3.4.4 2-1 chapter 4.2.3.13	Należy opisać cykl życia dokumentacji
3	Utworzyć SZBI dla informacji wykorzystywanych przez ICS	Complete 2-1	System Zarządzania Bezpieczeństwem Informacji (SZBI)
4	Utrzymywać plan sieci (fizyczny i logiczny) na którym jest uwidocznione rozmieszczenie elementów ICS.	2-1 chapter A.3.4.2.3.3 2-1 chapter 4.2.3.5	
5	Utrzymywać, w celu zapewnienia spójności, listę eksploatowanego oprogramowania i listę plików konfiguracyjnych dla elementów ICS.	2-1 chapter 4.2.3.4 3-1 chapter 8.7	
6	Wytworzyć, utrzymywać i udostępniać zainteresowanym dokumentację operacyjną dla administratorów i użytkowników ICS.	2-1 chapter A.3.3.5	Ang. *Administration and user manual*

Uzupełnieniem zalecenia 4 jest zalecenie 5, odnoszące się do eksploatowanego w ICS oprogramowania. Zaleca ono prowadzenie szczegółowej, regularnie uaktualnianej listy plików konfiguracyjnych komponentów ICS oraz danych identyfikacyjnych (wraz z ustawieniami konfiguracyjnymi) eksploatowanego oprogramowania. Ma to na celu przeciwdziałanie niekompatybilności i niespójności związanych z różnymi wersjami eksploatowanego oprogramowania oraz umożliwienie szybkiej identyfikacji oprogramowania wymagającego uaktualnienia bądź odnowienia licencji. Taka lista powinna zawierać co najmniej:

- nazwę programu,
- nazwę komputera-nosiciela oprogramowania,
- wskazanie fizycznego miejsca instalacji tego oprogramowania,
- adres MAC,
- adres IP,
- FQDN,
- system operacyjny pod którym oprogramowania działa,
- używane protokoły i porty,
- status uaktualnienia wraz z datą instalacji uaktualnienia,
- datę ostatniego skanowania w poszukiwania wirusów,
- zakres oraz rodzaj kopii bezpieczeństwa (pełna, przyrostowa, różnicowa) oraz datę i czas ostatniego wytworzenia kopii bezpieczeństwa,
- dane kontaktowe do administratora danego oprogramowania.

7. Podsumowanie

Zainteresowani bezpieczeństwem informacyjnym czytelnicy zapewne zauważą, że zalecenia dotyczące zarządzania ochroną informacji sterującej w sieciach i systemach przemysłowych nie różnią się od zaleceń podawanych dla „klasycznych" systemów informacyjnych. Zatem jak zwykle, „diabeł tkwi w szczegółach" i w tym przypadku chodzi o szczegóły techniczne konstrukcji, wdrożenia i eksploatacji zabezpieczeń. Natomiast sposób utrzymywania i zarządzania „bezpieczeństwem", czy to dla systemów informacyjnych, czy systemów przemysłowych, czy też systemów hybrydowych, jest taki sam.

Każdy ze zbiorów opisanych w rozdz. 5 rekomendacji dotyczących zarządzania ochroną informacji sterującej wskazanych przez NIST (SP 800-53), SANS (CIS-ICS), NERC (CIP) oraz niemiecki BSI (Kompendium) zawierał, czasami różnie sformułowane, ale co do meritum identyczne, zalecania dotyczące:

1. Opracowania, spisania i wdrożenia strategii/polityki bezpieczeństwa ICS.

2. Ustanowienie procesu zarządzania ryzykiem oraz wykorzystania wyników analizy ryzyka przy opracowywaniu i wdrażania strategii, polityki oraz planów i procedur z zakresu bezpieczeństwa ICS.
3. Ustanowienia, opisania w odpowiednich dokumentach i przydzielenia wybranym pracownikom ról z zakresu zarządzania i utrzymywania wymaganego poziomu bezpieczeństwa ICS.
4. Opracowania i wdrożenia programu stałego podnoszenia świadomości personelu w zakresie bezpieczeństwa ICS, w szczególności znajomości zasad polityki bezpieczeństwa.
5. Opracowania i wdrożenia planów przeprowadzania testów, treningów i monitorowania stanu bezpieczeństwa ICS.
6. Opracowania i wdrożenia procedur autoryzowania działań użytkowników ICS w sieciach i systemach sterowania oraz procedur przeciwdziałania nieautoryzowanym czynnościom i zmianom w ICS.
7. Wytworzenia dokumentacji bezpieczeństwa ICS: zarządczej (strategie, polityka, plany), operacyjnej (podręczniki dla administratorów i użytkowników ICS), inwentaryzacyjnej (schematy sieci i systemów, spisy urządzeń i oprogramowania, zawartość plików konfiguracyjnych sprzętu i oprogramowania), bieżącej (dokumentującej eksploatację ICS), szkoleniowej.
8. Właściwego zarządzania (przeglądania, aktualizacji i udostępniania) dokumentacji bezpieczeństwa ICS.

Zatem zsyntetyzowany zbiór dobrych praktyk dotyczących, zgodnie z tytułem artykułu, zarządzania ochroną informacji sterującej w systemach przemysłowych, sprowadza się do ww. ośmiu zaleceń.

8. Literatura

1. DesRuisseaux D.: *Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications*. Schneider Electric White Paper. 2018.
2. Filkins B., Wylie D.: *SANS 2019 State of OT/ICS Cybersecurity Survey*. ©2019 SANS™ Institute. June 2019.
3. Goble W.: *Applying the Global Automation Standard IEC 62443 to protect against cyber threats*. Prezentacja. 2019.
4. Liderman K.: *Bezpieczeństwo informacyjne. Nowe wyzwania*. WN PWN SA. Warszawa. 2017.
5. Liderman K.: *Bezpieczeństwo informacyjne*. WN PWN SA. Warszawa. 2012.

6. Szmuc T., Motet G.: *Specyfikacja i projektowanie oprogramowania czasu rzeczywistego*. CCATIE. Katedra Automatyki AGH. Kraków. 1998.
7. Żurakowski Z.*: Systemy komputerowe w zastosowaniach związanych z bezpieczeństwem*. Str.20-28. W: Informatyka. nr 3. 1995.
8. *21 Steps to Improve Cyber Security of SCADA Networks*, Office of Energy Assurance, U.S. Department of Energy, http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf. (dostęp 16.05.2020)
9. ENISA: *Industry 4.0 Cybersecurity: Challenges&Recommendations*. May.2019.
10. ENISA: *Analysis of ICS-SCADA Cyber Security Maturity Levels In Critical Sectors*. 2015.
11. GAO-04-354, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, U.S. GAO, 2004, http://www.gao.gov/new.items/d04354.pdf. (dostęp 16.05.2020)
12. *ICS Security Compendium*. V. 1.23. Federal Office for Information Security (BSI). Germany. 2013.
13. IEC 62443-1-1: Industrial communication networks - Network and system security - Part 1-1: *Terminology, concepts and models* (IEC/TR 62443-1-1:2009).
14. ISA-62443-1-2: Security for industrial automation and control systems - *Master Glossary*. Draft 1. Edit 5. August 2014 (ISA-TR62443-1-2).
15. ISA-62443-1-3: Security for industrial automation and control systems.- Part 1-3: *Cyber security system conformance metrics*. Draft 1. Edit 19. October 2015.
16. ISA-62443-2-1: Security for industrial automation and control systems: Part 2-1: *Industrial automation and control system security management system*. Draft 7. Edit 5. November 9. 2015.
17. ISA-62443-2-2: Security for industrial automation and control systems: *Implementation Guidance for and IACS Security Management System*. Draft 1. Edit 4. April 2013.
18. IEC 62443-2-3: Security for industrial automation and control systems: Part 2-3: *Patch Management in IACS environment* (IEC /TR 62443-2-3:2015).
19. IEC 62443-2-4: Security for industrial automation and control systems: Part 2-4: *Security program requirements for IACS providers* (IEC 62443-2-4:2015).
20. ISA-62443-3-2: Security for industrial automation and control systems: *Security risk assessment for system design*. Draft 6. Edit 3. August 5. 2015.
21. IEC 62443-3-3: Industrial communication networks - Network and system security - Part 3-3: *System security requirements and security levels* (IEC 62443-3-3: 2013).

22. IEC/NP 62443-4-1 Industrial communication networks - Network and system security - Part 4-1: *Product development requirements based on ISA-62443-04-01*. Draft 1. Edit 9. April 2013.
23. ISA-62443-4-1 Security for industrial automation and control systems Part 4-1: *Secure product development life - cycle requirements*. Draft 3. Edit 11. March 2016.
24. ISA-62443-4-2 Security for industrial automation and control systems *Technical security requirements for IACS components.* Draft 2. Edit 4. July 2. 2015.
25. NERC : *Top 10 vulnerabilities of control systems and their associated mitigations*. 2006.
26. NIST Special Publication 800-82 rev.2: *Guide to Industrial Control Systems (ICS) Security*. May 2015.
27. NIST Special Publication 800-53 Rev.5: *Security and Privacy Controls for Federal Information Systems and Organizations*. August 2017.
28. NISTIR 8276 (draft): *Key Practices in Cyber Supply Chain RiskManagement: Observations from Industry*. February. 2020.
29. NISTIR 8183A: Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: *Volume 1 – General Implementation Guidance*. September. 2019.
30. NISTIR 8183A: Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: *Volume 2 – Process-based Manufacturing System Use Case*. September. 2019.
31. NISTIR 8183A: Cybersecurity Framework Manufacturing Profile Low Impact Level Example Implementations Guide: *Volume 3 – Discrete-based Manufacturing System Use Case*. September. 2019.
32. PN-EN 61508-1:2010P: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem − Część 1: Wymagania ogólne
33. PN-EN 61508-2:2010E: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem − Część 2: Wymagania dotyczące elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem
34. PN-EN 61508-3:2010E: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem − Część 3: Wymagania dotyczące oprogramowania

35. PN-EN 61508-4:2010E: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem − Część 4: Definicje i skrótowce
36. PN-EN 61508-5:2010E: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem − Część 5: Przykłady metod określania poziomów nienaruszalności bezpieczeństwa
37. PN-EN 61508-6:2010E: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem − Część 6: Wytyczne do stosowania IEC 61508-2 i IEC 61508-3
38. PN-EN 61508-7:2010E: Bezpieczeństwo funkcjonalne elektrycznych/elektronicznych/programowalnych elektronicznych systemów związanych z bezpieczeństwem − Część 7: Przegląd technik i miar
39. US Industrial Control Systems Cyber Emergency Response Team: *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. September. 2016.
40. https://www.cisecurity.org/controls/: *Implementation Guide for Industrial Control Systems*. Version 7. CIS Controls™ (dostęp 22.05.2020).

ABSTRACT

MANAGING CONTROL INFORMATION PROTECTION IN INDUSTRIAL NETWORKS AND SYSTEMS

Summary: This chapter presents issues of security of industrial networks and systems related to the protection of production data and information controlling (not only) production processes. After a brief overview of the types of industrial networks and systems, with particular emphasis on the properties of real-time systems, the basic norms and standards for this problem area are briefly described: IEC 61508, IEC 62443, NIST SP 800-82 and NIST 800-53. A collection of "good practices" identified by NERC and the Bundesamt für Sichercheit in der Informationstechnik is also presented. On this basis, a set of good practices for the management of control information protection in industrial networks and systems was developed at the end of the article.

Keywords: industrial systems and networks, safety of industrial control networks, SCADA, IEC 61508, IEC 62443, NIST SP 800-82.

ROZDZIAŁ 4

WYZWANIA W ZAKRESIE ZAPEWNIANIA CYBERBEZPIECZEŃSTWA OBIEKTOM INFRASTRUKTURY PORTOWO-MORSKIEJ

dr inż. Jakub SYTA [58]

STRESZCZENIE: W rozdziale przedstawiono różnorodność oraz znaczenie zagadnień cyberbezpieczeństwa dla szeroko pojętej infrastruktury portowo-morskiej bazując na historycznych oraz hipotetycznych przykładach. Zagadnienia zostały podzielone na oszustwa, różnorodne incydenty kończące się przerwaniem ciągłości procesów biznesowych, a także nadchodzące zagrożenia, jeszcze rzadkie, lecz mogące z czasem odgrywać coraz większą rolę.

SŁOWA KLUCZOWE: cyberbezpieczeństwo, zagrożenia, porty, infrastruktura morska.

Cyberbezpieczeństwo przez lata mogło się kojarzyć rozgrywkami wywiadów potężnych państw i zagrożeniami, którymi zajmowały się wyłącznie najbogatsze z banków. Między i nnymi z tego powodu wiele mniejszych organizacji, jak również wiele potężnych, lecz działających w branżach dalekich od najnowszych technologii, nie traktowała priorytetowo tego zagadnienia.

[58] Morskie Centrum Cyberbezpieczeństwa AMW, jakub.syta@bezpiecznik.pl; ORCID: 0000-0002-0115-6432.

Sytuacja jednak wygląda inaczej – atak może dotknąć każą organizację w dowolnym momencie. Każdą, czyli nie tylko taką, która całość swojej działalności prowadzi w cyberprzestrzeni. Cyberataki dotykają również te z organizacji, których działalność jest przede wszystkim widoczna w świecie realnym np. w przedsiębiorstwach produkcyjnych oraz tzw. „twardej infrastrukturze". Takie organizacje często zupełnie gdzie indziej nakładają swoje priorytety, twierdząc, nie bez racji, że obszar nowoczesnych technologii IT jedynie wspomaga ich kluczowe procesy. Później jednak, w bardzo bolesny sposób, orientują się, że ten „wspomagający" obszar rozrósł się tak bardzo, by stać się krytycznym dla zapewnienia ciągłości całej organizacji.

W niniejszym artykule Autor pragnie zaprezentować różnorodność oraz znaczenie zagadnień cyberbezpieczeństwa dla szeroko pojętej infrastruktury portowo-morskiej bazując na historycznych oraz hipotetycznych przykładach. Zagadnienia zostały podzielone na oszustwa, różnorodne incydenty kończące się przerwaniem ciągłości procesów biznesowych a także nadchodzące zagrożenia, jeszcze rzadkie lecz mogące z czasem odgrywać coraz większą rolę.

Probvem badawczy

Infrastrukturę portowo-morską można podzielić na elementy liniowe i węzłowe (punktowe)[59]. Patrząc na ich zakres, istotny dla dalszych rozważań, można zauważyć, że elementy liniowej infrastruktury obejmują m. in. boje oraz latarnie morskie. Infrastruktura punktowa obejmuje natomiast, m. in. porty: handlowe, rybackie, jachtowe i wojenne. Port morski to umieszczony na zetknięciu się lądu z morzem obiekt przygotowany pod względem technicznym, organizacyjnym, ekonomicznym i prawnym do różnego rodzaju relacji lądowo morskiej i morsko-lądowej[60]. Infrastrukturę portu można z kolei podzielić na:

- infrastrukturę dostępu do portu obejmującą, m. in. kanały, śluzy, falochrony, drogi samochodowe, tory kolejowe;

59 Tubielewicz A., Zarządzanie logistyczne w transporcie morskim, Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, Gdańsk 2015, str. 1043–1054.
60 Ibidem.

- infrastrukturę wewnątrz-portową obejmującą nabrzeża, kanały, baseny, drogi portowe, obiekty i urządzenia transportu wodnego śródlądowego, systemy instalacyjne, systemy obiegu informacji;
- suprastrukturę portową obejmującą magazyny, place, urządzenia przeładunkowe, sprzęt zmechanizowany, urządzenia i wyposażenie pomocnicze.

Systemy IT wykorzystywane w portach wchodzą w interakcje z wieloma różnymi systemami. Coraz większa ilość informacji jest wymieniana w sposób automatyczny w ramach następujących kategorii[61]:

- obowiązkowe deklaracje i manifesty zgłaszane władzom portów oraz krajowym i międzynarodowym instytucjom;
- dokumenty upoważniające, potwierdzające np. zgodę na wejście do portu czy rozładunek;
- dane operacyjne związane z procesami realizowanymi przez port, np. potrzeby w zakresie tankowania czy harmonogramy operacji cargo;
- dane finansowe dotyczące np. faktur i płatności;
- dane nawigacyjne (GPS, AIS).

Przytoczenie powyższych przykładów jest istotne dla dalszych rozważań w zakresie zapewniania cyberbezpieczeństwa. Podkreśla bowiem różnorodność obiektów, które przetwarzają (przechowują, przesyłają, modyfikują) informacje. Dla różnych z rodzajów informacji przetwarzanych w różnych z obiektów zupełnie inną wagę będą mieć podstawowe właściwości bezpieczeństwa informacji. Międzynarodowa norma ISO 27001:2013[62] ustanawiająca wymagania dla bezpieczeństwa informacji wskazuje na następujące własności:

- poufność - mająca na celu zapewnienie, że informacja może być przekazana wyłącznie dla upoważnionych osób/procesów;

---

61 Drougkas A. (*et al.*), Good practices for cybersecurity in the maritime sector, ENISA 2019, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector.

62 ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO 2013.

- dostępność - potwierdzająca, że z informacji można skorzystać bezzwłocznie, gdy jest taka potrzeba;
- integralność - zapewniająca, że informacje nie zostały w nieautoryzowany sposób zmodyfikowane i są ze sobą spójne;
- rozliczalność - zapewniająca, że można odtworzyć niebezpieczne czynności wykonywane przez poszczególne osoby mające dostęp do informacji;
- autentyczność - która ma na celu zapewnienie, że informacja nie została podrobiona oraz że pochodzi z właściwego źródła;
- niezaprzeczalność - która potwierdza, że żaden z użytkowników nie może wyprzeć się wykonania określonych czynności przetwarzania informacji;
- niezawodność - zapewniająca, że systemy przetwarzające informacje funkcjonują w sposób nieprzerwany i bez błędów.

W ostatnich dziesięcioleciach, wraz z gwałtownym rozwojem globalnego handlu, można zauważyć bardzo szybki wzrost modernizacji portów. By nadążyć za potrzebami międzynarodowego handlu wdrażane są kolejne nowoczesne technologie. Obejmują one rozwiązania dla coraz szybszego gromadzenia oraz przetwarzania coraz potężniejszych ilości informacji, co stosowane bywa między innymi do automatyzacji wykonywanych czynności. Związane jest to zresztą z definiowaniem i budowaniem kolejnych generacji portów[63]. IV generacja portów miała uwzględniać takie kryteria jak: jakość usług portowych, wykorzystanie informatyki, kształtowanie środowiska interesariuszy czy istnienie klastra portowego/morskiego, konteneryzacja strumienia ładunków, stosowanie zaawansowanych rozwiązań automatyki, pełną integrację z branżą transportową oraz spedycyjną czy wykorzystanie TQM. Pojawiająca się obecnie V generacja ma dodatkowo koncentrować się na klientach oraz społeczności lokalnej, oferując głęboką integrację informatyczną z interesariuszami.

63 Kaliszewski A., Porty piątej oraz szóstej generacji (5GP, 6GP) - ewolucja ekonomicznej i społecznej roli portów, Studia i Materiały Instytutu Transportu i Handlu Morskiego 2017, str. 93-123.

Między innymi z tego powodu coraz powszechniej wdraża się koncepcję Przemysłu 4.0, która obejmuje [64]:

- autonomiczne systemy i roboty;
- integrację horyzontalną i wertykalną wykorzystywanych systemów;
- wykorzystywanie chmury obliczeniowej;
- druk 3D;
- przetwarzanie potężnych zbiorów informacji (ang. Big Data);
- rozszerzoną rzeczywistość (ang. Augumented Reality);
- symulacje (ang. Simulation Management);
- zapewnienie cyberbezpieczeństwa.

Autor pragnie zwrócić szczególną uwagę na ostatni z tych punktów, gdyż nie można wdrażać nowoczesnych technologii bez zastosowania adekwatnych zabezpieczeń. Jego znaczenie jest zresztą coraz częściej sygnalizowane. Pośród trzech największych wyzwań dla portów cyberbezpieczeństwo wymienia się tuż obok piractwa i terroryzmu.[65]

W literaturze przedmiotu podkreśla się że dla funkcjonowania portu kluczowe jest zachowanie następujących atrybutów[66]:

- szybkość i wydajność prowadzonej działalności;
- umiejętność prowadzenia działań w sposób bezpieczny;
- zapewnienie bezpieczeństwa i zasad higieny pracy dla personelu;
- zapewnienie integralności infrastruktury fizycznej.

64 Rüßmann M. (*et al.*) Industry 4.0: the Future of Productivity and Growth in Manufacturing Industries. Technical Report. Boston Consulting Group 2015, https://image-src.bcg.com/Images/Industry_40_Future_of_Productivity_April_2015_tcm9-61694.pdf .

65 DeepTrekker, Top 3 Risks at our Ports, https://www.deeptrekker.com/resources/maritime-port-security-risks.

66 Drougkas A. *op. cit.*

Ze względu na to, że powyższe w znaczniej mierze bazuje na poprawnie funkcjonujących systemach informatycznych, zapewnienie cyberbezpieczeństwa staje się jednym z priorytetów dla nowoczesnych portów. By to osiągnąć konieczne jest jednak zidentyfikowanie i zrozumienie zagrożeń, przed którymi przede wszystkim należy się ochronić.

Oszustwa

Oszustwa wydają się być najpowszechniejszym z ataków, gdyż są zdecydowanie najłatwiejsze do przeprowadzenia. Mimo, że wiele organizacji, szczególnie działających w branży logistycznej, ma z nimi do czynienia od wieków, w ostatnich latach można zaobserwować rozkwit nowych technik stosowanych przez przestępców.

Najczęstsze z ataków dotyczą próby kradzieży środków finansowych. Tak zwane ***ataki phishingowe*** mają na celu oszukanie odbiorców, przekonanie ich do wykonania potencjalnie niebezpiecznych czynności, którymi może być otwarcie załącznika do poczty elektronicznej, wejście na stronę www czy ujawnienie treści wrażliwych danych. Prostsze z ataków wymagają dalszej interakcji z ofiarą – tego by uruchomiła ona makra w pliku (czego w 99% przypadków w żadnym wypadku nie należy czynić), bądź też zainstalowania ze strony www dodatkowego oprogramowania, udającego, np. nową wersję oprogramowania (wszelkie dodatki powinny być instalowane przez osoby świadome cyberzagrożeń, np. z działu IT). Warto jednak wiedzieć, że najbardziej zaawansowane ataki nie wymagają takich interakcji, a samo odwiedzenie strony www może zainfekować komputer i pozwolić na realizację dalszych faz ataku. Stąd niezbędne w obecnych czasach jest korzystanie z zaawansowanych systemów bezpieczeństwa oraz nauczenie pracowników rozpoznawania oszukańczych wiadomości. Realizuje się to poprzez tzw. testy socjotechniczne oraz szkolenia podnoszące świadomość.

W momencie gdy przestępca zainstaluje na komputerze ofiary szkodliwy kod będzie w stanie poznać stosowane przez ofiarę dane identyfikujące i uwierzytelniające, takie jak loginy oraz hasła dostępu, pozna narzędzia, z których ona korzysta. Może tym samym, w dalszej kolejności, próbować:

- zmodyfikować tzw. dane statyczne, czyli np. numery rachunków trzymane w bazach danych czy arkuszach kalkulacyjnych czekając aż ofiara sama zacznie mu przesyłać dane;
- zmodyfikować przelewy w trakcie ich realizacji (tzw. technika man-in-the-middle) co jest trudniejsze, ale również wykonywalne, np. poprzez modyfikowanie numerów

rachunków w momencie, gdy wklejane są z pamięci operacyjnej do systemów bankowych;

- przekierować ofiarę na stronę fałszywego banku licząc, że ofiara nie czytając komunikatów z aplikacji bankowej wskaże jako „zaufane" konto kontrolowane przez przestępców;
- zacznie w imieniu ofiary prowadzić dalszą korespondencję próbując oszukać inne osoby – np. przekonać do wysłania przelewu na fikcyjne konto czy do zainstalowania szkodliwego oprogramowania.

Ostatni z tych przykładów często jest wykorzystywany do ataków typu ***BEC – Business E-mail Compromise.*** Oszuści podszywają się wówczas pod „ważną osobę" – np. członka zarządu przedsiębiorstwa lub przedstawiciela kontrahenta znanego ofierze z innych – rzeczywistych transakcji. Tworzona jest wówczas odpowiednia, wiarygodna historia oraz wywierana jest presja czasowa licząc, że ofiara „wyjątkowo" nie będzie przestrzegać wszystkich „biurokratycznych" procedur i „sprawnie" zrealizuje prośbę. W ten sposób, tak zwanym „mailem od prezesa" przestępcy próbują zmienić dotychczasowe numery rachunków i z sukcesem kraść wielomilionowe kwoty[67], [68].

Warto zwrócić uwagę, że opisywane powyżej oszustwa nie muszą dotyczyć prób kradzieży środków finansowych. Patrząc na ataki, które mogłyby szczególnie zaszkodzić organizacjom działającym w branży portowej i logistycznej scenariusze ataku mogą być znacznie „ciekawsze" – przykładowo mogą dotyczyć prób:

- wydania towaru nieuprawnionej osobie;
- wyłudzenia informacji nt. szczegółowej zawartości kontenerów;
- przekierowania kontenera w inne miejsce w celu zaszkodzenia konkurencji;

---

67 Roberts J., Exclusive: Facebook and Google Were Victims of $100M Payment Scam, https://fortune.com/2017/04/27/facebook-google-rimasauskas/.

68 TVN24, Zapłacili oszustowi. Lecą głowy w Metrze Warszawskim, https://tvn24.pl/tvnwarszawa/najnowsze/zaplacili-oszustowi-leca-glowy-w-metrze-warszawskim-241057.

- ukrywania kontenerów wykorzystywanych do przestępczej działalności, np. przemytu narkotyków[69], przemytu ludzi czy nawet wykorzystywania ich jako sale tortur[70].

Powyższe przykłady mają na celu zilustrować, jak istotne dla funkcjonowania portów, oraz powiązanych z nimi organizacji jest zapewnienie poufności, integralności, autentyczności, rozliczalności i niezaprzeczalności informacji.

Przerwanie procesów biznesowych

Opisana w poprzednim podrozdziale infekcja komputerów szkodliwym oprogramowaniem coraz częściej ma też inne skutki, bardziej widoczne niż kradzież informacji uwierzytelniających. Gdy przestępcy zorientują się, że udało się im dostać do sieci wewnętrznej organizacji, które obraca znaczną ilością pieniędzy, coraz częściej postanawiają sięgnąć do szantażu. Zamiast kraść setki tysięcy czy pojedyncze miliony złotych, co jest typowym oszustwem BEC, wolą otrzymać znacznie większy okup wykonując atak na kolejną właściwość bezpieczeństwa informacji, jaką jest dostępność. W momencie pisania tego artykułu największy znany okup zażądany przez przestępców wynosił 50 000 000 dolarów[71].

Osiąga się to stosując tzw. ***atak ransomware***. Polega on zaszyfrowaniu serwerów i stacji roboczych zawierające dane niezbędne do prowadzenia działalności gospodarczej. Często równocześnie przestępcy potrafią zaszyfrować kopie zapasowe. Komputery sterują infrastrukturą, przetwarzają informacje o towarze, trasie, nadawcach, odbiorcach. Utrata tych informacji prowadzi do potężnych problemów nie tylko wśród firm działających bezpośrednio w branży logistycznej. Dotyka wszystkich dziedzin gospodarki, o czym przekonały się największe firmy logistyczne takie jak Mearsk[72] (który musiał wydać ok 300 milionów dolarów

69 Ubmemea, Antwerp incident highlights maritime IT security risk, artykuł dostępny pod adresem https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk .

70 Niebezpiecznik.pl, Komnaty tortur namierzone przez policję. Dzięki włamaniu na telefon oprawców…, artykuł dostępny pod adresem https://niebezpiecznik.pl/post/komnaty-tortur-namierzone-przez-policje-dzieki-wlamaniu-na-telefon-oprawcow/.

71 Abrams L., Computer giant Acer hit by $50 million ransomware attack, artykuł dostępny pod adresem https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/.

72 Chirgwin R., IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation blitz, https://www.theregister.com/2018/01/25/after_notpetya_maersk_replaced_everything/.

by odtworzyć działalność po cyberataku), COSCO i MSC[73], a także operatorzy portów np. w Barcelonie[74] czy San Diego[75]. Brak możliwości otrzymania podzespołów przerywał procesy produkcyjne w fabrykach, zbyt długo nieodebrane towary się psuły. Zrozumiałe, że w takiej sytuacji wobec podmiotów winnych zaniechań w obszarze bezpieczeństwa IT, pojawiały się żądania wielomilionowych odszkodowań.

Odtwarzanie wszystkich systemów informatycznych to zadanie na wiele dni czy nawet tygodni, w zależności od wielkości infrastruktury IT. Wymaga to przede wszystkim posiadania możliwie aktualnych kopii bezpieczeństwa, co niestety bywa zbyt często zaniedbywane. Część przedsiębiorstw, która posiada aktualne kopie zapasowe i chce samodzielnie odzyskać ciągłość funkcjonowania musi jednak sprostać kolejnemu zagrożeniu. Przestępcy, aby dodatkowo zmusić firmy do zapłaty okupu, kradną wpierw wrażliwe dane oraz grożą ich opublikowaniem. Znane są więc organizacje, które postanawiają w takiej sytuacji zapłacić okup. Warto przy tej okazji zauważyć, że nie jest pewne czy przestępcy po uzyskaniu okupu będą chcieli przekazać kody. Nie jest też oczywiste czy przekazane kody na pewno zadziałają. Nawet jeżeli tak będzie, to trzeba pamiętać, że odzyskiwanie zaszyfrowanej infrastruktury może zająć całe tygodnie.

Innym rodzajem ataku, który jest w stanie w zdecydowanym stopniu utrudnić komunikację z klientami są ***ataki DDoS***. Mimo, że nie są tak zauważalne jak w poprzednich latach, to nieustannie rosną pod względem wolumenu. W momencie pisania niniejszego artykułu nieoficjalnym rekordzistą Polski był atak o wolumenie przekraczającym 400 Gbps na jednego z klientów mobilnych firmy Orange[76]. Tak potężne ataki, jeżeli nie są chronione zaawansowanymi systemami bezpieczeństwa, są w stanie nie tylko zablokować łącza klienta przez cały czas trwania ataku, ale przede wszystkim mogą unieruchomić urządzenia sieciowe uniemożliwiając dostęp do infrastruktury na czas trwania naprawy.

---

73 Kapadia S., 3 years, 3 cyberattacks on major ocean carriers. How can shippers protect themselves?, https://www.supplychaindive.com/news/ocean-carrier-cybersecurity-maersk-msc-cosco/576754/.

74 Esage A., Hacking attack in port of Barcelona, https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/.

75 Tsonchew A., Troubled waters: Cyber-attacks on San Diego and Barcelona's ports, https://www.darktrace.com/en/blog/troubled-waters-cyber-attacks-on-san-diego-and-barcelonas-ports/.

76 CERT OPL, 400 Gbps przebite - mamy rekordowy DDoS, https://cert.orange.pl/aktualnosci/400-gbps-przebite-mamy-rekordowy-ddos.

Jednak nie tylko ransomware czy ataki DDoS są w stanie zablokować funkcjonowanie infrastruktury portowej. Kolizje wywołane przez nieautoryzowane manipulowanie środkami łączności, o których piszę w kolejnym rozdziale, jak również wyrafinowane ataki na autonomiczne pojazdy, jak np. AGV, mogą również wprowadzić chaos i doprowadzić do wypadków przyczyniając się do przerwania procesów biznesowych[77]. A przypadków zainfekowania infrastruktury morskiej ***szkodliwym oprogramowaniem*** jest coraz więcej[78]. Kwestią czasu pozostaje np. kiedy udane ataki zaszkodzą pracy boi i latarni morskich.

Nadchodzące zagrożenia

Opisane we wcześniejszej części artykułu zagadnienia są już codziennością. Kampanie phishingowe, oszustwa BEC, ataki typu ransomware czy DDoS każdego dnia dotykają dziesiątek a nawet setek podmiotów - w tym również operatorów portów czy firm logistycznych. W tej części artykułu zasygnalizowane zostaną cyberzagrożenia specyficzne dla infrastruktury portowo-morskiej.

Większość okrętów do nawigacji wykorzystuje sygnał GPS. Technologia ta nie jest jednak odporna na ataki i istnieją możliwości zagłuszania (tzw. ***jamming***) bądź też modyfikowania sygnału (tzw. ***spoofing***). Obserwowane było to między innymi podczas manewrów wojskowych[79], chociaż nie we wszystkich przypadkach widoczne są jednoznaczne korelacje[80]. Próby utrudnienia marynarce wojennej prowadzenia ćwiczeń czy działań operacyjnych może również dotknąć jednostki cywilne. Tego typu działania mogą doprowadzić, np. do zderzeń czy wpłynięcia na mieliznę i w konsekwencji utraty części ładunku, uszkodzeń statku a nawet katastrof ekologicznych.

Innym zagrożeniem, które przede wszystkim mogłoby się objawić w portach, byłoby zagłuszanie komunikacji na kierunku kapitanat/statek. Łączność radiowa nie jest odporna

77 Kemme, N., Design and Operation of Automated Container Storage Systems, PhysicaVerlag Heidelberg 2013.

78 Knet 360, Collaboration in the Shipping Industry: Innovation and Technology, https://knect365.com/maritime/article/91705d00-6d9d-4ba3-98a4-9b10c92ad520/epaper-collaboration-in-the-shipping-industry-innovation-and-technology.

79 Goward D., GPS disrupted for maritime in Mediterranean, Red Sea, 2018, https://www.gpsworld.com/gps-disrupted-for-maritime-in-mediterranean-red-sea/.

80 The Navigation Center of Excellence, GPS Problem Reports Status, https://navcen.uscg.gov/?Do=GPSReportStatus.

na próby ataków a zablokowanie kanału radiowego, w najlepszym wypadku mogłoby doprowadzić do zamieszania, w gorszych scenariuszach do kolizji. Co gorsza przeprowadzenie tego typu ataków nie wymaga znacznych nakładów finansowych, choć pewnym zabezpieczeniem jest konieczność fizycznego zbliżenia się do atakowanej infrastruktury.

Zupełnie nowe ryzyka pojawią się wraz z rozpowszechnieniem autonomicznych okrętów. Prace w tym zakresie trwają od lat i są na tyle zaawansowane, że już przede wszystkim względy regulacyjne powodują, że nie stanowi to codzienności żeglugi morskiej. Autonomiczne jednostki są jednak podatne na zakłócenia komunikacji, o co nie trudno na morzu. Decyzje podejmowane są w oparciu o algorytmy uczenia maszynowego (ang. machine learning), które również bywa podatne na manipulacje i oszustwa, w wyniku czego podejmowane są irracjonalne decyzje[81], [82].

Wykorzystanie robotów w pracach portowych mimo oczywistych korzyści znów może prowadzić do tragedii[83], szczególnie jeżeli przestępcom uda się w nieautoryzowany sposób wpłynąć na ich funkcjonowanie. Autor żywi nadzieję, że ilość przypadków śmiertelnych będzie utrzymywać się na niewielkim poziomie, ale spodziewa się jednocześnie, że wraz z rozpowszechnianiem urządzeń IoT ilość przerw, wypadków, awarii czy błędów będzie coraz większa. Należy bowiem podkreślić, że urządzenia IoT służące powszechnie jako czujki i sterowniki są bardzo często są przygotowywane wbrew najlepszym praktykom z zakresu cyberbezpieczeństwa[84].

Rekomendacje

Przykłady historycznych jak i hipotetycznych cyberataków można mnożyć dalej. Nie jest to jednak celem niniejszego artykułu. To jest istotne to by osoby decyzyjne w świadomy sposób mogły podejmować decyzje dotyczące wdrażania nowych technologii – uwzględniając zarówno oczywiste korzyści jak i mniej oczywiste ryzyka. By od dostawców nowych techno-

81 OpenAI, Multimodal Neurons in Artificial Neural Networks, https://openai.com/blog/multimodal-neurons/.

82 Nassi B. (*et al.*), Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems, Uniwersytet Ben-Gurion, Negev, Israel, 2020, https://eprint.iacr.org/2020/085.pdf.

83 DW, Robot kills worker at Volkswagen plant in Germany, https://www.dw.com/en/robot-kills-worker-at-volkswagen-plant-in-germany/a-18556982.

84 IoT Security Foundation, https://www.iotsecurityfoundation.org/.

logii wymagano udowodnienia, że dołożyli wszelkich starań by zmniejszyć prawdopodobieństwo różnych typów cyberincydentów lub przynajmniej zapewnili, że ich ewentualne skutki będą zdecydowanie ograniczone. Nie ma jednak możliwości osiągnięcia tego celu, gdy kluczowym czynnikiem wpływającym na decyzje o wyborze technologii będzie cena. Analiza ryzyka, którą zdaniem Autora obowiązkowo należy przeprowadzać w przypadku wdrażania nowych technologii, powinna być równie istotnym zagadnieniem, gdyż potencjalne negatywne konsekwencje mogą w skrajnych przypadkach wielokrotnie przewyższać wartość inwestycji. Propozycje najbardziej skutecznych mechanizmów kontrolnych i rozbudowane katalogi zagrożeń są już powszechnie dostępne[85].

Mimo że Autor jest zdecydowanym zwolennikiem wykorzystywania nowoczesnych technologii cyfrowych, sugeruje on by podtrzymywać zdolność podtrzymywania ciągłości kluczowych procesów biznesowych w sposób tradycyjny: ręczny, „analogowy". Jak wykazano w poprzednich podrozdziałach, pędząca cyfryzacja i wprowadzenia modelu „Internet of Everything"[86], pełne są niebezpieczeństw. Przede wszystkim związanych z celową, szkodliwą działalnością przestępców, ale także z poziomem skomplikowania całej analizowanej materii. Stąd też warto by w przedsiębiorstwach, których działalność przejawia się przede wszystkim w tradycyjny, materialny sposób tworzyć i utrzymywać plany ciągłości oparte o tradycyjne techniki. Warto tu przypomnieć, że zespoły kontroli lotów wciąż szkolone są z pracy na tradycyjnych „fiszkach", że w wielu fabrykach istnieje możliwość ręcznego sterowania produkcją. Mimo, że tego typu czynności są znacznie wolniejsze i nie pozwalają już zazwyczaj na utrzymanie wcześniejszej wydajności, to jednak względy bezpieczeństwa powinny prowadzić do tego, by przynajmniej niektóre z procesów można było podtrzymać w ten sposób.

Dobrym punktem startowym dla zabezpieczania infrastruktury będzie wykonanie przez poszczególne z głównych portów morskich przeglądu w zakresie cyberbezpieczeństwa a także identyfikacja ustandaryzowanych wymagań, które sprowadzałyby ryzyko do poziomu akceptowalnego przez władze portów oraz głównych interesariuszy.

85 Drougkas A. *op. cit.*

86 Langley D. (*et al.*) The Internet of Everything: Smart things and their impact on business models, Journal of Business Research vol. 122 (2021), str. 853-863.

Podsumowanie

Nowoczesne rozwiązania cyfrowe w portach przyczyniają się do skrócenia czasu obsługi jednostek kontenerowych i zwiększenia przepustowości terminalu[87]. Zautomatyzowanie terminalu kontenerowego pozwoli na obsługę rosnącej liczby obsługiwanych ładunków. Wdrożenie pojazdów i urządzeń autonomicznych pozwoli na zwiększenie wydajności pracy i zmniejszenie kosztów w wielu obszarach. Pojazdy wyposażone w platformy umożliwiają z kolei samodzielny załadunek kontenera bez pomocy dodatkowych urządzeń, co wpłynie na szybszy proces załadunku i rozładunku. Wdrożenie bezzałogowych statków powietrznych do sprawnej inspekcji trudno dostępnych urządzeń (jakimi są np. suwnice i dźwigi), pozwoli zwiększyć efektywność pracy terminalu. Analiz pokazujących jak rozwinąć działalność polskich portów jest dużo, jednak wśród zagrożeń rzadko można znaleźć nawiązania do konieczności adekwatnego zapewnienia (cyber)bezpieczeństwa

Źródła wskazują, że jednym w poważniejszych wyzwań, którym trzeba będzie sprostać będzie podejście zarządów portów do kwestii bezpieczeństwa, gdyż wprowadzenie rozwiązań wykraczających poza zdefiniowane jako bazowe, wymaga większych nakładów finansowych[88]. W związku z tym, bezpieczeństwo zawsze stanowiło aspekt o niższym priorytecie, niż podstawowe kwestie związane z budową infrastruktury. Widać jednak powolną zmianę trendów i można się spodziewać, że z przyszłości armatorzy coraz chętniej wybiorą porty, w których ich jednostki i ładunki będą bezpieczne.

Producenci systemów bezpieczeństwa oferują coraz nowocześniejsze rozwiązania, jednak nawet najlepsze systemy nie spełnią swojej roli, jeśli nie będą funkcjonować we właściwie zaprojektowanych strukturach w oparciu o dobrze sformalizowane przepisy. Jak wykazała Najwyższa Izba Kontroli rozwój infrastruktury portowej nie odbywa się w sposób satysfakcjonujący[89]. Na niektóre z przytłaczających wniosków można jedna spojrzeć jako

87 Kuźmicz K. (*et al.*), Analiza potencjału automatyzacji terminalu kontenerowego w Gdańsku, Akademia Zarządzania 4(3), Wydział Inżynierii Zarządzania Politechniki Białostockiej 2020, str. 119-138.

88 Zawadzki J., Zintegrowane stanowisko bezpieczeństwa portu faktorem optymalnego wykorzystania potencjału sił i środków bezpieczeństwa, Rocznik Bezpieczeństwa Morskiego 2019, Akademia Marynarki Wojennej im. Bohaterów Westerplatte, str. 1-14.

89 NIK, Informacja o wynikach kontroli, Infrastruktura dostępowa do portów morskich, KIN.430.003.2017, https://www.nik.gov.pl/plik/id,17942,vp,20530.pdf.

na szanse. Polska nie musi być pionierem tworzącym i testującym nowe rozwiązania. Opóźnienie daje nam unikalną szansę by wykorzystać doświadczenia zdobyte przez inne państwa, nie powtarzać niektórych ze zidentyfikowanych błędów – w tym w zakresie cyberbezpieczeństwa. Wczesna adaptacja wymagań cyberbezpieczeństwa wskazywanych dyrektywą NIS2[90], odpowiednio wczesna i kompleksowa budowa świadomości personelu z zakresie cyberbezpieczeństwa, w ramach takich projektów jak Cyber-MAR[91].

Literatura

1. Abrams L., Computer giant Acer hit by $50 million ransomware attack, https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/
2. Canepa M. (*et al.*), Assessing the effectiveness of cybersecurity training and rising awareness within the maritime domain, 10.21125/inted.2021.0726. 2021
3. CERT OPL, 400 Gbps przebite – mamy rekordowy DDoS, https://cert.orange.pl/aktualnosci/400-gbps-przebite-mamy-rekordowy-ddos
4. Chirgwin R., IT 'heroes' saved Maersk from NotPetya with ten-day reinstallation blitz, https://www.theregister.com/2018/01/25/after_notpetya_maersk_replaced_everything/
5. DeepTrekker, Top 3 Risks at our Ports, https://www.deeptrekker.com/resources/maritime-port-security-risks
6. Drougkas A. (*et al.*), Good practices for cybersecurity in the maritime sector, ENISA 2019, https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector
7. DW, Robot kills worker at Volkswagen plant in Germany, https://www.dw.com/en/robot-kills-worker-at-volkswagen-plant-in-germany/a-18556982
8. Esage A., Hacking attack in port of Barcelona, https://www.securitynewspaper.com/2018/09/26/hacking-attack-in-port-of-barcelona/
9. EU - Directive on Security of Network and Information Systems (NIS 2 Directive), https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union

90 EU - Directive on Security of Network and Information Systems (NIS 2 Directive, https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union.

91 Canepa M. (*et al.*) Assessing the effectiveness of cybersecurity training and rising awareness within the maritime domain, 10.21125/inted.2021.0726. 2021.

10. Goward D., GPS disrupted for maritime in Mediterranean, Red Sea, 2018, https://www.gpsworld.com/gps-disrupted-for-maritime-in-mediterranean-red-sea/
11. IoT Security Foundation, https://www.iotsecurityfoundation.org/
12. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, ISO 2013
13. Kaliszewski A., Porty piątej oraz szóstej generacji (5GP, 6GP) - ewolucja ekonomicznej i społecznej roli portów, Studia i Materiały Instytutu Transportu i Handlu Morskiego 2017
14. Kapadia S., 3 years, 3 cyberattacks on major ocean carriers. How can shippers protect themselves? https://www.supplychaindive.com/news/ocean-carrier-cybersecurity-maersk-msc-cosco/576754/
15. Kemme, N., Design and Operation of Automated Container Storage Systems, PhysicaVerlag Heidelberg 2013
16. Knet 360, Collaboration in the Shipping Industry: Innovation and Technology, https://knect365.com/maritime/article/91705d00-6d9d-4ba3-98a4-9b10c92ad520/epaper-collaboration-in-the-shipping-industry-innovation-and-technology
17. Kuźmicz K. (*et al.*), Analiza potencjału automatyzacji terminalu kontenerowego w Gdańsku, Akademia Zarządzania 4(3), Wydział Inżynierii Zarządzania Politechniki Białostockiej 2020
18. Langley D. (*et al.*) The Internet of Everything: Smart things and their impact on business models, Journal of Business Research vol. 122 (2021)
19. Nassi B. (*et al.*), Phantom of the ADAS: Phantom Attacks on Driver-Assistance Systems, Uniwersytet Ben-Gurion, Negev, Israel, 2020, https://eprint.iacr.org/2020/085.pdf
20. Niebezpiecznik.pl Komnaty tortur namierzone przez policję. Dzięki włamaniu na telefon oprawców…, https://niebezpiecznik.pl/post/komnaty-tortur-namierzone-przez-policje-dzieki-wlamaniu-na-telefon-oprawcow/
21. NIK, Informacja o wynikach kontroli, Infrastruktura dostępowa do portów morskich, KIN.430.003.2017, https://www.nik.gov.pl/plik/id,17942,vp,20530.pdf
22. OpenAI, Multimodal Neurons in Artificial Neural Networks, https://openai.com/blog/multimodal-neurons/
23. Roberts J., Exclusive: Facebook and Google Were Victims of $100M Payment Scam, https://fortune.com/2017/04/27/facebook-google-rimasauskas/
24. Rüßmann M. (*et al.*) Industry 4.0: the Future of Productivity and Growth in Manufacturing Industries. Technical Report. Boston Consulting Group 2015, https://image-src.bcg.com/Images/Industry_40_Future_of_Productivity_April_2015_tcm9-61694.pdf

25. The Navigation Center of Excellence, GPS Problem Reports Status, https://navcen.uscg.gov/?Do=GPSReportStatus
26. Tsonchew A., Troubled waters: Cyber-attacks on San Diego and Barcelona's ports, https://www.darktrace.com/en/blog/troubled-waters-cyber-attacks-on-san-diego-and-barcelonas-ports/
27. Tubielewicz A., Zarządzanie logistyczne w transporcie morskim, Oficyna Wydawnicza Polskiego Towarzystwa Zarządzania Produkcją, Gdańsk 2015, str. 1043 – 1054
28. TVN24, Zapłacili oszustowi. Lecą głowy w Metrze Warszawskim, https://tvn24.pl/tvnwarszawa/najnowsze/zaplacili-oszustowi-leca-glowy-w-metrze-warszawskim-241057
29. Ubmemea, Antwerp incident highlights maritime IT security risk, https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk
30. Zawadzki J., Zintegrowane stanowisko bezpieczeństwa portu faktorem optymalnego wykorzystania potencjału sił i środków bezpieczeństwa, Rocznik Bezpieczeństwa Morskiego 2019, Akademia Marynarki Wojennej im. Bohaterów Westerplatte

ABSTRACT

CHALLENGES IN PROVIDING CYBER SECURITY TO THE PORT AND MARITIME INFRASTRUCTURE FACILITIES

Summary: This chapter presents the diversity and importance of cybersecurity issues for the broadly understood port and maritime infrastructure. It is based on historical and hypothetical examples. The issues have been divided into frauds, various incidents ending with the disruption of business processes as well as upcoming threats, still rare but potentially raising in their importance.

Keywords: cybrecurity, threats, ports, marine infrastructure.

ROZDZIAŁ 5

O GOTOWOŚCI DO CYFROWEGO ŚLEDZTWA. PODEJŚCIE NORMATYWNE

dr inż. Maciej SZMIT [92]

STRESZCZENIE: W rozdziale omówiono pojęcia związane z gotowością śledczą (forensic readiness) organizacji w odniesieniu do badania cyfrowych śladów dowodowych. Przedstawione podejście opiera się na normach ISO/IEC z serii 27k.

SŁOWA KLUCZOWE: ISO 27k, informatyka śledcza, nadzór i zarządzanie badaniami cyfrowych śladów dowodowych.

1. Wstęp

W 2012 roku pojawiło się pierwsze wydanie normy ISO/IEC 27037 ([1]). Wersja polska: PN-EN ISO/IEC 27037:2016-12 - wersja polska - Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego ([2]), została wydana w roku 2016. Od tej

[92] Uniwersytet Łódzki, maciej.szmit@uni.lodz.pl; ORCID: 0000-0002-6115-9213.

pory w rodzinie norm ISO/IEC 27k pojawił się szereg standardów dotyczących nie tylko informatyki śledczej, ale – sensu largo – zarządzania i nadzoru korporacyjnego (ang. corporate governance)[93] nad badaniami cyfrowych śladów dowodowych.

2. ISO/IEC 27014: Nadzór korporacyjny nad bezpieczeństwem informacji

Zarządzanie, według podejścia prezentowanego przez Międzynarodową Organizację Standaryzacyjną, powinno odbywać się zgodnie z zasadami podejść: systemowego i procesowego, stąd również badanie cyfrowych śladów dowodowych nie może pozostawać w swoistej próżni, w oderwaniu od innych aspektów działania organizacji. W szczególności powinno podlegać ciągłemu doskonaleniu oraz odbywać się pod kontrolą nadzoru korporacyjnego[94].

Nadzór korporacyjny w kontekście niniejszego artykułu odnosi się do organizacji relacji między właścicielami, akcjonariuszami i pozostałymi grupami udziałowymi (w szczególności reprezentowanymi przez rady nadzorcze spółek) a kierownictwem (managerami, zarządem, dyrektorami operacyjnymi) korporacji (por. [3], [4] s.22–25).

Polska Norma PN-EN ISO/IEC 30121:2016-12 - wersja angielska - Technika informatyczna -- Nadzór nad strukturą ryzyka związanego z informatyką śledczą ([6]) definiuje[95] **organ nadzorczy** (ang. governing body) jako osobę lub grupę osób, które odpowiadają przed interesariuszami za wydajność i zgodność (ang. conformance) w organizacji. Definicję tę powtarza za nią Norma ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security ([7]). **Nadzór korporacyjny nad bezpieczeństwem informacji** (ang. governance of information security) definiowany jest w tejże normie [7] jako system, za pomocą którego działania organizacji

[93] Jakkolwiek czasami słowo „governance" tłumaczy się przy użyciu słowa „zarzadzanie", dla zachowania czytelności dalej będzie ono zawsze tłumaczone przez „nadzór korporacyjny", zaś słowo „zarządzanie" będzie używane tam, gdzie normy używają słowa „management".

[94] Warto pamiętać, że normy ISO/IEC 27k pisane są z punktu widzenia organizacji (a nie systemu prawnego poszczególnych krajów), stąd ich stosowalność w zakresie czynności śledczych w postępowaniach przed organami procesowymi może być ograniczona. Choć w zasadzie normy nie powinny pozostawać w konflikcie z przepisami prawa, specyficzny charakter zagadnień śledczych może prowadzić do powstania pewnych niespójności (zob. np. [5]).

[95] Wszystkie tłumaczenia z norm w języku angielskim zawarte w niniejszym artykule są tłumaczeniami nieoficjalnymi.

w zakresie bezpieczeństwa informacji są kierowane i kontrolowane. Organizacja tego systemu opiera się o pięć pryncypiów:

- kompleksowe i zintegrowane podejście do zarzadzania bezpieczeństwem informacji w całej organizacji,
- stosowanie podejścia zorientowanego na ryzyko,
- strategię inwestowania w bezpieczeństwo informacji,
- zapewnienie zgodności z wymaganiami zewnętrznymi i wewnętrznymi oraz
- wspieranie środowiska przyjaznego bezpieczeństwu informacji)

oraz o pięć procesów,

- ewaluowanie (ang. evaluate),
- przewodzenie (ang. direct),
- monitorowanie (ang. monitor)
- komunikowanie (ang. communicate)
- wsparcie (ang. assure).

Cztery pierwsze procesy prowadzone są przez organ nadzorczy, natomiast piąty, obejmuje zlecanie niezależnych i obiektywnych audytów bądź przeglądów dostarczających opinii na temat zarządzania bezpieczeństwem informacji i osiągniętego poziomu bezpieczeństwa informacji.

3. Informatyka śledcza i zarządzanie incydentami w normach ISO/IEC 27x

W ramach rodziny ISOIEC 27k powstały (i ciągle powstają) normy dotyczące incydentów bezpieczeństwa informacji, w tym postępowania po incydentach. Najwcześniej opublikowana norma ISO/IEC 27037 ([1]) zawiera wytyczne do specyficznych działań w ramach postępowania z cyfrowym materiałem dowodowym (identyfikacja, gromadzenie, pozyskiwanie i zachowywanie cyfrowego materiału dowodowego, który może mieć wartość dowodową). Normy ISO/IEC 27038 i ISO/IEC 27039 nie są bezpośrednio związane z informatyką śledczą: pierwsza z nich poświęcona jest trwałemu usuwaniu informacji z dokumentów cyfrowych (ang. digital redaction), druga natomiast – systemom wykrywania włamań (ang. Intruder Detection Systems, IDS).

Norma ISO/IEC 27040 ([8]) poświęcona jest **bezpieczeństwu pamięci masowych**, w tym również zagadnieniom takim jak metody nieodwracalnego usuwania danych z dysków oraz urządzeń SAN i NAS. W normie zdefiniowane jest, między innymi, bezpieczeństwo pamięci masowych, przez które rozumie się użycie programowych bądź fizycznych, technicznych oraz administracyjnych zabezpieczeń (ang. controls) w celu ochrony systemu i infrastruktury pamięci masowych oraz danych w nich przechowywanych, skupione na ich ochronie przed nieautoryzowanym ujawnieniem, modyfikacją lub zniszczeniem i na zapewnieniu ich dostępności dla autoryzowanych użytkowników. Zabezpieczenia, o których mowa, norma dzieli na: prewencyjne (ang. preventive), wykrywcze (ang. detective), naprawcze (ang. corrective), zapobiegające (ang. deterrent)[96], odzyskujące (ang. recovery)[97] oraz kompensacyjne (ang. compensatory)[98].

Norma ISO/IEC 27041 ([9]) jest to liczący sobie osiemnaście stron dokument poświęcony zapewnianiu przydatności i adekwatności metod i narzędzi używanych do badania incydentów bezpieczeństwa informacji. Do ciągłego doskonalenia metod używanych do badania incydentów wykorzystuje, znany z innych norm ISO, cykl Plan-Do-Check-Act (koło Demminga), jak to zapisano w punkcie 5.2 normy: „w celu zapewnienia, że wszystkie procesy podlegają przeglądowi co najmniej tak często tak, jak są używane". Warto zauważyć, że tego rodzaju podejście powinno być właściwe dla organizacji zajmujących się profesjonalnie informatyką śledczą (w tym wymiaru sprawiedliwości).

Norma wprowadza między innymi pojęcia:

- **walidacji**, rozumianej jako potwierdzenie, poprzez dostarczenie obiektywnych dowodów, że wymagania dla określonego, zamierzonego użycia lub zastosowania zostały spełnione (walidacja przeprowadzana jest dla procesu, aby upewnić się,

[96] Przez „deterrent controls" rozumie się zabezpieczenia zmniejszające prawdopodobieństwo wykorzystania podatności bez zmniejszania rzeczywistej ekspozycji zasobu na ryzyko. Przykładem mogą być działania podnoszące świadomość użytkowników (np. kampanie antyphishingowe).

[97] Zabezpieczenia naprawcze (ang. corrective controls) dedykowane są korekcji skutków konkretnego problemu. Zabezpiecenia odzyskujące (ang. recovery control) mają na celu przywrócenie całego systemu bądź danych do stanu pozwalającego na realizacje jego celów biznesowych.

[98] Zabezpieczenia kompensacyjne są wprowadzane w celu spełnienia wymogu posiadania zabezpieczenia, które jest obecnie zbyt trudne do wdrożenia lub niepraktyczne. Na przykład zamiast szyfrowania całości danych wprowadza się mechanizmy kontroli dostępu do nich, rozwiązania zapobiegaące wyciekowi danych i częściowe szyfrowanie (np. najważniejszych baz danych).

że spełnia on zamierzony cel, to jest aby zapewnić, że wdrożony proces daje oczekiwane wyniki w spójny, powtarzalny i odtwarzalny[99] sposób);

- **zbioru walidacyjnego**, tj. serii obiektywnych testów z jasno określonymi celami, danymi wejściowymi i wyjściowymi, bezpośrednio związanych z uzgodnionymi wymaganiami dla procesu podlegającego walidacji oraz
- **weryfikacji**, czyli potwierdzenia, poprzez dostarczenie obiektywnych dowodów, że określone wymagania zostały spełnione (zapewnienia, że produkt jest zgodny z jego secyfikacją).

Oczywiście walidacja i weryfikacja powinna dotyczyć procesów i narzędzi stosowanych w informatyce śledczej.

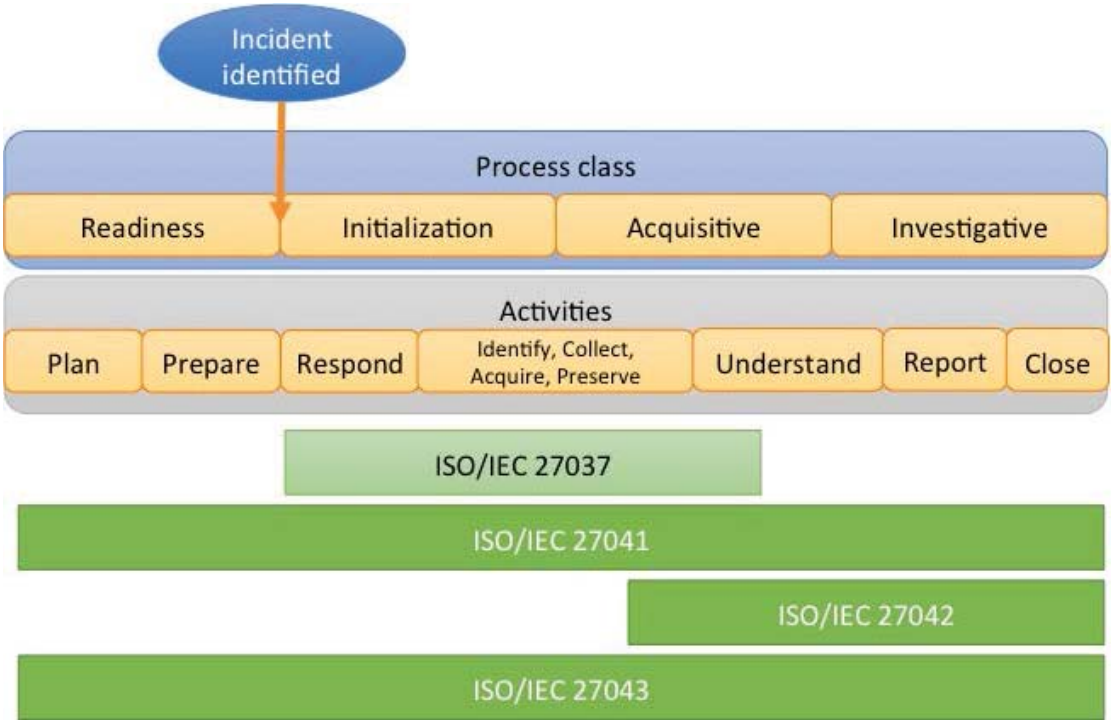
Norma 27042 ([10]) licząca czternaście stron, dostarcza zaleceń odnośnie analizy i interpretacji cyfrowych śladów dowodowych z uwzględnieniem problemów ciągłości, ważności, odtwarzalności i powtarzalności. Zawiera najlepsze praktyki dotyczące wyboru, projektowania i wdrażania procesów analitycznych oraz rejestrowania wystarczających informacji, aby umożliwić niezależną kontrolę tych procesów. Wewnątrz normy można znaleźć szereg wytycznych (między innymi dotyczących interpretacji znalezionych podczas dochodzenia informacji czy zawartości raportu z badań).

Norma ISO/IEC 27043 ([11]) jest trzydziestostronicową normą określającą kluczowe wspólne zasady i procesy leżące u podstaw badania incydentów i definiuje model ramowy dla wszystkich etapów dochodzeń. W normie zdefiniowano pojęcie gotowości (ang. readiness) – procesu polegającego na byciu przygotowanym na cyfrowe dochodzenie (ang. digital investigation), przy czym gotowość ta ma mieć miejsce zanim wydarzy się incydent. Przez proces rozumie się w powołanej normie zbiór działań mających wspólny cel i ograniczony czas trwania.

Wzajemny stosunek norm [9], [10] i [11] oraz [1] obrazuje Rysunek 1, będący fragmentem schematu zamieszczonego w normach [9], [10] i [11]. Porządkuje on klasy procesów, które występują w organizacji w związku z wystąpieniem incydentu i śledztwem,

[99] Pojęcia powtarzalności (ang. repeatability) i odtwarzalności (ang. reproductibility) są zdefiniowane w normie ISO/IEC 27037:2016.

wyodrębniając gotowość (procesy zachodzące przed wystąpieniem incydentu), inicjalizację, akwizycję i dochodzenie.

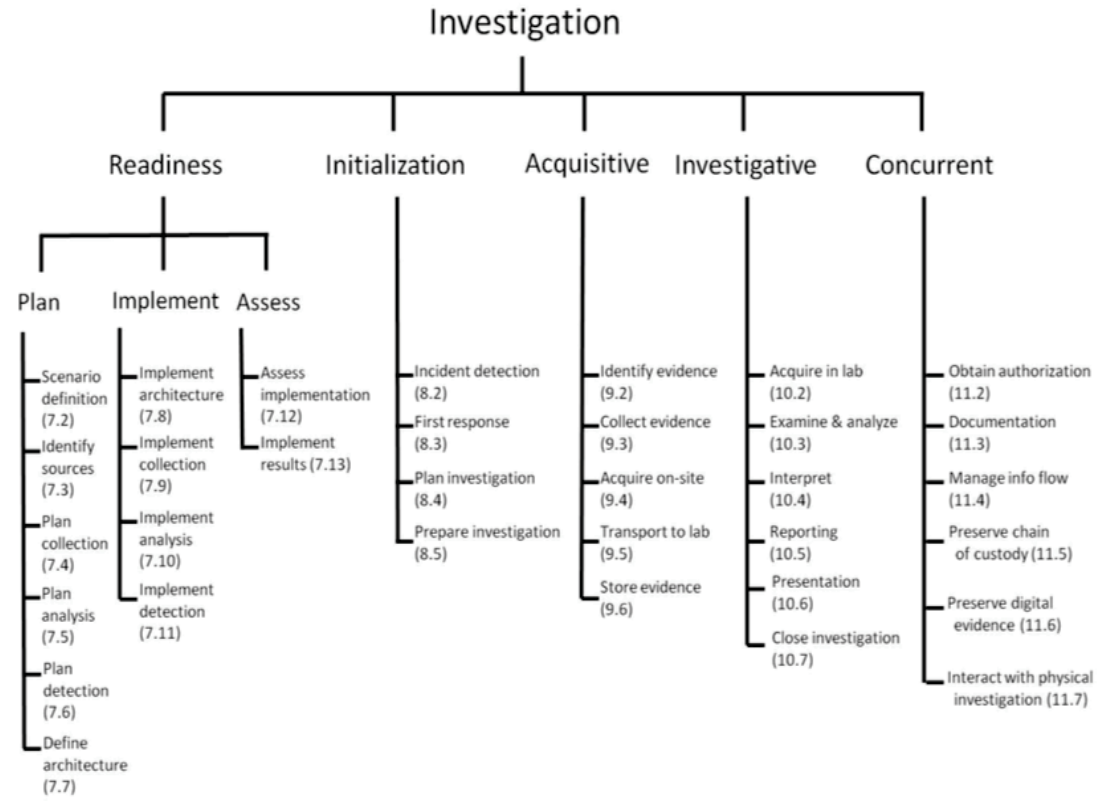


Rys. 1. Zakres stosowalności wybranych standardów i poszczególne klasy procesów oraz działań. Źródło: opracowanie własne na podstawie [9], [10], [11].

Poszczególne działania zdefiniowane w normie [11] można przyporządkować do procesów jak na rysunku 2. Oprócz procesów należących do którejś z wymienionych czterech klas, wyodrębniono równie procesy zachodzące równocześnie (ang. concurrent) z innymi.

Norma ISO/IEC 27050 podzielona jest na cztery części ([14], [15], [16] oraz znajdującą się obecnie na etapie tworzenia [17]). Porządkują one sposób prowadzenia dochodzeń cyfrowych. Dochodzenie elektroniczne (ang. electronic discovery) obejmuje między innymi postępowanie z materiałem dowodowym opisane w omawianej już normie ISO/IEC 27037 [1]. Podobnie ona, również normy z serii 27050-x zalecenia starają się być neutralne względem obowiązujących przepisów prawnych. Między innymi zrezygnowano

z użycia słowa „dowód” (ang. evidence), zastępując je pojęciem informacji przechowywanej elektronicznie (ang. Electronically Stored Information, ESI).



Rys. 2. Procesy zdefiniowane w normie [11] w podziale na klasy. Źródło: [12].

Norma ISO/IEC 27050-1, dostępna nieodpłatnie[100], zawiera szereg definicji, w tym między innymi definicję łańcucha dowodowego (ang. chain of custody), rozumianego jako możliwe do udokumentowania losy śladu dowodowego (tj. jego posiadanie, przemieszczenie, postępowanie i lokalizację) pomiędzy dwoma chwilami czasu. Szczegółowe informacje i aktualizowane omówienie zawartości poszczególnych części tej normy (i innych norm z rodziny 27k) można znaleźć na stronie [18].

[100] pod adresem https://standards.iso.org/ittf/PubliclyAvailableStandards/c063081_ISO_IEC_27050-1_2016.zip.

4. Podsumowanie

Informatyka śledcza w Polsce w ciągu ostatnich lat poczyniła ogromne postępy. Bez trudu można zauważyć profesjonalizację działań zarówno biegłych, jak i specjalistów policyjnych. Powstał szereg firm zajmujących się informatyką śledczą, jak również utworzone zostały odpowiednie komórki w polskich oddziałach międzynarodowych korporacji). Niestety, szczególnie w przypadku państwowych służb zajmujących się tymi zagadnieniami, można zauważyć wybitnie niską dojrzałość organizacyjną odnośnie budowy i implementacji odpowiednich części Systemów Zarządzania Bezpieczeństwem Informacji. Ewentualna zmiana takiego stanu rzeczy wymagałaby daleko idących zmian organizacyjnych na poziomie państwa.

Wydaje się w tej sytuacji wskazane postulowanie wykorzystywania wspomnianych powyżej norm w najbardziej elementarny sposób – jako źródła znormalizowanego słownictwa i zbioru dobrych praktyk, które powinny być przez poszczególnych biegłych stosowane przynajmniej ad hoc, dla osiągnięcia pewnej powtarzalności sposobu działania.

5. Bibliografia

1. ISO/IEC 27037:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence
2. PN-EN ISO/IEC 27037:2016-12 - wersja polska - Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego, PKN 2016
3. Rudolf W.: Koncepcja governance i jej zastosowanie – od instytucji międzynarodowych do niższych szczebli władzy, Acta Universitatis Lodziensis Folia Oeconomica 245, 2010, s. 83-92
4. Jerzemowska M.: Nadzór korporacyjny, PWE, Warszawa, 2002
5. Szmit M.: Kilka uwag o ISO/IEC 27037:2012 oraz ENISA electronic evidence — a basic guide for First Responders, [w:] Kosiński J. (red): Przestępczość teleinformatyczna 2015, p. 101-110, WSPol., Szczytno 2015
6. PN-EN ISO/IEC 30121:2016-12 - wersja angielska - Technika informatyczna -- Nadzór nad strukturą ryzyka związanego z informatyką śledczą, PKN 2016
7. ISO/IEC 27014:2013 Information technology -- Security techniques -- Governance of information security, ISO 2013

8. PN-EN ISO/IEC 27040:2016-12 - wersja angielska Technika informatyczna -- Techniki bezpieczeństwa -- Bezpieczeństwo pamięci masowych, PKN 2016
9. PN-EN ISO/IEC 27041:2016-12 - wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydentem, PKN 2016
10. PN-EN ISO/IEC 27042:2016-12 - wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- Wytyczne do analizy i interpretacji cyfrowego śladu dowodowego, PKN 2016
11. PN-EN ISO/IEC 27043:2016-12 - wersja angielska, Technika informatyczna -- Techniki bezpieczeństwa -- Pryncypia i procesy w dochodzeniach związanych z incydentami, PKN 2016
12. Tim Grant, Erwin van Eijk, H.S. Venter: Assessing the Feasibility of Conducting the Digital Forensic Process in Real Time, ICCWS 2016 Boston, MA
13. ISO/IEC 27050-1:2016 Information technology -- Security techniques -- Electronic discovery -- Part 1: Overview and concepts, ISO 2016
14. ISO/IEC 27050-1:2016 Information technology — Security techniques — Electronic discovery — Overview and concepts, ISO 2016
15. ISO/IEC 27050-2:2018 Information technology — Security techniques — Electronic discovery — Guidance for governance and management of electronic discovery, ISO 2018
16. ISO/IEC 27050-3:2017 Information technology — Security techniques — Electronic discovery — Code of practice for electronic discovery, ISO 2017
17. ISO/IEC 27050-4 Information technology — Electronic discovery — technical readiness, ISO (under construction)
18. https://www.iso27001security.com

ABSTRACT

ABOUT DIGITAL FORENSIC READINESS. STANDARD APPROACH

Summary: Digital forensic and related terms and concepts are discussed in the article. The basics of ISO/IEC 27k approach are also presented.

Keywords: ISO 27k, computer forensics, governance and management of electronic discovery.

ROZDZIAŁ 6

ZABEZPIECZENIE CYFROWEGO MATERIAŁU DOWODOWEGO W KONTEKŚCIE POLSKIEJ NORMY PN-EN ISO/IEC 27037

Tomasz PAWLICKI [101]

STRESZCZENIE: Rozdział jest poświęcony problematyce zabezpieczenia cyfrowego materiału dowodowego w oparciu o normę PN-EN ISO/IEC 27037 która została opublikowana w dniu 26.10.2017 r. W aspekcie certyfikowania Laboratoriów Kryminalistycznych zgodnie z Polską Normą PN-EN ISO/IEC 17025:2005 jest to pierwszy polski dokument uwzględniający i wyjaśniający w sposób szczegółowy poszczególne etapy i zadania związane z pozyskiwaniem do badania próbek cyfrowych.

SŁOWA KLUCZOWE: dowód cyfrowy, PN-EN ISO/IEC 27037, dane, kopia bitowa, łańcuch dowodowy.

1. Wstęp

Przestępczość z wykorzystaniem technologii informatycznych i nowoczesnych mediów transmisyjnych to nieustanny rozwój i zmiany. Pomimo znacznego upływu czasu od wydania anglojęzycznego odpowiednika, Polska Norma PN-EN ISO/IEC 27037 "Technika

[101] Naczelnik Wydziału Rozpoznania Biura do Walki z Cyberprzestępczością Komendy Głównej Policji, tomasz.pawlicki@policja.gov.pl.

informatyczna; Techniki bezpieczeństwa; Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego" jest pierwszym polskim dokumentem zawierającym szczegółowe wytyczne dotyczące zabezpieczenia materiału dowodowego. Należy również podkreślić, iż nie wprowadza on zamieszania w dotychczas stosowanych technikach i „procedurach", a jedynie je systematyzuje.

Niniejszy artykuł ma na celu przybliżenie czytelnikowi zasad, do tej pory traktowanych jako "dobre praktyki", w kwestii gromadzenia dowodów cyfrowych na miejscu zdarzenia. Może on również być potraktowany, z uwagi na liczne pytania od słuchaczy, jako element uzupełniający do realizowanego przez Krajową Szkołę Sądownictwa i Prokuratury w Lublinie projektu szkoleniowego: „Zapobieganie i zwalczanie cyberprzestępczości" realizowanego w ramach Programu operacyjnego Wiedza Edukacja Rozwój 2014-2020.

2. Najważniejsze pojęcia użyte w Normie

Na stronach 8-10 Polskiej Normy PN-EN ISO/IEC 27037 znajduje się wyjaśnienie wielu pojęć, które z punktu widzenia informatyki śledczej stanowią pewnego rodzaju unormowanie dotychczas stosowanych określeń. W przypadku, gdy na gruncie polskich uwarunkowań mogłyby one budzić pewne wątpliwości zostało to wyjaśnione.

Wśród użytych pojęć są[102]:

• DES (ang. Digital Evidence Specialists) – ekspert informatyki śledczej.

W odniesieniu do przyjętego nazewnictwa ujednoliconego przez Centralne Laboratorium Kryminalistyczne Policji będzie to Biegły z zakresu informatyki[103] lub Specjalista certyfikowany[104].

---

[102] Polska Norma PN-EN ISO/IEC 27037 s.8-10. Podstawowe definicje w rozdziale Najważniejsze pojęcia użyte w Normie są cytatami z Normy.Artykuł warto porównać z artykułem M. Szmit, Kilka uwag o ISO/IEC 27037:2012 oraz ENISA electronic evidence — a basic guide for First Responders, [w:] Kosiński J. (red): Przestępczość teleinformatyczna 2015, ss. 101-110, WSPol., Szczytno 2015.

[103] "biegły policyjnego laboratorium kryminalistycznego – policjant lub pracownik policyjnego laboratorium kryminalistycznego, posiadający uprawnienia w zakresie określonych specjalności kryminalistycznych". Zarządzenie nr 3 Komendanta Głównego Policji z dnia 17 stycznia 2014 r. w sprawie uprawnień do wydawania opinii oraz wykonywania czynności w policyjnych laboratoriach kryminalistycznych.

[104] Zakres czynności wykonywanych przez biegłego oraz certyfikowanego specjalisty jest określony w Decyzji nr 85 Dyrektora CLKP z dnia 21 kwietnia 2016 r. W zależności od stopnia trudności przeprowadzenia czynności będzie różny, przy czym biegły może wykonywać wszystkie czynności przewidziane dla certyfikowanego specjalisty.

• DEFR (ang. Digital Evidence First Responders) specjalista pierwszego kontaktu z cyfrowym materiałem dowodowym.

W chwili obecnej w policyjnej nomenklaturze nie ma właściwego odpowiednika odnoszącego się stricte do tej funkcji, rolę tą zamiennie może pełnić każdy policjant znajdujący się na miejscu zdarzenia, technik kryminalistyki oraz biegły/specjalista certyfikowany CLKP/LK/KSP lub biegły sądowy.

• Cyfrowy materiał dowodowy – informacje lub dane, składowane lub transmitowane w formie binarnej, które mogą być traktowane jako materiał dowodowy.

Na uwagę zasługuje tu zapis „transmitowane". Należy zwrócić uwagę, iż sama transmisja oraz jej „zawartość" może być dowodem. Dlatego też winno się uwzględnić i wdrożyć mechanizmy pozwalające na zabezpieczenie danych, np. w postaci wysyłanych/odbieranych pakietów, np.: gdy mamy do czynienia z działaniem skryptu znajdującego się na komputerze sprawcy lub ataku z sieci w przypadku komputera „ofiary". W takim wypadku celowym wydaje się uruchomienie oprogramowania, np. typu Wireshark[105] umożliwiającego pobranie transmitowanych danych, celem późniejszego ich opiniowania.

• Cyfrowy nośnik danych – urządzenie, na którym mogą być zapisane dane w postaci cyfrowej.

• Dane ulotne – dane szczególnie podatne na zmianę, które można łatwo modyfikować.

W szczególności określenie to będzie dotyczyć danych, które w sposób nieodwracalny mogą zostać utracone. Najbardziej charakterystyczny przykład to informacje z pamięci RAM, które po wyłączeniu zasilania po prostu znikną. W obecnej praktyce dowodowej rzadko stosuje się wykonywanie zrzutu pamięci RAM, jednak z uwagi na ilość i rodzaj danych, które są w niej przechowywane, chociażby zapisane hasła logowania czy też programy działające w pamięci, wykonanie kopii tych danych staje się po prostu konieczne.

• Tworzenie obrazu – proces tworzenia bitowej kopii cyfrowego nośnika danych.

Tworzenie obrazu dysku twardego to proces ekstrakcji danych na potrzeby kryminalistyczne, wykonany z nośnika „ofiary", „podejrzanego", „świadka" etc. w celu przeprowadzenia późniejszej analizy/badań obrazu dysku źródłowego zamiast oryginalnego nośnika[106]. Zgodnie z powszechnie stosowanymi technikami w informatyce śledczej obrazem danych może być klon nośnika lub jego obraz bitowy zapisany do pliku. Sam sposób, użyte środki

[105] Program możliwy do pobrania ze strony https://www.wireshark.org/.
[106] tłumaczenie autora, Practical Windows Forensics, poz. 111, Packt Publishing 2016.

techniczne, będą determinowane od zastanej sytuacji i będą zależały od DEFR. Powyższe czynności można wykonać za pomocą dedykowanych do tego urządzeń lub oprogramowania, przy czym nie ma wymogu, aby oprogramowanie to było komercyjne. Istnieje wiele doskonałych dystrybucji niekomercyjnych, które z całą pewnością przeprowadzą proces kopiowania w sposób właściwy. Tak naprawdę istnieją trzy rodzaje kopii:

- kopia fizyczna całego dysku – jest to sposób wykonania obrazu zawierający wszystkie możliwe dane znajdujące się na nośniku, a zatem to najbardziej kompletna forma zabezpieczenia danych. W przypadku, gdy część danych jest zaszyfrowana, będą one również zaszyfrowane na sporządzonej kopii;
- kopia logiczna partycji – to rozwiązanie stosowane jest, m.in. gdy partycja dysku jest zaszyfrowana i odzwierciedlona w systemie informatycznym jako odszyfrowana partycja logiczna. Jedyny możliwy sposób dokonania późniejszej analizy takich danych, w odniesieniu do ewentualnego braku możliwości odszyfrowania takich danych, jest wykonanie właśnie takiej kopii;
- kopia części danych – w przypadku, gdy dane będące w zainteresowaniu organów ścigania/wymiaru sprawiedliwości są ściśle określone, a ich forma nie budzi wątpliwości. Takie rozwiązanie można stosować również w przypadku znacznej objętości dowodowej przestrzeni dyskowej i konieczności dokonania wstępnej selekcji danych.

Koniecznym jest również wyjaśnienie różnic i podobieństw między klonem bitowym, a obrazem bitowym dysku twardego. Bardzo często prowadzący czynności nie jest w stanie wskazać odmienności między tymi dwoma technikami, a tym samym w sposób właściwy technicznie przygotować się do sprawnego przeprowadzenia czynności. Co gorsza wskazywane są również rozbieżności między zabezpieczonymi w ten sposób danymi traktujące o wyższości i większej szczegółowości w zgromadzonych w ten sposób informacji na korzyść klonu dysku twardego.

Klon dysku będzie obejmował wykonanie obrazu nośnika (źródłowego) na inny nośnik (docelowy) w skali 1:1 w postaci przegrania danych w takiej „samej formie", przy czym nośnik docelowy, na którym wykonana jest kopia winien być fabrycznie nowy lub uprzednio przygotowany[107].

[107] W przypadku wykorzystania nośników będących w zasobach DES/DEFR należy przeprowadzić i udokumentować proces kasowania danych na dyskach przeznaczonych do powtórnego wykorzystania poprzez nadpisywanie.

Obraz bitowy dysku będzie obejmował wykonanie obrazu nośnika (źródłowego) na inny nośnik (docelowy) w skali 1:n[108], w postaci pliku/plików. Dane te mogą być zapisane w wielu formatach (kontenerach). Do najpopularniejszych należą formaty RAW, A01, AD1, SMART[109].

Z punktu widzenia późniejszego badania dysków, a w szczególności możliwości odzyskiwania i analizy danych bez względu na zastosowaną technikę wyniki będą tożsame.

• Funkcja weryfikująca – funkcja stosowana do zweryfikowania, czy dwa zestawy danych są identyczne.

W przypadku danych informatycznych wyliczenie funkcji weryfikującej powinno następować w każdym przypadku wykonania obrazu bitowego zabezpieczonego nośnika na miejscu oraz przy rozpoczęciu i zakończeniu badań cyfrowego materiału dowodowego. Z praktycznego punktu widzenia funkcję weryfikującą można zastosować do pojedynczych plików znajdujących się na badanym nośniku w części lub w całości[110].

3. Postępowanie z cyfrowym materiałem dowodowym

Od prawidłowego zabezpieczenia cyfrowego materiału dowodowego w znacznym stopniu zależą późniejsze możliwości badawcze. Należy niezmiernie rozważnie i z dużą odpowiedzialnością z nim postępować i nie dopuścić do jego skompromitowania[111], np. podczas nieprawidłowo zastosowanej metodyki badawczej. Norma wskazuje, iż zabezpieczenie materiału dowodowego winno opierać się na trzech fundamentalnych zasadach: istotności, wiarygodności i wystarczalności.

---

[108] n – dowolna ilość wykonanych kopii nośnika źródłowego – ograniczenie wynika z pojemności nośnika docelowego.

[109] Shah, Makhdoom Syed Muhammad Baqir, Saleem, Shahzad, Zulqarnain, Roha, Protecting digital evidence integrity and preserving chain of custody, Journal of Digital Forensics, Security & Law, 2017, str.122.

[110] W przypadku nośników typu SSD kolejna weryfikacja danych i zmiana wartości funkcji weryfikującej może błędnie prowadzić do wniosków, iż materiał dowodowy został zmodyfikowany. Powyższe wynika z rozwiązań technologicznych zastosowanych w urządzeniu. Dlatego też celowym jest wyliczenia funkcji weryfikującej dla wszystkich plików. Ponadto w przypadku użycia technik Live Forensics lub Triage oczywistym jest konieczność wyliczenia funkcji weryfikującej dla zabezpieczonych plików.

[111] Skompromitowanie materiału dowodowego oznacza naruszenie jego integralności poprzez wprowadzenie zmian w jego zapisie.

- Istotność – to wskazanie, iż zgromadzony materiał dowodowy jest istotnym elementem dla prowadzonego postępowania.
- Wiarygodność – to wskazanie, iż zgromadzony ,na podstawie czynności wykonanych na miejscu, materiał dowodowy jest odtwarzalny.
- Wystarczalność – to wskazanie, iż zgromadzony materiał dowodowy jest wystarczający do przeprowadzenia czynności badawczych.

W każdym rozpatrywanym wypadku podjęte decyzje, czy też wykonane czynności winny być odtwarzalne. Zaleca się również, aby każda z czynności była udokumentowana w celu umożliwienia jej późniejszego odtworzenia krok po kroku.

3.1. Postępowanie na miejscu zdarzenia – czynności wstępne

Z uwagi na ulotność[112] i możliwość bezpowrotnej utraty cyfrowego materiału dowodowego postępowanie na miejscu zdarzenia winno od samego początku przybrać formę zdecydowanych działań. Należy tu zaznaczyć, iż w sprawach związanych z szerokorozumianym pojęciem cyberprzestępczości, sprawcy zdają sobie sprawę z możliwości szybkiego „usunięcia" danych. Z technicznego punktu widzenia może to być zarówno ich skasowanie (a w szczególności nadpisanie[113]), jak i „ponowne" zaszyfrowanie. Dane niezbędne do deszyfracji mogą znajdować się zarówno w pamięci , jak i tokenach, kartach inteligentnych, innych urządzeniach bądź mediach, a także w chmurach obliczeniowych[114], np. klucz deszyfrujący do funkcji BitLocker.

Aby zminimalizować związane z tym niebezpieczeństwo norma wskazuje podstawowe czynności, które należy przedsięwziąć na miejscu zdarzenia, w szczególności obejmują one:

• zabezpieczenie i przejęcie kontroli nad obszarem zawierającym urządzenia.

W praktyce technicznej jest to „pierwsza" czynności, jaką winno się wykonać na miejscu zdarzenia. Niejednokrotnie bowiem podczas pierwszych minut „zamieszania" urządzenia, bądź dane są niszczone, bądź ukrywane.

---

[112] Szerzej omówiono w Polska Norma PN-EN ISO/IEC 27037 Rozdziały 5.4.2 i 6.8.

[113] Nadpisanie danych - proces bezpowrotnego usuwania danych polegający na ich wymazaniu a następnie zastąpieniu innymi danymi o charakterze pseudolosowym. Tym samym proces ich odzyskania w praktyce staje się niemożliwy. Istnieją różnego rodzaju standardy szerzej na ten temat NIST Special Publication - Guidelines for Media Sanitization

[114] Chmura obliczeniowa - (ang. cloud computing) jest usługą polegającą na zdalnym udostępnieniu mocy lub przestrzeni obliczeniowej przez zewnętrzne podmioty.

• ustalenie, kto jest osobą odpowiedzialną za daną lokalizację.

W praktyce należy ustalić, kto jest odpowiedzialny za daną sieć lokalną/grupę komputerów/serwer. W przypadku skomplikowanej infrastruktury oraz serwerów administrator może oć dgrywać kluczową rolę w dochodzeniu do prawdy. Należy jednak mieć na uwadze, iż może on zarówno skomplikować, a wręcz uniemożliwić wykonaniee czynności na danym sprzęcie lub na danym obszarze, jak i również w sposób istotny pomóc. W szczególności jeśli chodzi o strukturę sieciowo organizacyjną systemu teleinformatycznego znajdującego się w danej lokalizacji.

• upewnienie się, że osoby zostały odseparowane od urządzeń i zasilaczy.

W praktyce należy dopilnować, aby żaden z użytkowników systemu nie miał szansy na wprowadzenie zmian tuż po lub w trakcie rozpoczęcia czynności przez organy ściągania. Z praktyki wynika, iż użytkownicy są skłonni do kasowania danych, często nawet nie mających znaczenia dla prowadzonego postępowania. Co w efekcie może mieć odbicie w opinii biegłego z zakresu informatyki.

• udokumentowanie każdej osoby, która ma dostęp do danej lokalizacji i każdego, kto może być związany z miejscem zdarzenia.

W praktyce należy sprawdzić, kto ma dostęp do danego komputera/systemu komputerowego. Zapisać jego hasła, loginy, używane programy oraz inne spersonalizowane informacje dotyczące jego działalności w danym systemie. Oczywiście ważnym elementem jest pozyskanie wiedzy, czy z komputera korzysta wyłącznie jedna osoba, czy też wiele osób oraz czy organizacja sieci wewnętrznej pozwala użytkownikom korzystać z dowolnego komputera poprzez zalogowanie się na swoim koncie. Należy wtedy ustalić gdzie przechowywane są dane poszczególnych użytkowników i czy mają one charakter scentralizowany – dostępne są z poziomu serwera, czy też częściowo rozproszony – dostępne są zarówno z poziomu serwera, jak i z poziomu komputera, gdzie zapisywane są na jego dysku twardym.

• jeśli urządzenie jest WŁĄCZONE, nie WYŁĄCZAĆ, a jeśli urządzenie jest WYŁĄCZONE, nie WŁĄCZAĆ.

W praktyce należy upewnić się czy włączony system nie posiada sieciowych połączeń z innymi podsystemami, maszynami urządzeniami magazynującymi dane. W szczególności w przypadku podłączenia zaszyfrowanych nośników ich odłączenie spowoduje bezpowrotną utratę informacji. W takiej sytuacji należy wykonać zrzut danych najlepiej poprzez wykonanie kopii logicznej nośnika.

• jeśli to możliwe, udokumentować (np. za pomocą szkicu, zdjęcia lub nagrania wideo) miejsce zdarzenia, wszystkie komponenty i kable w ich pierwotnej pozycji. Jeśli aparat

fotograficzny lub kamera wideo nie są dostępne, naszkicować plan systemu, oznakować porty i kable, dzięki czemu będzie można sprawdzić system i odtworzyć go w późniejszym terminie.

W praktyce należy doprowadzić do utrwalenia dokonanych czynności. W szczególności należy udokumentować jakie procesy bądź programy, a także nazwy otwartych dokumentów czy też plików są w chwili zabezpieczenia uruchomione. Należy spodziewać się, iż część z nich będzie działała wyłącznie w obszarze pamięci ulotnej. Tak też po wyłączeniu zostanie „bezpowrotnie" stracona. Istotnym elementem jest ustalenie czasu i daty włączonego urządzenia i porównanie go z czasem rzeczywistym. W przypadku gdy ustalenie pewnych istotnych faktów wymusza ingerencję w uruchomione środowisko systemowe czynność tą powinien wykonywać wyłączenie personel posiadający niezbędną wiedzę w tym zakresie.

W przypadku komputera wyłączonego nie należy go włączać, gdyż zmieni on wtedy swoją zawartość.

• jeśli jest to dozwolone, przeszukać obszary, aby znaleźć przedmioty, takie jak karteczki samoprzylepne.

W praktyce użytkownicy często nie pamiętają stosowanych haseł czy skrótów dlatego też zapisują je w miejscu dostępnym i łatwo zauważalnym lub częściowo ukrytym, np. pod klawiaturą czy w szufladzie. Należy przypuszczać również, iż będzie on używał jednego, tego samego lub nieznacznie zmodyfikowanego hasła, do wielu zasobów.

• odszukać dzienniki, dokumenty, notebooki lub podręczniki dotyczące użytkowania sprzętu i oprogramowania, z istotnymi szczegółami na temat urządzeń, takimi jak hasła i numery PIN.

W praktyce należy zabezpieczyć wszelką dokumentację związaną ze znajdowanym sprzętem który zostanie uznany jako istotny i włączony jako materiał dowodowy. W tym przypadku dokumenty te należy zapakować w oryginale lub kopii, jeśli jest taka możliwość razem ze sprzętem. Takie postępowanie pozwoli na przeprowadzenie późniejszego procesu badawczego w sposób łatwiejszy i szybszy.

4. Łańcuch dowodowy

W celu zapewnienia możliwie najlepszego nadzoru nad cyfrowym materiałem dowodowym zaleca się, aby w każdym momencie można było odtworzyć chronologię postępowania. Dlatego też istotnym elementem jest udokumentowanie przeprowadzonej czynności w jednym dokumencie, bądź zbiorze dokumentów wzajemnie powiązanych.

Z informatycznego punktu widzenia jednym z elementów kontrolnych będzie użycie funkcji weryfikującej, o której była mowa wcześniej. Oczywiście należy zastanowić się kiedy

tak naprawdę należy ją wyliczyć. W przypadku zabezpieczenia materiału dowodowego w całości, np. dysku twardego wyliczenie funkcji weryfikującej na miejscu zdarzenia wydaje się elementem zbędnym, gdyż w tym wypadku polegamy na zabezpieczeniu technicznym urządzenia i sporządzonej w tym celu dokumentacji. W takim przypadku czynność tą winien wykonać DES w chwili rozpoczęcia badań lub DEFR przed wykonaniem jakichkolwiek czynności z cyfrowym materiałem dowodowym. Natomiast w chwili wykonywania kopii danych, w postaci klonu lub/i obrazu nośnika oraz fragmentu danych, niewątpliwie taka czynność winna być przeprowadzona.

Jednym z szczególnych przypadków zabezpieczenia jest wykonanie zrzutu pamięci RAM lub/i częściowej kopii danych oraz zabezpieczenie transmisji danych. Należy zaznaczyć, iż sama czynności powinna być szczegółowo opisana z uwzględnieniem takich informacji jak: data i czas, użyte oprogramowanie, urządzenie podłączone w celu zapisania danych, dane DEFR lub DES. Nie ma jednak potrzeby, aby nośnik, na którym pierwotnie były zapisane dane w chwili eksportu[115] (np. dysk twardy, który w tym celu był podłączony do dowodowego komputera) stanowił sam w sobie materiał dowodowy. Z uwagi na koszty materiałowe same dane można w konsekwencji zapisać na nośnik optyczny[116]. W takim przypadku wyliczenie funkcji weryfikującej pierwotnych danych jest konieczne.

Samo pakowanie cyfrowego materiału dowodowego/techniczne jego zabezpieczenie winno nastąpić, już na miejscu zdarzenia w trakcie prowadzenia czynności.

5. Podsumowanie

Nie ma wątpliwości, iż w dobie tak dynamicznego rozwoju technologii IT kluczowym jest prawidłowe zabezpieczenie cyfrowego materiału dowodowego. Z punktu wykonywania technicznych czynności nadrzędną rolę pełni DEFR, który w ramach swoich wiadomości i doświadczenia podejmuje decyzje, co do kluczowych zadań wykonywanych na miejscu zdarzenia. Jednak samo usystematyzowanie tych czynności i wyjaśnienie podstawowych zagadnień stanowi podstawę do wykonania dalszych czynności w dowodzeniu prawdy o czynie.

---

[115] Wykonanie kopii danych bezpośrednio na nośniku zamontowanym w urządzeniu dowodowym jest niedopuszczalne, chyba że uwarunkowania techniczne nie dopuszczają innej możliwości (np. wykonanie częściowej kopii danych w systemach serwerowych).

[116] Należy jednak pamiętać, iż nośniki optyczne są wrażliwe na uszkodzenia mechaniczne dlatego w tym celu należy wykonać dodatkowe kopie tych danych.

6. Bibliografia

1. PN-EN ISO/IEC 27037:2016-12 "Technika informatyczna; Techniki bezpieczeństwa; Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego".
2. Holt T. J., Bossler A. M., Seigfried-Spellar K. C, Cybercrime and Digital Forensics An Introduction, Routledge 2018; ISBN: 978-1-138-23872-5 (hbk) ISBN: 978-1-138-23873-2 (pbk) ISBN: 978-1-315-29697-5 (ebk).
3. Shah, Makhdoom Syed Muhammad Baqir, Saleem, Shahzad, Zulqarnain, Roha, Protecting digital evidence integrity and preserving chain of custody, Journal of Digital Forensics, Security & Law. 2017, Vol. 12 Issue 2, s. 121-130, ISSN 558-7215.
4. Szmit M., Kilka uwag o ISO/IEC 27037:2012 oraz ENISA electronic evidence — a basic guide for First Responders, [w:] Kosiński J. (red): Przestępczość teleinformatyczna 2015, p. 101-110, WSPol., Szczytno 2015.
5. Zarządzenie nr 3 Komendanta Głównego Policji z dnia 17 stycznia 2014 r. w sprawie uprawnień do wydawania opinii oraz wykonywania czynności w policyjnych laboratoriach kryminalistycznych.
6. Decyzja nr 85 Dyrektora CLKP z dnia 21 kwietnia 2016 r.

ABSTRACT

DIGITAL EVIDENCE COLLECTION IN PN-EN ISO/IEC 27037 CONTEXT

Summary: This chapter is devoted to the issue of digital evidence collection based on the PN-EN ISO/IEC 27037 standard which was published on October 26th, 2017. As regards the certification of Police Forensic Laboratories in accordance with Polish Standard PN-EN ISO/IEC 17025:2005 is the first Polish document, taking into account and explaining in details the various stages and tasks involved in acquiring digital samples. The chapter discusses the issues related to problems connected with collecting evidence on crime stage explaining the primary steps. The author tries to assign commonly used "good practices" to the norm records.

Keywords: digital evedence, PN-EN ISO/IEC 27037, data, bit copy, chain of evidence.

ROZDZIAŁ 7

ODPOWIEDZIALNOŚĆ POŚREDNIKÓW INTERNETOWYCH W ŚWIETLE PRAWA UNII EUROPEJSKIEJ

Łukasz STERNOWSKI [117]

STRESZCZENIE: Niniejszy rozdział przedstawia przepisy prawa pochodnego Unii Europejskiej, które dotyczą odpowiedzialności pośredników za treści umieszczane w Internecie przez użytkowników ich usług. Zagadnienie to jest niezwykle istotne w świetle rosnącej popularności dystrybucji treści za pośrednictwem platform internetowych. Rozdział podejmuje próbę oceny czy obowiązujące przepisy pozostają aktualne i wystarczające do należytej ochrony praw własności intelektualnej.

SŁOWA KLUCZOWE: prawo własności intelektualnej, prawo autorskie, piractwo, Sprawiedliwości Unii Europejskiej, prawo Unii Europejskiej.

1. Wstęp

Nieustannie rosnąca popularność Internetu oraz świadczonych w nim usług, a także pojawiające się nowe rodzaje działalności internetowych sprawiają, że skala naruszeń w Internecie, choć w poszczególnych sektorach przejawia tendencje spadkowe, to wciąż plasuje

[117] LL. M., Członek Zarządu Stowarzyszenia Sygnał, Kierownik Działu Ochrony Własności Intelektualnej Cyfrowego Polsatu, lsternowski@cyfrowypolsat.pl.

się na bardzo wysokim poziomie – przeciętny użytkownik Internetu w Unii Europejskiej korzysta z pirackich treści 9,7 razy w miesiącu, przy czym na Łotwie jest to 26 razy, a w Finlandii mniej niż 4 razy w miesiącu[118].

Ponieważ pośrednicy usług internetowych zazwyczaj posiadają jedynie ograniczoną wiedzę na temat przetwarzanych lub przechowywanych przez nich danych, rozdzielenie odpowiedzialności pomiędzy dostawców tych usług, a ich użytkownikami może być problematyczne. Ponieważ dostawcy usług są podmiotami działającymi w sposób otwarty, tzn. nie ukrywają swojej tożsamości prawnej, wystąpienie do nich o usunięcie treści bezprawnych jest z praktycznego punktu widzenia dużo łatwiejsze, niż dotarcie do osoby, które daną treść zamieściła nie ujawniając przy tym swojej tożsamości.

Odpowiedzialność za treści umieszczane w Internecie może odnosić się, m.in. do praw autorskich, znaków towarowych, tajemnic handlowych oraz czynów nieuczciwej konkurencji. Odpowiedzialność pośredników internetowych oraz nałożone na nich obowiązki znajdują źródło w prawie pochodnym Unii Europejskiej. Niniejszy rozdział ma na celu przedstawienie regulacji UE dotyczących tej tematyki.

2. Wybrane rodzaje usług pośredników internetowych

Pojęcie pośrednika internetowego (Intermediary Service Provider, ISP) zostało wprowadzone w dyrektywie 2000/31 o handlu elektronicznym[119] (tzw. dyrektywa e-commerce), jednak nie zostało zdefiniowane w niej, ani w innych aktach prawa UE[120]. Wskazówki, co do charakteru działalności pośrednika internetowego odnajdujemy w motywie 42 dyrektywy, zgodnie z którym: „*działalność podmiotu świadczącego usługi społeczeństwa informacyjnego jest ograniczona do technicznego procesu obsługi i udzielania dostępu do sieci komunikacyjnej, w której informacje udostępniane przez osoby trzecie są przekazywane lub*

[118] Raport na zlecenie Europejskiego Urzędu ds. Własności Intelektualnej wskazuje, że w latach 2017-2018 piractwo telewizyjne spadło o 8%, filmowe o 19%, a muzyczne o aż 32%. Zob. EUIPO, Online Copyright Infringement in the European Union, Music, Films, and TV (2017-2018), Trends and Drivers, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/quantification-of-ipr-infringement/online-copyright-infringement-in-eu/online_copyright_infringement_in_eu_en.pdf (dostęp 16.06.2020 r.).

[119] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), OJ L 178, 17/7/2000, s.1-16.

[120] M. Piech, Pośrednicy Internetowi w Prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników, Warszawa 2019, s. 32.

przechowywane czasowo, w celu poprawienia skuteczności przekazu; działanie takie przybiera charakter czysto techniczny, automatyczny i bierny, który zakłada, że podmiot świadczący usługi społeczeństwa informacyjnego nie posiada wiedzy o informacjach przekazywanych lub przechowywanych ani kontroli nad nimi." Charakterystyka wybranych rodzajów działalności ISP przedstawiona został w dalszej części niniejszego rozdziału.

3. Hosting

Dostawcy usług hostingowych przechowują w swoich systemach teleinformatycznych dane dostarczane przez swoich użytkowników. To użytkownik decyduje jakie dane i na jak długo umieszcza w zasobach usługodawcy. Klasycznym przykładem usługi hostingu jest t.zw. webhosting będący udostępnieniem przestrzeni dyskowej na serwerze z przeznaczeniem na umieszczenie na nim strony internetowej.

Do hostingu odnosi się art. 14 dyrektywy, który w pkt 1 stanowi:

Państwa Członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę usługodawca nie był odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem, że:

a) usługodawca nie ma wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji, a w odniesieniu do roszczeń odszkodowawczych — nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o tej bezprawności; lub

b) usługodawca podejmuje niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony.

Jak wynika z przytoczonego powyżej przepisu, podstawą do wyłączenia odpowiedzialności dostawcy usługi hostingu jest brak wiedzy o bezprawnym charakterze treści przechowywanych w jego zasobach. Nie jest jednak wskazane źródło tej wiedzy, można zatem domniemywać, że nie ma ono znaczenia – niezależnie od sposobu uzyskania wiedzy usługodawca zobligowany jest do usunięcia lub zablokowania dostępu do wskazanej treści. Problematyczna natomiast może okazać się ocena przez usługodawcę czy wskazane treści charakteryzują się bezprawnością. Należy również zauważyć, że określone treści mogą być w sposób oczywisty bezprawne w świetle regulacji krajowych jednego państwa członkowskiego, podczas gdy w innym państwie członkowskim ocena kryterium bezprawności treści może być sporna. Jednym z najmniej kłopotliwych w tej materii rodzajów treści są pirackie

treści audiowizualne. W sytuacji, gdy premiera kinowa filmu, bądź premiera serialu na platformie VOD miała miejsce w niedalekiej przeszłości ocena legalności pliku zamieszczonego w serwisie hostingowym przez internautę wydaje się być bezsprzeczna.

4. Serwis społecznościowy

Przepisy dyrektywy e-commerce mają zastosowanie do wszystkich usług społeczeństwa informacyjnego. To szerokie pojęcie obejmuje swoim zakresem, m.in. sprzedaż towarów online, dostarczanie narzędzi wyszukiwania online, udostępnianie platform VOD[121]. W efekcie zakresem stosowania dyrektywy objęty jest szeroki wachlarz podmiotów działających w Internecie, w tym m.in. platformy społecznościowe[122]. Kwestie związane z odpowiedzialnością platformy społecznościowej za umieszczane na niej treści Trybunał Sprawiedliwości Unii Europejskiej rozważał w orzeczeniu C-360/10 w sprawie SABAM[123]. Sprawa trafiła do Trybunału w wyniku pytania prejudycjalnego skierowanego przez sąd belgijski, który miał wątpliwości czy może zażądać od platformy społecznościowej Netlog natychmiastowego zaprzestania udostępniania utworów z repertuaru SABAM. Trybunał orzekł, że nakaz zobowiązujący Netlog nie tylko do zainstalowania systemu filtrującego, który zobowiązywałby Netlog do aktywnego monitorowania wszystkich danych jej użytkowników i do zapobiegania naruszeniom praw własności intelektualnej w przyszłości, jest sprzeczny z art. 15 dyrektywy, lecz także z Kartą praw podstawowych. W orzeczeniu tym Trybunał szczegółowo przedstawił zasady działania platformy społecznościowej: „*Netlog obsługuje platformę sieci społecznościowej online. Na platformie tej każda zarejestrowana osoba otrzymuje do dyspozycji swój osobisty obszar zwany „profilem", który użytkownik ten może sam wypełnić i który jest dostępny na całym świecie. Zasadnicze zadanie tej platformy, z której codziennie korzystają dziesiątki milionów osób, polega na tworzeniu wirtualnych wspólnot, w ramach których osoby te mogą się komunikować i w ten sposób zawierać przyjaźnie. Na swoich profilach użytkownicy mogą w szczególności prowadzić dziennik, wskazywać, jakie są ich rozrywki i upodobania, pokazywać przyjaciół, umieszczać zdjęcia osobiste lub fragmenty filmów wideo. Jednakże zdaniem SABAM obsługiwana przez Netlog sieć społecznościowa umożliwia wszystkim użytkownikom korzystanie za pośrednictwem swojego profilu z utworów muzycznych i audiowizualnych z repertuaru SABAM poprzez udostępnianie tych utworów publiczności*

[121] Zob. motyw 18 dyrektywy.

[122] Zob. European Parlament, Reform of the EU liability regime for online intermediaries. Background on the forthcoming digidal services act. In-Depth Analysis, May 2020, s. 1.

[123] Wyrok Trybunału C-360/10 z dnia 16 lutego 2012 r., Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) przeciwko Netlog NV, ECLI:EU:C:2012:85.

w taki sposób, że inni użytkownicy wspomnianej sieci mogą mieć do nich dostęp, przy czym następuje to bez zgody SABAM, zaś Netlog nie uiszcza za to żadnej opłaty."[124] Natomiast w pkt 24 orzeczenia Trybunał wskazał, że „*bezsporne jest przede wszystkim, że operator platformy sieci społecznościowej online, taki jak Netlog, przechowuje na swoich serwerach informacje dostarczone przez użytkowników tej platformy dotyczące ich profili i że jest tym samym podmiotem świadczącym usługi hostingowe w rozumieniu art. 14 dyrektywy 2000/31*".

Powyższy opis mógłby z powodzeniem przedstawiać działalność każdej z popularnych platform społecznościowych, w tym portalu Facebook, co pozwala stwierdzić, że wszystkie platformy społecznościowe jakie funkcjonują obecnie w Internecie należy traktować jako działalność hostingową.

5. Dostawca Internetu. Dostawca sieci WiFi

Art. 12 dyrektywy odnosi się do usługi zwykłego przekazu polegającej na transmisji danych w sieci telekomunikacyjnej, które są dostarczane przez odbiorcę usługi lub na zapewnieniu dostępu do usługi telekomunikacyjnej. Dostawca usługi nie może być inicjatorem przekazu, nie wybiera odbiorcy przekazu oraz nie wybiera oraz nie modyfikuje informacji zawartych w przekazie. Jeżeli warunki te zostaną spełnione, dostawca usługi nie ponosi odpowiedzialności za przekazywane informacje (dane). Biorąc pod uwagę powyższe wytyczne do usług zwykłego przekazu można zaliczyć, m.in. dostarczanie infrastruktury sieciowej, dostępu do sieci, VPN czy DNS.

Kwestia czy dostawca publicznie dostępnej sieci WiFi odpowiada za naruszenia praw do treści chronionych została poruszona przez Trybunał w orzeczeniu C-484/14 w sprawie Mc Fadden[125]. Sprawa dotyczyła Tobiasa Mc Fadden, który prowadził sklep z oświetleniem oraz nagłośnieniem, w którym to sklepie zapewnił bezpłatny dostęp do sieci WiFi dla swoich klientów. Jedna z osób korzystających z sieci WiFi wykorzystała ją do udostępnienia do pobrania utworu, co naruszyło prawa Sony Music, które doręczyło Tobiasowi Mc Fadden formalne zawiadomienie o naruszeniu. Ten twierdząc, że nie sprawował on kontroli na siecią podniósł, że nie odpowiada za zaistniałe naruszenie. W efekcie przebiegu postępowania przed sądem krajowym, ten skierował pytania prejudycjalne do TSUE. Pytania dotyczyły, m.in. kwestii czy operator bezpłatnej sieci Wi-Fi, który eksploatuje sieć jedynie jako działalność

[124] Pkt 16-18 wyroku.

[125] Wyrok Trybunału C-484/14 z dnia 15 września 2016 r., Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH, ECLI:EU:C:2016:689.

pomocniczą w stosunku do swojej głównej działalności, jest objęty zakresem zwolnienia z odpowiedzialności przewidzianego w art. 12 dyrektywy o handlu elektronicznym. Trybunał stwierdził, że nieodpłatne udostępnianie sieci Wi-Fi w celu zwrócenia uwagi potencjalnych klientów na towary i usługi oferowane przez sklep stanowi „usługę społeczeństwa informacyjnego" w rozumieniu dyrektywy. Dalej Trybunał wskazał, że właściciel praw autorskich może zwrócić się do organu krajowego lub do sądu o nakazanie takiemu usługodawcy zaprzestania lub zapobieżenia naruszeniu prawa autorskiego popełnionemu przez jego klientów[126].

6. Występowanie o usunięcie treści o bezprawnym charakterze

Chociaż dyrektywa e-commerce nie formułuje procedury występowania o usunięcie treści o bezprawnym charakterze to jej art. 14 stanowi podstawę do jej wdrożenia przez państwa członkowskie. Jednakże poszczególne kraje rozwiązały tę kwestię na różne sposoby[127]. Pierwsza grupa to kraje nie posiadające szczególnych przepisów dotyczących blokowania, usuwania, bądź filtrowania treści. W tej sytuacji zastosowanie mają przepisy ogólne, bądź mechanizmy samoregulacji przyjęte przez rynek. Argumentem dla takiego rozwiązania jest brak możliwości nadążania przez ustawodawcę za rozwojem technologicznym. Niektóre państwa, w tym Polska zdecydowały, że do kwestii związanych z Internetem stosować należy przepisy ogólne, które de facto, gdy były tworzone, w żaden sposób nie miały dotyczyć zagadnień internetowych. Podobne podejście przyjęły Czechy. Druga grupa państw to te, które zdecydowały się podjąć próbę „uregulowania Internetu" poprzez przyjęcie odpowiednich przepisów wykonawczych stanowiących podstawę do występowania o zablokowanie określonych treści.

Kolejna, niezwykle istotna regulacja dotycząca blokowania treści przez pośredników znajduje się w dyrektywie 2001/29/WE w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, której art. 8 stanowi:

1. Państwa Członkowskie przewidują stosowne sankcje i środki naprawcze w przypadku naruszenia praw i obowiązków wymienionych w niniejszej dyrektywie i podejmują wszelkie niezbędne środki w celu zapewnienia ich realizacji. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.

---

[126] Pkt 79 wyroku.

[127] Szczegółowa analiza porównawcza tego zagadnienia dostępna jest w raporcie Rady Europy: Comparative Study on Blocking, Filtering and Take-Down of Illigal Internet Content 2015, https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html# (dostęp 25.06.2020 r.)

2. Każde Państwo Członkowskie podejmuje niezbędne środki w celu zapewnienia, aby podmiot praw autorskich, którego interesy zostaną naruszone przez czynności dokonane na jego terytorium, mógł wytoczyć powództwo o odszkodowanie i/lub wnioskować o wydanie nakazu i w miarę potrzeby, domagać się przepadku naruszonych dóbr, jak również urządzeń, produktów lub części składowych określonych w art. 6 ust. 2.

3. Państwa Członkowskie zapewnią, aby podmioty praw autorskich mogły wnioskować o wydanie nakazu przeciwko pośrednikom, których usługi są wykorzystywane przez stronę trzecią w celu naruszenia praw autorskich lub pokrewnych.

Warto zauważyć, że ustawodawca już w 2001 roku zdawał sobie sprawę z istoty ochrony praw autorskich w Internecie czego odzwierciedleniem jest motyw 59 preambuły:

Usługi pośredników mogą być, w szczególności w środowisku cyfrowym, coraz częściej wykorzystywane przez osoby trzecie w działalności naruszającej prawa. W wielu przypadkach pośrednicy tacy mają najwięcej możliwości, aby zakończyć takie naruszenia. Dlatego, z zastrzeżeniem wszystkich innych dostępnych sankcji lub środków naprawczych, podmioty praw autorskich powinny mieć możliwość domagania się wydania zakazu skierowanego do pośrednika, który w sieci utrzymuje naruszenia praw autorskich utworu lub innego przedmiotu objętego ochroną przez osobę trzecią. Możliwość taka powinna być dostępna, nawet jeżeli działania pośrednika stanowią przedmiot wyjątku na mocy art. 5. Warunki i metody dotyczące takich nakazów powinny być uregulowane w ramach prawa krajowego Państw Członkowskich.

W kontekście odpowiedzialności pośredników najistotniejszy jest art. 8 pkt 3 dyrektywy, pozwalający na uzyskanie nakazu zablokowania, co jest nieporównywalnie skuteczniejszym narzędziem, niż jedynie informowanie pośrednika o bezprawnym charakterze treści. Poszczególne państwa w wyniku implementacji dyrektywy wprowadziły przepisy krajowe w tym zakresie[128]. Dla przykładu, w Wielkiej Brytanii i w Danii istnieją mechanizmy pozwalające na zablokowanie strony internetowej z pirackimi treściami na poziomie krajowego DNS, dzięki czemu osoby znajdujące się na terytorium tych krajów nie mogą danej strony otworzyć. W Polsce trwa spór o to, czy implementacja została przeprowadzona we właściwy sposób. Przedstawiciele rynku reprezentujący posiadaczy praw autorskich i majątkowych twierdzą, że nie mają możliwości wystąpienia o nakaz przeciwko pośrednikowi, w wyniku

[128] Szczegółowa analiza porównawcza w zakresie implementacji dyrektywy 2001/29/WE przez państwa członkowskie: Foundation for Information Policy Reasearch, Implementing the EU Copyright Directive 2003, https://www.fipr.org/copyright/guide/eucd-guide.pdf (dostęp 25.06.2020 r.)

czego, jeżeli ten nie reaguje na wezwania do zablokowania treści, te nadal są onr dostępne dla internautów[129]. Natomiast strona rządowa podnosi, że istniejące przepisy prawa krajowego pozwalają na skuteczne wystąpienie o wydanie nakazu zaniechania naruszenia przeciwko pośrednikom[130].

7. Problemy praktyczne w dochodzeniu ochrony praw

Obecnie obowiązujące przepisy nie nakładają na pośredników obowiązku uniemożliwienia ponownego umieszczenia przez użytkownika tej samej treści. W praktyce oznacza to, że serwisy pirackie nawet jeżeli blokują treści, to niemal natychmiast te pojawiają się ponownie w serwisie. Należałoby zastanowić się czy w tego typu przypadkach pośrednik może faktycznie zasłaniać się brakiem wiedzy o bezprawnym charakterze treści. Przecież profesjonalnie działający przedsiębiorca powinien mieć wiedzę na temat uwarunkowań branży, w której prowadzi działalność. Przyjmując taki punkt widzenia wydaje się być naturalnym, że profesjonalista działający na rynku video online, jak np. operator (administrator) serwisu VOD powinien bez problemu ocenić, że jeżeli internauta umieszcza w jego zasobach superprodukcję amerykańskiej wytwórni filmowej, kilka dni po premierze, podczas gdy wytwórnia ta prowadzi szeroko zakrojone działania marketingowe, to internauta ten najprawdopodobniej nie dysponuje prawami do danego filmu.

Drugim najczęściej pojawiającym się problem w usuwaniu bezprawnych treści jest czas reakcji administratora serwisu. Jeżeli dochodzi do bezprawnego rozpowszechniania transmisji sportowej na żywo, to jedynie natychmiastowe zablokowanie treści może przynieść żądany efekt. Jeżeli podjęcie działań przez pośrednika trwa dłużej, to jest już ono bez znaczenia. Podobna sytuacja ma miejsce z wysokobudżetowymi produkcjami filmowymi w okresie tuż po premierze. Jeżeli nielegalny plik pojawi się w sieci, np. równo z premierą filmu, która najczęściej ma miejsce w piątki i posiadacz praw do danego filmu wystosuje wezwanie do usunięcia treści, które zostanie rozpatrzone przez pośrednika dopiero po weekendzie, to spowodowane straty będą ogromne.

---

[129] Zob. Stanowisko Stowarzyszenia Sygnał w sprawie komunikatu Komisji Europejskiej z dnia 28 września 2017 roku „Zwalczanie nielegalnych treści w Internecie. W kierunku większej odpowiedzialności platform internetowych COM(2017) 555 final, https://sygnal.org.pl//wp-content/uploads/2019/05/0a8963b445fe3cbc03f6478f618967bb.pdf (dostęp 26.06.2020 r.).

[130] Odpowiedź Ministerstwa Kultury i Dziedzictwa Narodowego na skargę Komisji Europejskiej dotyczącej nieprawidłowej transpozycji art. 8 ust. 3 dyrektywy 2001/29/WE z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, EU-Pilot 7935/15/CNCT.

Biorąc pod uwagę powyższe dla właściwej ochrony praw własności intelektualnej w Internecie niezbędnym jest taka implementacja art.8 pkt 3 dyrektywy 2001/29, aby właściciele praw mogli uzyskać nakaz wydany przeciwko pośrednikowi w przeciągu godzin, a nie tygodni czy miesięcy.

8. Podsumowanie

Ze względu na charakter prowadzonej działalności, pośrednicy internetowi mają szerokie możliwości techniczne, aby przeciwdziałać naruszeniom prawa dokonywanym z wykorzystaniem świadczonych przez nich usług. Przytoczone w niniejszym artykule przesłanki wyłączenia ich odpowiedzialności mają na celu ochronę przedsiębiorców przed kosztami ewentualnego filtrowania swoich zasobów pod kątem treści bezprawnych. Jest to zrozumiałe podejście ustawodawcy, jednakże wydaje się, że w świetle postępującej technologii argument ten zaczyna tracić na wartości. Przykładem mogą być największe platformy internetowe, jak Google czy Facebook, które zaimplementowały takie rozwiązania technologiczne, które pozwalają na niemal całkowite wyeliminowanie bezprawnych treści z aktywnym udziałem posiadaczy praw, którzy składając stosowne oświadczenia mogą łatwo i szybko wskazywać materiały naruszające ich prawo. Jeżeli natomiast nadal uznać, że tego rodzaju rozwiązania są zbyt dużym obciążeniem dla pośredników lub że dla niektórych kategorii pośredników jest to wręcz niemożliwe, to dobrym rozwiązaniem wydaje się być stworzenie szybkiego mechanizmu pozwalającego na uzyskanie przez posiadacza praw nakazu zablokowania treści, co mogłoby nastąpić w drodze wydania rozporządzenia UE.

9. Bibliografia

1. Comparative Study on Blocking, Filtering and Take-Down of Illigal Internet Content 2015, https://edoc.coe.int/en/internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-internet-content-.html#.
2. Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), OJ L 178, 17/7/2000.
3. Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, OJ L 167, 22.6.2001.

4. EUIPO, Online Copyright Infringement in the European Union, Music, Films, and TV (2017-2018), Trends and Drivers, https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/quantification-of-ipr-infringement/online-copyright-infringement-in-eu/online_copyright_infringement_in_eu_en.pdf
5. European Parlament, Reform of the EU liability regime for online intermediaries. Background on the forthcoming digidal services act. In-Depth Analysis, May 2020.
6. Foundation for Information Policy Reasearch, Implementing the EU Copyright Directive 2003, https://www.fipr.org/copyright/guide/eucd-guide.pdf.
7. Odpowiedź Ministerstwa Kultury i Dziedzictwa Narodowego na skargę Komisji Europejskiej dotyczącej nieprawidłowej transpozycji art. 8 ust. 3 dyrektywy 2001/29/WE z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, EU-Pilot 7935/15/CNCT.
8. Piech M., Pośrednicy Internetowi w Prawie Unii Europejskiej. Rola i obowiązki wobec treści użytkowników, Warszawa 2019.
9. Stanowisko Stowarzyszenia Sygnał w sprawie komunikatu Komisji Europejskiej z dnia 28 września 2017 roku „Zwalczanie nielegalnych treści w Internecie. W kierunku większej odpowiedzialności platform internetowych COM(2017) 555 final, https://sygnal.org.pl//wp-content/uplads/2019/05/0a8963b445fe3cbc03f6478f618967bb.pdf.
10. Wyrok Trybunału C-360/10 z dnia 16 lutego 2012 r., Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) przeciwko Netlog NV, ECLI:EU:C:2012:85.
11. Wyrok Trybunału C-484/14 z dnia 15 września 2016 r., Tobias Mc Fadden przeciwko Sony Music Entertainment Germany GmbH, ECLI:EU:C:2016:689.

ABSTRACT

THE RESPONSIBILITY OF ONLINE INTERMEDIARIES IN THE LIGHT OF EUROPEAN UNION LAW

Summary: This chapter sets out the European Union's legislation on the liability of intermediaries for content placed on the Internet by users of their services. This issue is extremely important in the light of the growing popularity of distributing content through online platforms. The chapter attempts to assess whether the existing provisions remain valid and sufficient to adequately protect intellectual property rights.

Keywords: intellectual property law, copyright, piracy, the Court of Justice of the European Union, European Union law.

ROZDZIAŁ 8

ODTWARZANIE ADRESÓW E-MAIL UŻYTKOWNIKÓW WYBRANYCH SERWISÓW ZAJMUJĄCYCH SIĘ BEZPIECZEŃSTWEM NA PODSTAWIE GRAVATARA

Dariusz KUŚNIERZ [131], dr inż. Przemysław RODWALD [132]

STRESZCZENIE: Duża część internautów pragnie być anonimowa podczas korzystania z usług i serwisów internetowych, nie podając swoich prawdziwych danych lub kryjąc się pod różnymi pseudonimami. Niestety niektóre usługi wykorzystywane na przykład na forach dyskusyjnych pozwalają na deanonimizację użytkowników. Taką usługą jest między innymi Gravatar oferujący wyświetlanie awataru użytkownika na podstawie adresu e-mail, prezentowanego nie w postaci jawnej, lecz w formie skrótu MD5. W rozdziale pokazano atak odtwarzający adresy e-mail na trzy najpopularniejsze polskie serwisy internetowe zajmujące się bezpieczeństwem.

SŁOWA KLUCZOWE: gravatar, funkcja skrótu, MD5.

1. Wprowadzenie

Gravatar (ang. *Globally Recognized Avatar*) jest szeroko stosowaną usługą, która dostarcza użytkownikowi publiczny profil, przypisujący awatar użytkownika do podanego adresu e-mail. Awatar ten pojawia się podczas zamieszczania postów na blogach oraz forach internetowych, korzystających z usługi Gravatara.

[131] Katedra Informatyki, Akademia Marynarki Wojennej, kusnierz.darius@gmail.com.
[132] Katedra Informatyki, Akademia Marynarki Wojennej, p.rodwald@amw.gdynia.pl; ORCID: 0000-0003-4261-8688.

Do identyfikacji użytkowników, usługa ta wykorzystuje przypisane każdemu użytkownikowi unikalne ciągi znaków, które zostały stworzone na postawie podanych przez nich adresów e-mail. Używana jest w tym celu kryptograficzna funkcja skrótu MD5. Ta jednokierunkowa funkcja, generująca 128-bitowy skrót (ang. *hash*), została opracowana przez Ronalda Rivest'a w 1991 roku [1]. Sama funkcja została złamana przez zespół z Shandong University w 2004 roku [2] i aktualnie generowanie dla niej kolizji, czyli dwóch wiadomości dających taki sam skrót, nie stanowi większego problemu. Jednak funkcja MD5 ciągle jest uznawana za odporną na znalezienie przeciwobrazu.

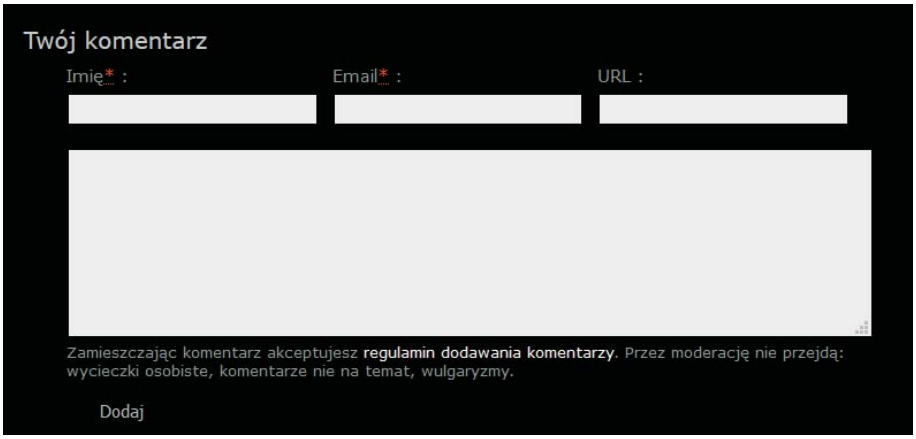
Podczas przeprowadzania ataków, zwłaszcza metodą ataku siłowego, kluczowym elementem jest moc obliczeniowa wykorzystywanej maszyny. Podczas łamania haseł lub w tym przypadku łamania adresów e-mail, powszechnie stosowanym i znacznie wydajniejszym podejściem jest wykonywanie operacji z wykorzystaniem kart graficznych zamiast procesora. Do przeprowadzenia ataków, została wykorzystana platforma sprzętowa posiadająca cztery karty graficzne GeForce RTX 2080 Ti FE 11GB przy użyciu oprogramowania hashcat. Został wykonany benchmark tej maszyny pod względem szybkości łamania skrotów MD5. Uzyskano wydajność na poziomie 220 GH/s.

Jednym z celów tego rozdziału jest przedstawienie możliwych sposobów ataku, mających na celu odtworzenie jak największej liczby adresów e-mail ze skrótów MD5, wykorzystywanych przez serwis Gravatar. Pokazana zostanie także skuteczność poszczególnych typów ataków.

W kolejnych częściach rozdziału zostanie przedstawiona szczegółowa metodologia wykorzystana podczas ataku na trzy wybrane polskie serwisy internetowe zajmujące się bezpieczeństwem. Następnie pokazane zostaną wyniki przeprowadzonych ataków wraz z oceną ich skuteczności. Na koniec zostaną przedstawione wnioski wypływające z przeprowadzonych badań.

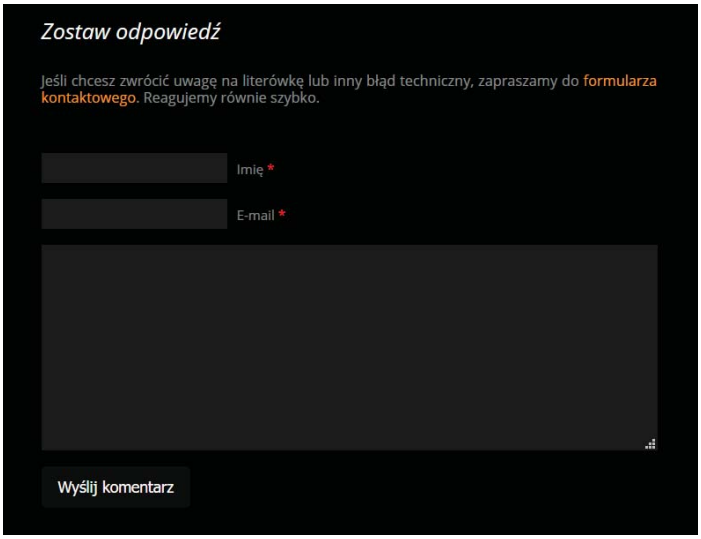
2. Ekstrakcja skrótów MD5

Przed rozpoczęciem badań, wybrano serwisy internetowe korzystające z usługi Gravatara do wyświetlania awatarów swoich użytkowników. Wybór padł na trzy serwisy związane z tematyką bezpieczeństwa: niebezpiecznik.pl (NBZ), sekurak.pl (SEK) oraz zaufanatrzeciastrona.pl (Z3S). Badanie rozpoczęto od sprawdzenia jakich danych serwisy te wymagają od swoich użytkowników przy umieszczaniu przez nich komentarzy. Zrzuty ekranów zawierające odpowiednie elementy formularza pokazane zostały na rysunkach 1-3.



Rys. 1. Formularz dodawania komentarza w serwisie niebezpiecznik.pl. Źródło: serwis niebezpiecznik.pl, dostęp: 22.05.2020.

Rys. 2. Formularz dodawania komentarza w serwisie sekurak.pl. Źródło: serwis sekurak.pl, dostęp: 22.05.2020.

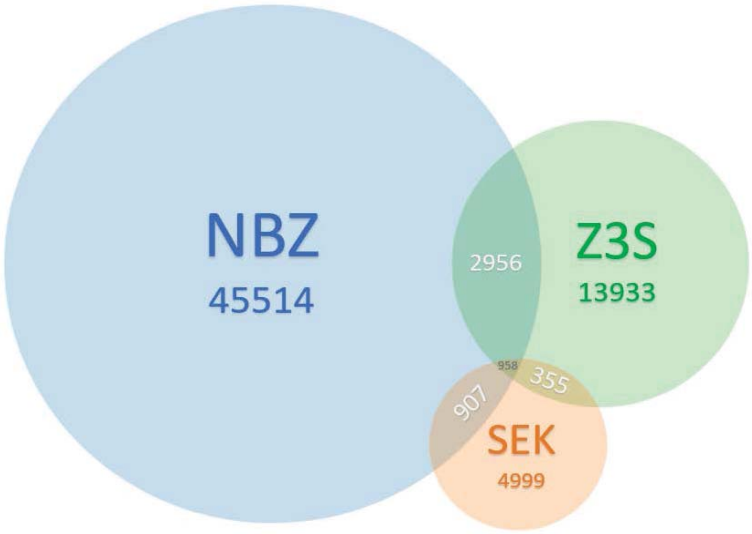


Rys. 3. Formularz dodawania komentarza w serwisie zaufanatrzeciastrona.pl. Źródło: serwis z3s.pl, dostęp: 22.05.2020.

Z załączonych rysunków wynika, że podanie imienia oraz adresu e-mail jest niezbędne przy dodawaniu komentarza we wszystkich trzech analizowanych serwisach. Tylko jeden serwis - SEK informuje swoich użytkowników, że adres e-mail nie zostanie opublikowany, co nie jest zgodne z prawdą, gdyż adres ten znajduje się w miejscu komentarza w formie skrótu MD5, a więc jest opublikowany lecz w zaciemnionej (ang. *obfuscated*) postaci. Pozostałe dwa serwisy – NBZ i Z3S – nie ustosunkowują się bezpośrednio do zagadnienia ewentualnego udostępniania adresów e-mail. W serwisie SEK przeszukano wszystkie komentarze znajdujące się pod wpisami znajdującymi się w działach Aktualności oraz Teksty. W serwisach Z3S oraz NBZ przeszukano wszystkie komentarze znajdujące się pod postami znajdującymi się na stronie głównej, w tym wszystkie wpisy archiwalne. Do ekstrakcji skrótów MD5 zawierających adresy e-mail użytkowników wykorzystano, specjalnie do tego celu przygotowany skrypt. Jego zadaniem było przeszukanie wszystkich podstron z komentarzami należących do danego serwisu i z każdej z nich wyciągnięcie oraz zapisanie skrótu MD5 oraz nazwy użytkownika (pole Imię w formularzach).

Skrypt został uruchomiony w dniach 21-22.05.2020, w rezultacie jego działania otrzymano łącznie 69622 unikalnych skrótów MD5: 50335 dla serwisu NBZ, 7219 dla SEK, oraz 18202 dla Z3S. Dane te zostały zapisane w bazie danych MySQL. Diagram Venna uka-

zujący liczby pozyskanych unikalnych skrótów MD5 zawierających adresy e-mail użytkowników zaprezentowano na rysunku 4. Pośród wyekstrahowanych skrótów, 958 znaleziono we wszystkich trzech serwisach (część wspólna wszystkich trzech zbiorów).



Rys. 4. Diagram Venna ilustrujący liczby wyekstrahowanych skrótów MD5. Źródło: opracowanie własne.

3. Struktura adresu e-mail

Przed przystąpieniem do tworzenia słowników czy nawet samego ataku, należało dokonać analizy struktury adresu e-mail, jego specyfikacji oraz najczęściej występujących w nim wzorców. Dokument RFC 5322 [3] specyfikuje, iż adres e-mail składa się z części lokalnej (ang. *local-part*), znaku „@" oraz z części domenowej (ang. *domain*). Może on się składać z maksymalnie 255 znaków, gdzie na część domenową przypadają 63 znaki, zgodnie z RFC 1035 [4]. Sam adres e-mail może zawierać w sobie znaki ASCII o kodach 33-90 i 94-126, a więc z wyłączeniem znaków: „[" , „]" oraz „\" [3].

Uwzględniając powyższy fakt, przeprowadzenie ataku siłowego na całej przestrzeni znaków byłoby nieefektywne. Ponieważ sprawdzane miały być adresy e-mail użytkowników, korzystających z polskich serwisów internetowych zawężono zbiór sprawdzanych adresów e-mail, do najpopularniejszych dostawców poczty elektronicznej w Polsce. Na podstawie do-

stępnych analiz [5-6] zdecydowano się na zawężenie części domenowej dla ataku hybrydowego i wybranych wariantów ataku brutalnego, do następujących jedenastu domen: gmail.com, wp.pl, op.pl, vp.pl, o2.pl, go2.pl, interia.pl, poczta.fm, poczta.onet.pl, gazeta.pl, tlen.pl.

W ramach fazy przygotowań do ataku hybrydowego oprócz domeny, przygotowano również zbiór możliwych części lokalnych adresu e-mail. Pobrano dwie listy: polskich imion oraz nazwisk, ponieważ częstą praktyką jest właśnie używanie tych właśnie danych przy tworzeniu adresów e-mail. Aby zwiększyć skuteczność ataku, została utworzona lista zawierająca różne połączenia tych danych osobowych z wybranymi znakami specjalnymi, dla wszystkich wzorców przedstawionych w tabeli 1. Lista ta nie zawiera pokazanych w tabeli cyfr, dołączanych na końcu części lokalnej, które to ze względów wydajnościowych dołączane były w formie maski podczas ataku hybrydowego.

Tab. 1. Wzorce dla części lokalnej adresu e-mail. Źródło: opracowanie własne.

Wzór	**Przykłady**
[nazwisko][?s][?d]{0,4}	kusnierz3, rodwald-123
[imię][?s][?d]{0,4}	dariusz, przemek_77
[nazwisko][?s][imię][?d]{0,4}	kusnierz.dariusz13, rodwaldprzemek2021
[imię][?s][nazwisko][?d]{0,4}	dariusz.kusnierz, przemyslaw_rodwald2
[nazwisko][?s][?l][?d]{0,4}	kusnierz.d, rodwald_p43
[?l][?s][nazwisko][?d]{0,4}	dkusnierz0808, p-rodwald
?d – cyfra, ?l – litera, ?s – znaki specjalne (tutaj: „.”, „-„, „_”)	

4. Przeprowadzenie ataków na skróty MD5

4.1. Atak siłowy

Atak rozpoczęto od metody siłowej, zwanej atakiem brutalnym. Polega on na sprawdzeniu wszystkich możliwych kombinacji z wybranego zestawu znaków. Każda kombinacja jest ustawiana w miejsce części lokalnej adresu e-mail i dostawiana jest do niej część domenowa wraz ze znakiem „@”. Z tak przygotowanego adresu e-mail, generowany jest skrót MD5, który następnie porównywany jest ze skrótami adresów e-mail użytkowników Gravatara. Po pomyślnym ich dopasowaniu zapisywany jest adres odpowiadający za dany skrót. Wykonano kilka wariantów ataku brutalnego.

Pierwszym z nich było sprawdzenie kombinacji zbioru wszystkich liter i cyfr, wraz ze znakiem „.” oraz „_” dla części lokalnej adresu e-mail, a dla części domenowej została użyta

przygotowana lista dziesięciu najpopularniejszych domen. Sprawdzenie wszystkich kombinacji dla części lokalnej złożonej z maksymalnie dziewięciu znaków, zajęło 30 minut dla każdej pojedynczej domeny, natomiast dla kombinacji 10 znaków było to już 18 godzin. Łącznie przeprowadzenie tego wariantu ataku siłowego, zajęło w przybliżeniu 204 godziny.

W drugim przygotowanym wariancie tego ataku dla części domenowej, wybrano zarówno domeny związane z atakowanymi serwisami: niebezpiecznik.pl, sekurak.pl oraz zaufanatrzeciastrona.pl, jak i wybrane domeny należące do tak zwanych jednorazowych adresów e-mail (ang. *disposable temporary e-mail address*): mailinator.com, protonmail.com, niepodam.pl, koszmail.pl, safe-mail.net. Za pomocą tego wariantu udało się odtworzyć 1136 adresów e-mail (1,63%). Czas ataku dla każdej domeny odpowiada czasom z wariantu pierwszego.

W trzecim, odmiennym wariancie ataku brutalnego, sprawdzono adresy e-mail składające się maksymalnie z 12 znaków, a więc i takie które są niepoprawne lub nie istnieją w rzeczywistości, ale użytkownicy ceniący sobie anonimowość mogli je podawać podczas umieszczania komentarzy, przykładowo: aaa@aa.pl, x@xxx.eu. Wykorzystano tu kombinację zbioru liter oraz cyfr, z wyznaczonym miejscem na znak „@" oraz „.". Kilka przykładowych masek wykorzystanych w tym ataku to: ?2?2@?2.?2?2, ?2?2@?2?2?2.?2?2, ?2?2?2?2?2?1@?2?2.?2?2, gdzie symbol ?2 odpowiada zbiorowi małych liter i cyfr (?l?d). Przeprowadzenie tego wariantu ataku siłowego, zajęło łącznie w przybliżeniu 130 godzin. Za pomocą wariantu pierwszego i trzeciego udało się sumarycznie odtworzyć 31279 adresów e-mail (44,93%).

4.2. Atak słownikowy

Atak słownikowy polega na pobieraniu kolejnych rekordów z pewnego słownika [7], generowaniu z każdego z nich skrótu i porównaniu otrzymanego wyniku ze skrótami adresów e-mail użytkowników Gravatara. W tym przypadku słownik stanowić więc będzie zbiór adresów e-mail. W celu przygotowania takiego słownika, skorzystano z danych pochodzących z jednych z największych kolekcji wycieków danych uwierzytelniających. Użyto danych pochodzących z części wycieków Exploit.in – która łącznie zawiera ponad 600 milionów rekordów oraz z danych zawartych w Collection#1 (773 milionów unikalnych adresów e-mail) oraz części Collection#2-6 (łączna liczba rekordów w nim zawartych wynosi 2,2 miliarda, a rozmiar całej kolekcji zajmuje 845 GB). W celu przygotowania słowników wyodrębniono adresy e-mail zawarte we wspomnianych zbiorach. Zajęło to autorom ponad 3 miesiące.

Po przygotowaniu słowników z wyekstrahowanymi adresami e-mail, wystarczyło porównywać stworzone na ich podstawie skróty MD5 ze skrótami użytkowników Gravatara. Słownik stworzony na podstawie Exploit.in został sprawdzony w 3 minuty, przy skuteczności

11371 (16,33%) odtworzonych adresów e-mail, a obie kolekcje Collection odpowiednio w 15 i 19 minut, przy sumarycznej skuteczności wynoszącej 20551 odtworzonych adresów (29,52%). Sumaryczna skuteczność ataku słownikowego wyniosła 20575 (29,55%). Znaczna część adresów znajdująca się w kolekcji Exploit.in zawiera się także w zbiorach Collection.

2.3. Atak hybrydowy

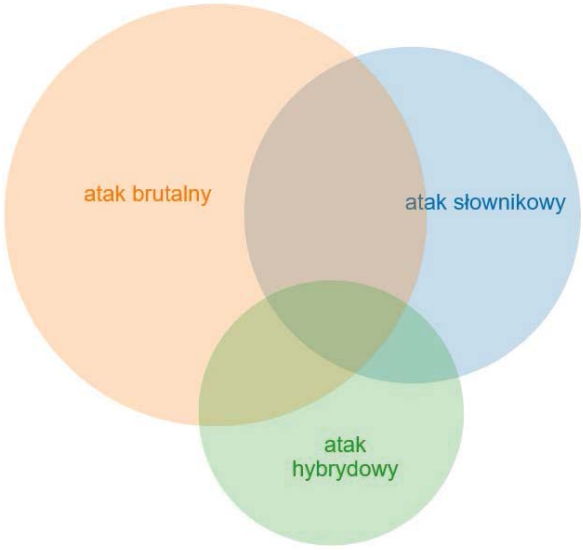
Podczas tego ataku, wykorzystano przygotowany i omówiony wcześniej słownik, zawierający różne kombinacje imion, nazwisk i wybranych znaków specjalnych (tabela 1). Słownik ten został użyty jako część lokalna adresu e-mail, natomiast jako część domenowa, posłużyły wpisy w masce zawierające listę przygotowanych wcześniej domen, w strukturze od „@domena" do „?d?d?d?d@domena". Łącznie sprawdzenie wszystkich masek zajęło 20 godzin, a skuteczność ataku wyniosła 18,36% (12780 z 69622).

2.4. Otrzymane wyniki

Poza wynikami pokazanymi w poprzednim punkcie, można przedstawić następujące rezultaty: dla NBZ złamano 61,03% (30717 z 50335) adresów e-mail, dla SEK złamano 57,78% (4171 z 7219) adresów e-mail, natomiast dla Z3S złamano 54,99% (10009 z 18202) adresów e-mail. Sumarycznie złamano **58,11%** (40463 z 69622) wszystkich skrótów MD5. Otrzymane wyniki są porównywalne z innymi tego typu atakami: w roku 2013 Bongard [9] po pobraniu 2400 skrótów MD5 Gravatara z francuskiego serwisu blogowego fdesouche.com, odtworzył 70% adresów e-mail jego użytkowników, w roku 2019 Rodwald [8] odtworzył 63,54% (8854 z 13935) adresów e-mail pochodzących z serwisu jakoszczedzacpieniadze.pl. Wartym podkreślenia jest, że tak wysoka skuteczność osiągana jest dla lokalnych, narodowych serwisów. W przypadku stron o zasięgu globalnym rezultaty są znacznie gorsze: w roku 2009 autor ukrywający się pod pseudonimem abell [10] po przeszukaniu 80000 skrótów MD5 Gravatara, odtworzył 10% adresów e-mail ze strony stackoverflow.com, a roku 2020 Rodwald [5] odtworzył z tego samego serwisu 1,25 miliona adresów e-mail (20,88%).

Próbując odpowiedzieć na pytanie jakie adresy e-mail są ukryte za tymi skrótami MD5 Gravatara, których nie udało się odzyskać, do możliwych domen zaliczyć można między innymi: domeny osobiste (np. rodwald.pl), domeny regionalne (np. gdynia.pl), domeny instytucjonalne (np. policja.gov.pl), domeny korporacyjne i firmowe (np. sailingbyte.com), mało popularni dostawcy poczty, błędnie wpisane domeny (np. gmial.com), domeny z innych krajów (np. mail.ru), czy też nieistniejące domeny (np. @cjttaslf.oj). W przypadku, gdy taki adres nie znajduje się z żadnym wycieku danych, na podstawie którego tworzony jest słownik, jego odtworzenie staje się obliczeniowo nieopłacalne.

Analizę skuteczności poszczególnych form zastosowanych ataków obrazuje diagram Venna zaprezentowany na rysunku 5.



Rys. 5. Diagram Venna ilustrujący skuteczność poszczególnych ataków. Źródło: opracowanie własne.

Diagram pokazuje, że zastosowane metody się uzupełniają, zastosowanie wszystkich trzech podejść daje najlepsze rezultaty. Dla ataku słownikowego kluczowe znaczenie ma wcześniejsze przygotowanie odpowiednich słowników, które (jak miało to miejsce w niniejszym ataku) może być czynnością bardzo czasochłonną. Jednak jest to czynność jednorazowa i tak przygotowany słownik może być wykorzystywany w kolejnych atakach.

Podczas badań zwrócono się do autora serwisu Z3S z prośbą o udostępnienie statystyk najpopularniejszych domen dla adresów e-mail podawanych przez użytkowników. Do najpopularniejszych dziesięciu domen należą kolejno: gmail.com, wp.pl, o2.pl, op.pl, interia.pl, onet.pl, poczta.onet.pl, niepodam.pl, tlen.pl, protonmail.com. W tabeli 2 pokazano częstości poszczególnych domen dla odzyskanych w ramach niniejszych badań adresów e-mail. Można zauważyć, że kolejność, przynajmniej dla najpopularniejszych domen, jest dość zbieżna.

Tab. 2. Częstotliwość adresów należących do najpopularniejszych domen dla odzyskanych adresów e-mail. Źródło: opracowanie własne.

Lp	Domena	Częstość
1	gmail.com	35,77%
2	wp.pl	16,14%
3	o2.pl	11,32%
4	interia.pl	3,33%
5	op.pl	3,16%
6	tlen.pl	1,66%
7	poczta.onet.pl	1,64%
8	poczta.fm	1,17%

Lp	Domena	Częstość
9	gazeta.pl	0,98%
10	niepodam.pl	0,89%
11	vp.pl	0,84%
12	mailinator.com	0,69%
13	hotmail.com	0,64%
14	onet.pl	0,62%
15	protonmail.com	0,55%
16	outlook.com	0,48%

Losowo wybierane skróty MD5 wraz z odpowiadającymi im odtworzonymi adresami e-mail (przedstawionymi w postaci zanonimizowanej, na przykład p******r@wp.pl) są prezentowane dynamicznie na dedykowanych stronach[133].

4. Podsumowanie

Zaprezentowane metody przeprowadzenia ataków na strony internetowe korzystające z Gravatara, na przykładzie trzech polskich serwisów poświęconych bezpieczeństwu, pokazują, iż korzystanie z tego typu usług, wiąże się z realnym zagrożeniem pozyskania adresów e-mail podawanych przez użytkowników podczas dodawania komentarzy. Zauważyć należy również, iż adres e-mail może zawierać dane jednoznacznie identyfikujące jego właściciela, a więc grozić jego potencjalną deanonimizacją.

Porównując statystyki domen wśród odzyskanych adresów e-mail z badanych serwisów zajmujących się bezpieczeństwem w stosunku do innych serwisów (na przykład jakoszczedzacpieniadze.pl [8]) można zauważyć większą popularność wykorzystywania przez użytkowników jednorazowych adresów e-mail (np. w domenie niepodam.pl). Pokazuje to większą świadomość tych użytkowników, którzy pragną pozostać bardziej anonimowi.

[133] https://rodwald.pl/blog/1413/adresy-e-mail-odtworzone-z-gravatarow-w-serwisie-niebezpiecznik-pl, https://rodwald.pl/blog/1415/adresy-e-mail-odtworzone-z-gravatarow-w-serwisie-sekurak-pl, https://rodwald.pl/blog/1417/adresy-e-mail-odtworzone-z-gravatarow-w-serwisie-zaufanatrzecia-strona-pl

Przedstawiony atak ma również na celu zwiększenie świadomości użytkowników publikujących komentarze w różnych serwisach internetowych, w zakresie potencjalnej możliwości ujawnienia ich adresów e-mail. Współcześnie większość stron internetowych, w tym te analizowane w niniejszej pracy, jest oparta na WordPressie. Ten system zarządzania treścią ma domyślnie włączoną usługę korzystającą z Gravatara, co może narażać użytkowników na ujawnianie adresów e-mail, a czasami nawet na pełną identyfikację.

Podziękowania

Autorzy pragną podziękować Adamowi Haertle – autorowi serwisu zaufanatrzeciastrona.pl za podzielenie się statystykami, dotyczącymi domen adresów e-mail, umieszczonych w nim komentarzy.

5. Bibliografia

1. Rivest R., *The MD5 Message-Digest Algorithm. RFC 1321,* 1992, https://tools.ietf.org/html/rfc1321 (dostęp: 03.01.2021).
2. Wang X., Feng D., Lai X., Yu H., *Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD,* 2004, https://eprint.iacr.org/2004/199.pdf (dostęp: 03.01.2021).
3. Resnick P., Ed., *Internet Message Format 2004*, https://tools.ietf.org/html/rfc5322 (dostęp: 03.01.2021).
4. Mockapetris P., *Domain names – implementation and specification 1987,* https://tools.ietf.org/html/rfc1035 (dostęp: 03.01.2021).
5. Rodwald P., *Large Scale Attack on Gravatars from Stack Overflow*, International Conference on Dependability and Complex Systems, Springer, Cham, 2020, s. 503-512.
6. tw, *Gmail i WP Poczta zyskują, w dół Poczta Onet i Yahoo Mail (TOP serwisów mailowych),* 11.05.2020, https://www.wirtualnemedia.pl/artykul/gmail-i-wp-poczta-zyskuja-w-dol-poczta-onet-i-yahoo-mail-top-serwisow-mailowych (dostęp: 05.01.2021).
7. Rodwald P., *Wybór strategii łamania hasła przy nałożonych ograniczeniach czasowych*, Biuletyn Wojskowej Akademii Technicznej, 2019, 68(1).
8. Rodwald P., *Możliwości pozyskiwania adresów e-mail z serwisów internetowych używających Gravatara*, Biuletyn Wojskowej Akademii Technicznej, 2019, 68(2).
9. Bongard D., *De-anonymizing Users of French Political Forums*, 0xcite LLC, Luxembourg, 2013, http://archive.hack.lu/2013/dbongard_hacklu_2013.pdf (dostęp: 07.01.2021).

10. abell, *Gravatars: why publishing your email's hash is not a good idea*, developer.it, 08.12.2009, http://www.developer.it/post/gravatars-why-publishing-your-email-s-hash-is-not-a-good-idea (dostęp: 07.01.2020).

ABSTRACT

GRAVATAR-BASED RECONSTRUCTION OF EMAIL ADDRESSES OF SELECTED SECURITY SERVICES USERS

Summary: A large number of Internet users wish to be anonymous while using Internet services and websites, not giving their real data, or hiding under various pseudonyms. Unfortunately some services used for example on discussion forums allow for deanonymization of users. One of such services is Gravatar, which displays a user's avatar based on their email address, presented not in plain text but as an MD5 hash. The chapter shows an email address recreation attack on three of the most popular Polish security websites.

Keywords: gravatar, hash function, MD5.

ROZDZIAŁ 9

WYKORZYSTANIE COVID-19 W SCENARIUSZACH ATAKÓW OPARTYCH NA SOCJOTECHNICE

dr hab. inż. Agnieszka GRYSZCZYŃSKA [134]

STRESZCZENIE: Pandemia COVID -19 znacząco wpłynęła na metody pracy, nauki czy realizacji zadań publicznych. Zarówno w Polsce jak i na świecie pandemia COVID – 19 dla cyberprzestępców stała się okazją do zwiększenia skuteczności ataków opartych na socjotechnice. Dotychczasowe scenariusze ataków, zostały dostosowane do aktualnej sytuacji pandemicznej. Niewątpliwie najczęstszymi w Polsce incydentami bazującymi nad lęku przed pandemią, za które odpowiedzialni są rodzimi cyberprzestępcy, są czyny nakierowane na monetyzację - oszustwa, oszustwa internetowe oraz kradzieże z włamaniem środków pieniężnych zapisanych na rachunku bankowym. Bardzo aktywnie działają grupy zajmujące się tworzeniem fałszywych stron podszywających się pod strony internetowe agentów rozliczeniowych i banków. Dużą skalę przestępczej działalności wykazują również cyberprzestępcy przejmujący dane do logowania do portali społecznościowych.
Nowe zagrożenia skłaniają do dyskusji nad anonimowym korzystaniem z usług elektronicznych oraz metodami weryfikacji tożsamości osób, które z usług tych chcą korzystać. Zagadnienie to nierozerwalnie wiąże się z narastającym zjawiskiem kradzieży tożsamości.
W rozdziale omówiono najczęstsze, bazujące na socjotechnice scenariusze ataków nakierowanych na osiągnięcie przez sprawców korzyści majątkowych obserwowane w Polsce. Analizie poddano czynniki ułatwiające przestępcom skuteczne przeprowadzenie ataku i utrudniające ustalenie ich tożsamości.

SŁOWA KLUCZOWE: cyberbezpieczeństwo, cyberprzestępczość, inżynieria społeczna, socjotechnika, phishing, kradzież tożsamości.

[134] Katedra Prawa Informatycznego, Wydział Prawa i Administracji, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, a.gryszczynska@uksw.edu.pl, ORCID: 0000-0003-3004-5253.

Wstęp

Analiza krajowych i międzynarodowych raportów dotyczących cyberbezpieczeństwa pozwala zaobserwować stały, znaczny wzrost ilości incydentów[135]. Znaczna część z nich to czyny zabronione. W 2020 roku problemy cyberbezpieczeństwa unaocznił i wyeksponował związany z pandemią COVID-19 *lockdown*, powodujący nagłe przejście do wykonywania pracy, świadczenia usług oraz realizacji zadań publicznych *online*. Do nowych warunków niezwykle szybko dostosowali się również sprawcy cyberprzestępstw, uznawanych za najbardziej dynamiczną formę przestępczości[136]. Cyberprzestępcy tworzą zarówno nowe *modi operandi*, jak również dostosowują już istniejące do nowej sytuacji, wykorzystują nowe wektory ataków i obejmują nimi nowe kategorie ofiar.

Dla cyberprzestępców COVID-19 jest okazją do zwiększenia skuteczności ataków opartych na socjotechnice. Różne scenariusze ataków obserwowano w różnych fazach wprowadzania obostrzeń. Niewątpliwie najczęstszymi w Polsce incydentami bazującymi na lęku przed pandemią były oszustwa. Popełniano je zarówno przy wykorzystaniu istniejących już portali aukcyjnych jak również przez tworzenie fałszywych sklepów internetowych, gdzie oferowano środki higieniczne i ochronne (płyny do dezynfekcji, maseczki, rękawiczki, przyłbice), jak również wykorzystując czasowe ograniczenia w możliwości dokonywania osobistych zakupów w sklepach stacjonarnych (sprzedaż, m.in. elektroniki). Ponadto bardzo aktywnie działały grupy zajmujące się tworzeniem fałszywych stron agentów rozliczeniowych i banków oraz grupy przejmujące dane do logowania do portali społecznościowych. Scenariusze ataków związane z COVID-19 wykorzystano również w oszustwach w modelu BEC

---

[135] Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf, Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2019, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf (dostęp: 24.10.2020), Check Point Blog 2020. Coronavirus update: not the type of CV you're looking for. https://blog.checkpoint.com/2020/06/04/coronavirus-update-not-the-type-of-cv-youre-looking-for/ (dostęp 24.10.2020), H2 REPORT 2020. Email Fraud & Identity Deception Trends. Global Insights from the Agari Identity Graph. 2020. https://www.agari.com/cyber-intelligence-research/e-books/agari-h2-2020-email-fraud-report.pdf (24.10.2020), IC3 Internet Crime Report 2019, s. 9. https://pdf.ic3.gov/2019_IC3Report.pdf (dostęp: 24.10.2020), Internet Organised Crime Threat Assessment (IOCTA) 2020, Europol, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020, dalej: IOCTA 2020 (dostęp: 24.10.2020).

[136] IOCTA 2020, s. 4.

oraz oszustwach nigeryjskich.

W rozdziale analizie poddano dwa najczęstsze, bazujące na socjotechnice scenariusze ataków nakierowanych na osiągnięcie przez sprawców korzyści majątkowych obserwowane w Polsce – tworzenie fałszywych stron agentów rozliczeniowych i banków oraz tworzenie fałszywych stron informacyjnych w celu przejęcia danych do logowania do portali społecznościowych. Celem pogłębionej analizy tych ataków, obejmującej sposoby działania sprawców i mechanizmy przez nich wykorzystywane jest wskazanie czynników ułatwiających przestępcom popełnienie czynu zabronionego i utrudniających ustalenie ich tożsamości. Pozwoli to na sformułowanie postulatów zmian przepisów niezbędnych do skutecznego przeciwdziałania nowym zagrożeniom.

Wykorzystanie inżynierii społecznej przez cyberprzestępców

Inżynieria społeczna (socjotechnika) od wielu lat była przedmiotem badań socjologicznych i rozumiana jako umiejętność skutecznego oddziaływania na innych, a także jako ogół metod i działań indywidulanych lub grupowych, których celem jest uzyskanie pożądanego zachowania jednostek lub grup społecznych[137]. Stosunkowo niedawno inżynieria społeczna stała się przedmiotem badań nauki o bezpieczeństwie oraz informatyki. W informatyce socjotechniką określa się sztukę manipulacji ludźmi w celu nakłonienia ich do podjęcia określonych działań lub ujawnienia poufnych informacji. W atakach socjotechnicznych nie jest wymagana zaawansowana wiedza techniczna, sprzęt lub złośliwe oprogramowanie, kluczowe są jedynie umiejętności oddziaływania na ludzi w celu, np. skłonienia ich do wykonania określonych czynności czy podania określonych informacji.

Jak wskazuje Europol, zarówno przedstawiciele organów ścigania, jak i sektora prywatnego uznają wykorzystanie inżynierii społecznej za podstawowe zagrożenie i czynnik ułatwiający popełnienie innych typów cyberprzestępstw – zarówno ułatwianych przez sieci i systemy informacyjne (*cyber-enabled crimes*), jak również bez nich niemożliwych (*cyber-dependent crimes*). Zauważalny jest również zróżnicowany poziom zaawansowania ataków i atakujących. Z uwagi na nieodpowiednie środki bezpieczeństwa lub niewystarczającą wiedzę i umiejętności użytkowników, nawet słabo przygotowane ataki oparte na socjotechnice kończą się sukcesem sprawców. Jednocześnie rośnie ilość dobrze przygotowanych ataków, za które odpowiadają sprawcy stosujący holistyczne strategie łączące socjotechnikę z umie-

[137] Socjotechnika: praktyczne zastosowania socjologii, red. A. Podgórecki, Warszawa 1968.

jętnością wykorzystania narzędzi, systemów i luk w zabezpieczeniach, wykorzystaniem fałszywych tożsamości oraz działaniem w ścisłej współpracy z innymi cyberprzestępcami. Ukierunkowane ataki stały się łatwiejsze dzięki modelowi CaaS (*Cybercrime-as-a-Service*), zaś wzrost wyrafinowania sprawców szczególnie widoczny jest w obszarze płatności bezgotówkowych[138].

Do najczęstszych ataków opartych na inżynierii społecznej można zaliczyć: *phishing* – czyli atak wykorzystujący inżynierię społeczną w celu wyłudzenia poufnych informacji poprzez podszycie się pod inny, zaufany podmiot. Jak wskazują raporty zespołu CERT Polska w 2018 roku *phishing*[139] stanowił 44 % wszystkich incydentów[140], w 2019 r. jako phishing sklasyfikowano 3 516 incydentów, co stanowiło 54,2 %[141]. CSIRT GOV w 2019 r. na 12 405 wszystkich zarejestrowanych incydentów odnotował 1 178 incydentów sklasyfikowanych jako phishing[142].

W literaturze rozróżnia się ataki ukierunkowane na konkretne osoby (*spear phishing*), na osoby decyzyjne, kierowników jednostek organizacyjnych (*whaling*), ataki w których do wyłudzanie danych dochodzi w trakcie rozmowy telefonicznej (*vishing*) lub za pośrednictwem wiadomości SMS (*smishing*). Do ataków socjotechnicznych zalicza się również *Business Email Compromise* (BEC), *SIM swapping* oraz oszustwo nigeryjskie, a także wymagające lepszego przygotowania technicznego *spoofing* i *pharming*. Z uwagi na to, że scenariusze ataków opartych na socjotechnice są bardzo zróżnicowane to zastosowane techniki oraz cel działania sprawców będą w dużej mierze determinowały właściwą kwalifi-

---

[138] IOCTA 2020, s. 6-7, 13-17.

[139] Zgodnie z Incident Classification/ Incident Taxonomy according to eCSIRT.net 2012, stanowiącą podstawę klasyfikacji infcydentów w raportach CERT Polska phishing rozumiany jest jako "podszywanie się pod inną jednostkę w celu przekonania użytkownika do ujawnienia prywatnych danych uwierzytelniających" (masquerading as another entity in order to persuade the user to reveal a private credential), więcej patrz: Incident Classification/ Incident Taxonomy according to eCSIRT.net, International Version Don Stikvoort, 11 Jan – 19 Dec 2012 (version mkVI of 31 March 2015). https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (dostęp 24.10.2020).

[140] Krajobraz bezpieczeństwa polskiego Internetu, Raport roczny z działalności CERT Polska 2018, s. 12.

[141] Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2019, s. 9, 15-16.

[142] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku, CSIRT GOV, s. 8-9, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html (dostęp 24.10.2020).

kację prawną konkretnego czynu. Jeśli działanie sprawców polega na nieuprawnionym uzyskaniu danych do logowania do konta poczty elektronicznej ofiary poprzez przełamanie lub ominięcie zabezpieczeń – wypełnią znamiona czynu z art. 267 § 1 kk[143]. Znamiona czynu z art. 286 § 1 kk zostaną wypełnione jeśli sprawca w celu osiągnięcia korzyści majątkowej doprowadzi inną osobę do niekorzystnego rozporządzenia mieniem poprzez prowadzenie jej w błąd lub wyzyskanie błędu (dla przykładu BEC lub oszustwo nigeryjskie), jeśli zaś w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody bez upoważnienia wpłynie na automatyczne przetwarzanie danych (np. *pharming*) – popełni czyn z art. 287 § 1 kk.

Analiza raportów bezpieczeństwa i piśmiennictwa wskazuje, że *phishing* staje się coraz bardziej wyszukany czy wyrafinowany[144], ukierunkowany na konkretnych użytkowników lub ich grupy, a przez to również trudniejszy do wykrycia. Kampanie są szybsze i coraz bardziej zautomatyzowane, skraca się również czas pomiędzy pozyskaniem danych od użytkownika (np. loginów i haseł) do ich wykorzystania w kolejnym ataku. W atakach ukierunkowanych (*spear phishing*) sprawcy nie tylko dbają o językową poprawność ale również w komunikacji z ofiarą uwzględniają zwyczaje czy aktualne wydarzenia polityczne i kulturalne[145].

W Polsce obserwuje się zarówno oparte na socjotechnice wykorzystującej COVID-19 ataki o globalnym charakterze, jak również działalność polskich cyberprzestępców, którzy pandemię wykorzystują głównie do popełniania oszustw (fałszywe sklepy i oferty sprzedaży środków ochronnych), infekowania użytkowników Internetu złośliwym oprogramowaniem (aktualnie dynamicznie wzrasta ilość infekcji złośliwym oprogramowaniem urządzeń mobilnych z systemem Android), przejmowania danych do logowania do portali społecznościowych, jak również dokonywania kradzieży z włamaniem środków z rachunków bankowych przy wykorzystaniu stron internetowych podszywających się pod agentów rozliczeniowych i banki oraz nieuprawnionego uzyskiwania danych do logowania.

---

[143] Kodeks karny z dnia 6 czerwca 1997 r., t.j. Dz.U. z 2020 r. poz. 1444, dalej jako kk.

[144] W literaturze anglojęzycznej często używane jest określenie "sophistication" – patrz: N. DePaula, G. Sanjay, "A Sophistication Index for Evaluating Security Breaches", 11th Annual Symposium on Information Assurance, 2016, https://www.albany.edu/iasymposium/proceedings/2016/06_DePaula_Goel_ASIA2016.pdf, B. Buchanan, "The Legend of Sophistication in Cyber Operations", https://www.belfercenter.org/publication/legend-sophistication-cyber-operations, 2017 (dostęp: 24.10.2020).

[145] IOCTA 2020, s. 13-17.

Wykorzystanie COVID-19 w scenariuszach ataków ukierunkowanych na przejmowanie danych do logowania do bankowości elektronicznej i kradzież środków pieniężnych zapisanych na rachunkach bankowych

Zgodnie z raportami zespołu CERT Polska, jednym z częstszych ataków na obywateli Polski jest wykorzystanie scenariuszy, w których sprawcy podszywają się pod strony agentów rozliczeniowych Dotpay Sp. z o.o. i PayU S.A. oraz banki. Incydenty z tej kategorii obserwowane są od połowy 2017 roku, przy czym od 2018 r. znacząco zwiększyła się ilość rejestrowanych dla tego scenariusza nazw domenowych - od kilku dziennie do kilkudziesięciu miesięcznie. Różnice w specyficznych ścieżkach używanych w fałszywym systemie płatności pozwoliły na rozpoznanie 5 odrębnych grup wykorzystujących ten modus operandi[146].

W ataku wykorzystującym tzw. „fałszywą bramkę płatności" przestępcy przy użyciu różnych scenariuszy i metod socjotechnicznych przekonują ofiary do dokonania płatności online. Dotychczas udało się zaobserwować różne sposoby nakłonienia pokrzywdzonych do wejścia na fałszywą stronę internetową płatności. Jednym z nich jest publikowanie na portalach ogłoszeniowych (np. OLX) lub portalach społecznościowych (np. Facebook) ofert sprzedaży towaru po bardzo atrakcyjnych cenach (np. telefonów, dronów) lub oddania za darmo różnych produktów (głównie zabawek, wózków dziecięcych, artykułów pielęgnacyjnych i higienicznych dla dzieci). Kolejnym jest tworzenie stron fałszywych sklepów internetowych z atrakcyjnymi cenami (np. sklep arya-toys.com i powiązana ze sklepem nazwa domenowa payu24.com, pod którą dostępna była strona podszywająca się pod Dotpay Sp z o.o.). Osoby, które dokonają zakupu otrzymują od sprawców wiadomość przesłaną pocztą elektroniczną, SMSem lub komunikatorem elektronicznym (np. Messenger), w której znajduje się informacja o płatności wraz z linkiem prowadzącym do fałszywej strony imitującej stronę agenta rozliczeniowego, a następnie banku. Osoby, które odpowiedziały na ogłoszenie o oddaniu za darmo produktu otrzymują wiadomość o konieczności opłacenia przesyłki wraz z hiperłączem do płatności, który również prowadzi do fałszywej strony internetowej. W tym modelu sprawcy wysyłają wiadomości jedynie do osób, które wcześniej były zainteresowane udostępnioną przez nich ofertą.

[146] Krajobraz bezpieczeństwa polskiego Internetu, Raport roczny z działalności CERT Polska 2018, s. 59-67 oraz Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2019, s. 9, 51-53.

Innym sposobem nakłonienia ofiar do dokonania płatności jest wykorzystanie danych dostępnych na portalach ogłoszeniowych (numerów telefonów oraz adresów e-mail) i wysłanie do osób, które umieściły tam ogłoszenia informacji o konieczności dopłaty lub odblokowania konta zablokowanego z uwagi na zadłużenie (przykładowe nazwy domenowe: otomoto.platnosci24.net, otomoto.transfery24.com, p-otomoto.com, otomoto-platnosc.net).

W modelu tzw. „fałszywej bramki płatności" wykorzystany został również nieuprawniony dostęp do bazy danych klientów sklepu internetowego Morele.net Sp. z o.o. Co najmniej od 21 listopada 2018 r. do połowy grudnia 2018 r. klienci sklepu bezpośrednio po dokonaniu zakupu otrzymywali wiadomości SMS nakłaniające do dopłaty niewielkiej kwoty do zamówienia. W treści wiadomości znajdowało się hiperłącze prowadzące do fałszywej strony internetowej podszywającej się pod stronę Dotpay Sp. z o.o. (platnosci-morele.online, platnosc24.com). Dopiero w dniu 18.12.2019 roku sklep internetowy poinformował o incydencie bezpieczeństwa obejmującym dane osobowe ponad 2 mln klientów. W związku ze stwierdzonym przez Prezesa UODO niewystarczającym zastosowaniem środków technicznych i organizacyjnych do zabezpieczenia danych klientów, decyzją z dnia 10 września 2019 r. nałożono na spółkę Morele.net Sp. z o. o. rekordową administracyjną karę pieniężną w wysokości 2,8 mln zł[147]. Wojewódzki Sąd Administracyjny w Warszawie wyrokiem z dnia 3 września 2020 r. oddalił skargę na decyzję Prezesa UODO uznając decyzję za zasadną[148]. Dotychczas brak jest przekazanych do publicznej wiadomości informacji o ustaleniu sprawców, którzy uzyskali nieuprawniony dostęp do bazy danych spółki oraz wykorzystywali go do wysyłania kupującym linków prowadzących do fałszywych stron pośredników płatności.

Hiperłącza do fałszywych stron płatności rozsyłane są również masowo, bez wcześniejszego dostosowania do odbiorców scenariusza ataku. Sprawcy najczęściej wysyłają wiadomości SMS (w zdecydowanej mniejszości w niespersonalizowanych kampaniach wysyłane są wiadomości e-mail) z informacją o konieczności dokonania płatności. Dominuje socjotechnika związana z koniecznością dopłacenia do przesyłki i podszyciem się pod przedsiębiorców świadczących usługi przewozowe, spedycyjne lub pocztowe usługi kurierskie (głównie DHL, DPD, Inpost, Pocztę Polską), dopłatą do zamówienia, anulowaniem subskrypcji. W pierwszej

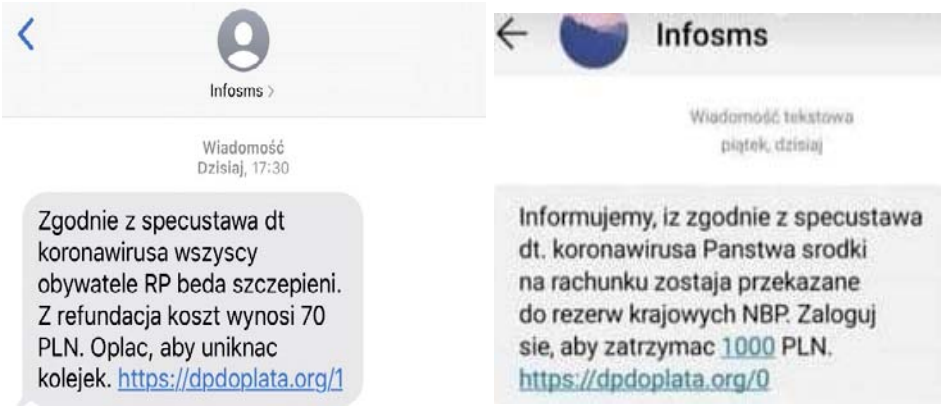
---

[147] Patrz: Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 10.9.2019 r, ZSPR.421.2.2019, https://uodo.gov.pl/decyzje/ZSPR.421.2.2019 a także https://zaufanatrzeciastrona.pl/post/jak-zlodzieje-chcieli-morele-net-szantazowac-z-nasza-pomoca/ (dostęp 24.10.2020).

[148] Wyrok WSA w Warszawie z 3.9.2020 r., II SA/Wa 2559/19.

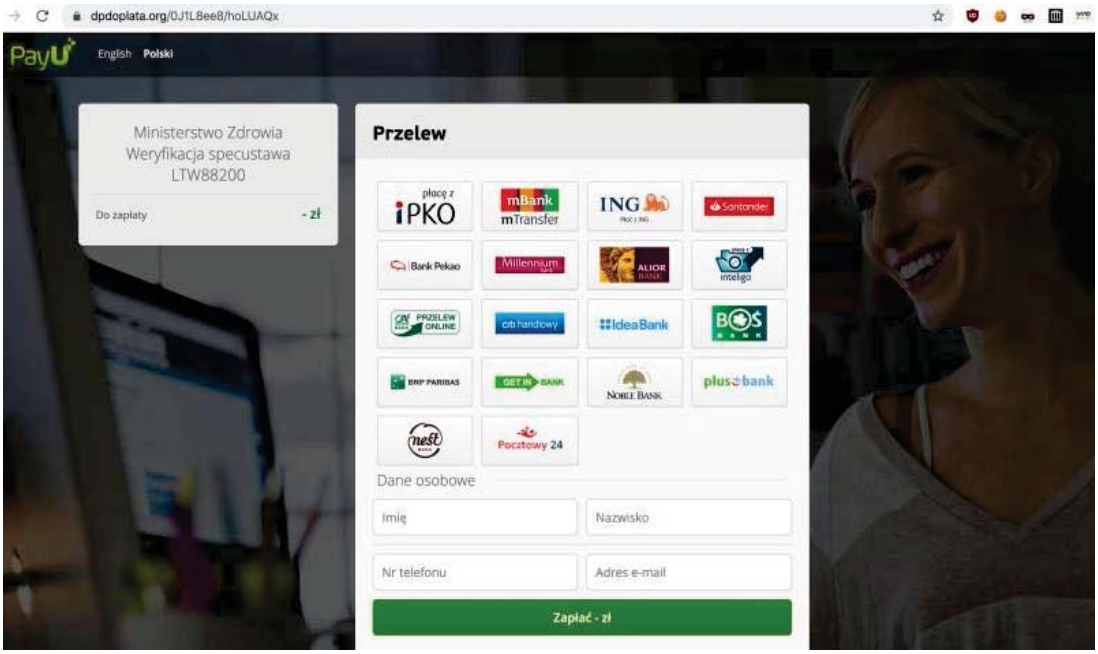
połowie 2020 roku częste były również dystrybucje wiadomości SMS z informacją o konieczności dopłaty do rachunku za energię elektryczną i podszyciem pod dostawców energii (głównie PGE, ENEA, Tauron).

W związku z pandemią, cyberprzestępcy zmienili wykorzystywany scenariusz. Już w dniu 13.3.2020 r., to jest dwa dni po ogłoszeniu rozporządzenia, którym ograniczono funkcjonowanie publicznych i niepublicznych jednostek oświaty z powodu COVID-19[149], dystrybuowane były wiadomości SMS o treści *„Informujemy, że zgodnie ze specustawą dotycząca koronawirusa Państwa środki na rachunku bankowym zostają przekazane do rezerw krajowych Narodowego Banku Polskiego. Zaloguj się aby zatrzymać 1000 PLN"* oraz *„Zgodnie ze specustawą dotyczącą koronawirusa wszyscy obywatele RP będą szczepieni. Z refundacją koszt wynosi 70 PLN. Opłać, aby uniknąć kolejek"*.



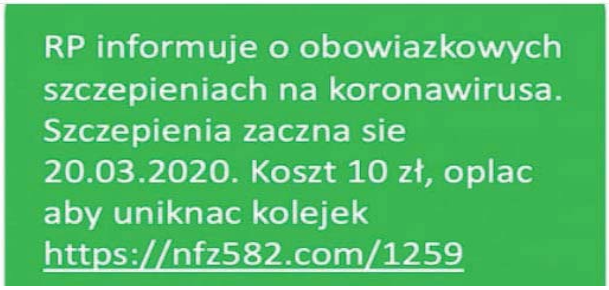
Rys. 1. Przykładowe wiadomości SMS wysyłane do pokrzywdzonych. Źródło: Materiały własne.

[149] Rozporządzenie Ministra Edukacji Narodowej z dnia 11 marca 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. poz. 410 z późn. zm.).



Rys. 2. Strona internetowa podszywająca się pod stronę PayU S.A. Źródło: Materiały własne.

W obu atakach sprawcy wykorzystali nazwę domenową *https://dpdoplata.org* zarejestrowaną wcześniej w celu dystrybucji wiadomości SMS z prośbą o dopłatę do przesyłki. Scenariusz oparty na obowiązkowym szczepieniu na COVID-19 zastosowano również w ataku, w którym wykorzystano nazwę domenową podszywającą się pod Narodowy Fundusz Zdrowia (https://nfz582.com/1259).



Rys. 3. Przykładowa wiadomość SMS informująca o szczepieniu na COVID-19. Źródło: Materiały własne.

Ponadto sprawcy wysyłali wiadomości SMS o treści: *„Ministerstwo Zdrowia: Dla każdego obywatela przysługuje wsparcie żywieniowe w związku z epidemia Koronawirusa. Zapisz sie na https://mzgov[.]net."* Hiperłącze z wiadomości SMS prowadziło do fałszywej strony *https://mzgov[.]net*, na której wyłudzano login i hasło do bankowości elektronicznej nakłaniając do zalogowania się do Elektronicznej Platformy Usług Administracji Publicznej (ePUAP).

Rys.4. Strona internetowa podszywająca się pod stronę Ministerstwa Zdrowia. Źródło: Materiały własne.

W dniu 27.03.2020 roku sprawcy dystrybuowali informację o zaległości wobec Urzędu Skarbowego, która uniemożliwia skorzystanie z tzw. tarczy antykryzysowej. Również ten atak uwzględniał bieżącą sytuację – w dniu 26.03.2020 r. do Sejmu wpłynął druk nr 299 stanowiący rządowy projekt ustawy o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw[150]. Ze strony

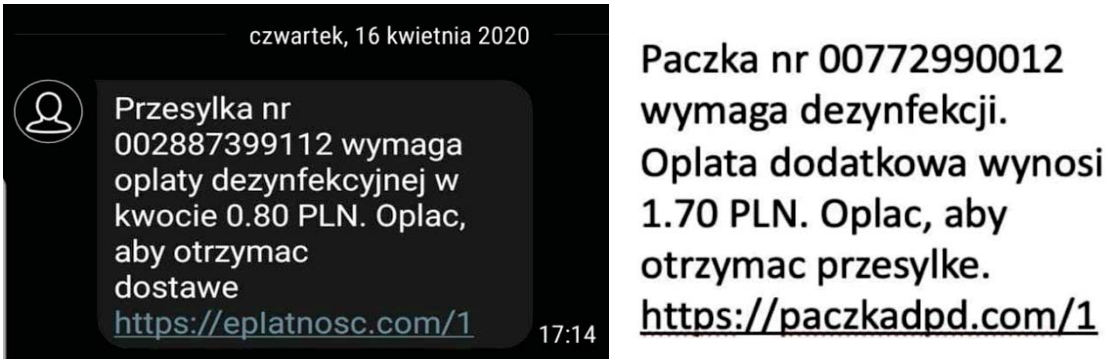
[150] Rządowy projekt ustawy o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych

internetowej podszywającej się pod stronę gov.pl o adresie *https://gov-24.com* następowało przekierowanie na stronę podszywającą się pod stronę PayU S.A. o adresie *https://paqu24.com.*

Rys. 5. Strona internetowa podszywająca się pod stronę gov.pl. Źródło: Materiały własne.

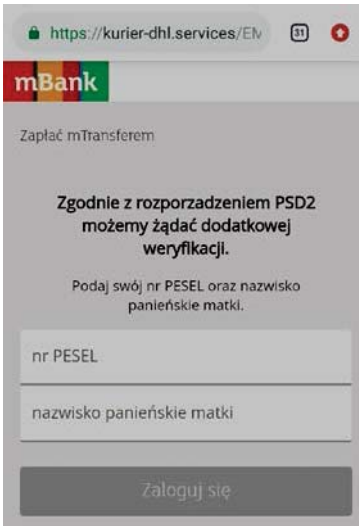
W kwietniu i maju 2020 r. do wyłudzenia danych do logowania do bankowości elektronicznej oraz kodów autoryzacyjnych najczęściej dochodziło w scenariuszach, w których sprawcy podszywali się pod przedsiębiorców świadczących usługi przewozowe, spedycyjne lub pocztowe usługi kurierskie i wysyłali wiadomości SMS z informacją o konieczności dopłacenia do dezynfekcji przesyłki (przykładowe nazwy domenowe: *eplatnosc.com*, *paczkadpd.com*).

oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw, druk nr 299 z dnia 26.3.2020, http://sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=299.



Rys. 6. Przykładowe wiadomość SMS informujące o dopłacie do dezynfekcji przesyłki. Źródło: Materiały własne.

Ofiara, która korzystając z hiperłącza przesłanego, np. w wiadomości SMS wejdzie na stronę podszywającą się pod pośrednika płatności dokonuje wyboru banku oraz najczęściej (w wariancie podszycia się pod stronę PayU S.A.) nakłaniana jest do podania danych osobowych – imienia i nazwiska, numeru telefonu i adresu e-mail. Po wyborze banku przez ofiarę na stronie podszywającej się pod agenta rozliczeniowego, jest ona przekierowywana na stronę podszywającą się pod bank. Czasem na stronie banku ofiara jest nakłaniana do podania nr PESEL oraz nazwiska panieńskiego matki, co następnie umożliwi sprawcom dostęp do rachunku ofiary przez infolinię.



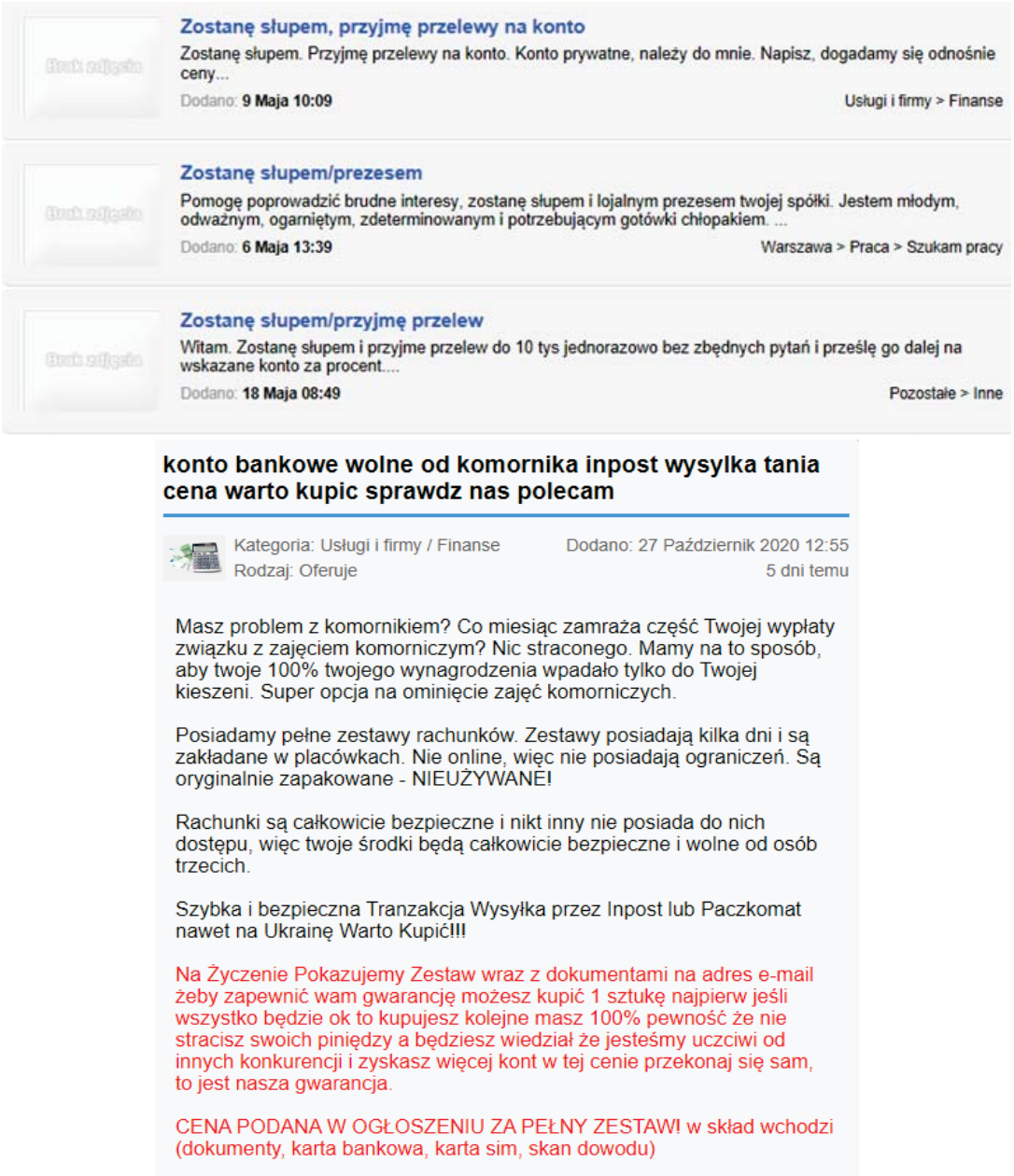
Rys. 7. Przykładowa strona podszywająca się pod bankowość elektroniczną wyłudzająca dane osobowe. Źródło: Materiały własne.

Jeśli ofiara na fikcyjnej stronie banku poda login i hasło do bankowości elektronicznej, sprawcy w tym samym czasie, przy pomocy tych danych, logują się na konto ofiary i dodają tzw. „zaufanego odbiorcę", którym jest rachunek tzw. słupa wykorzystywany w procederze prania pieniędzy. Ponieważ atak jest obsługiwany w czasie rzeczywistym, po zalogowaniu się przez sprawców do bankowości elektronicznej ofiary, otrzymuje ona wiadomość SMS o poprawnym logowaniu – co tylko utwierdza ją w przekonaniu, że znajduje się na stronie bankowości elektronicznej. Dla zdefiniowania odbiory zaufanego i wytransferowania środków z rachunku ofiary sprawcy potrzebują przesyłanego SMSem kodu autoryzacyjnego, dlatego też na fałszywej stronie obsługiwanej przez przestępców pojawia się formularz płatności online z polem do wpisania kodu jednorazowego, w celu potwierdzenia płatności, np. za szczepienie czy dopłatę do dezynfekcji przesyłki. Jeżeli ofiara nie przeczyta uważnie wiadomości SMS i poda kod na fałszywej stronie bankowości, atakujący odczytuje kod w panelu zarządzającym „fałszywą bramką płatności" i potwierdza dodanie nowego odbiorcy zaufanego. Po zdefiniowaniu odbiorcy zaufanego możliwe jest wytransferowanie środków z rachunku pokrzywdzonego bez konieczności potwierdzania kodami autoryzacyjnymi kolejnych transakcji.

Z uwagi na to, że występuje kilka wariantów tzw. „fałszywej bramki płatności", a przestępnym procederem zajmują się różne grupy występują różnice w sposobie działania sprawców. Opisany powyżej schemat działania podlega więc modyfikacjom, np. bezpośrednio z rachunku pokrzywdzonego środki transferowane są na giełdy kryptowalut lub na inne rachunki bankowe bez definiowania odbiorcy zaufanego. Jedna z pierwszych obserwowanych już w maju 2017 roku fałszywych bramek płatności została wystawiona na sprzedaż 20.12.2017 roku na forum Cebulka. Aktualnie na forum Cebulka regularnie pojawiają się ogłoszenia dotyczące zatrudnienia tzw. „bramkarzy", czyli osób, które obsługiwałaby fałszywą „bramkę płatności", co wskazuje, że jest ona dostępna w modelu CaaS. Z uwagi na konieczność obsługi ofiar w czasie rzeczywistym atak ten zakłada współdziałanie i podział ról obejmujących: rejestrację nazw domenowych i przygotowanie strony podszywającej się pod agentów rozliczeniowych i banki, przygotowanie wiadomości SMS i ich wysyłkę na pozyskane wcześniej numery telefonów, logowanie do bankowości elektronicznej przy pomocy loginów i haseł podanych przez ofiary na fałszywej stronie internetowej, zdefiniowanie odbiorcy zaufanego (zwykle jest to pozyskany wcześniej rachunek służący do prania pieniędzy na dane tzw. „słupa") przy pomocy kodów SMS jakie pokrzywdzeni podają na stronie internetowej podszywającej się pod bank, zlecanie przelewów z rachunków pokrzywdzonych na rachunki służące do prania pieniędzy, dokonanie transferów z rachunków służących

do prania pieniędzy na giełdy lub kantory wymiany kryptowalut, bądź też wygenerowanie kodów BLIK, na podstawie których osoby zajmujące się praniem pieniędzy dokonają wypłat w bankomatach, a następnie wpłat na ustalone dane tzw. „słupa" (np. przy wykorzystaniu usług Poczty Polskiej), rachunki bankowe (we wpłatomatach) lub adresy kryptowaluty (w bitomatach). Obsługą fałszywej bramki zajmuje się osoba określana jako „bramkarz" – przy czym może być to nie tylko osoba dysponująca własną „bramką", ale również osoba która odpłatnie – za udział w zysku – uzyskała dostęp do bramki udostępnianej przez inną osobę. Wysyłaniem wcześniej przygotowanych wiadomości SMS zajmują się tzw. „telefoniści". Procederem prania pieniędzy – tzn. przygotowaniem rachunków, na który transferowane są środki, generowaniem kodów BLIK, zarządzaniem wypłatami środków w bankomatach, ich podziałem i przekazaniem do poszczególnych osób zaangażowanych w przestępny proceder zajmuje się osoba o tzw. randze „bankiera".

Przestępczy proceder znacząco ułatwia dostępność rachunków bankowych, które można wykorzystać do transferowania środków. Za niewielkimi opłatami osoby uzależnione od alkoholu lub środków odurzających, bezrobotne i będące w trudnej sytuacji finansowej zakładają od kilku do kilkudziesięciu rachunków bankowych w różnych bankach oraz stają się abonentami przedpłaconych usług telekomunikacyjnych – to jest kupują i rejestrują zestawy startowe z kartą SIM, wykorzystywane do obsługi sprzedawanych rachunków bankowych. Cena sprzedawanego pakietu tj. rachunku bankowego wraz z zarejestrowaną kartą SIM oraz zdjęcia „selfie" z dowodem osobistym wynosi od 100 do 1 000 zł. Dodatkowo na dane osób sprzedających rachunki tworzone są konta na giełdach kryptowalut lub kantorach internetowych. Osoby kupujące rachunki bezpośrednio od tzw. „słupów" zwykle sprzedają je dalej przy wykorzystaniu stron ogłoszeniowych lub forów w DarkWeb. Sprzedaż rachunku polega zazwyczaj na przekazaniu danych do logowania do rachunku (loginu i hasła), karty bankomatowej oraz zarejestrowanej karty SIM, na którą będą przesyłane kody autoryzacyjne z banku.



Rys. 8. Przykładowe ogłoszenia dotyczące sprzedaży rachunków bankowych dostępne na popularnych stronach z ogłoszeniami. Źródło: Materiały własne.

Poza osobami świadomie sprzedającymi swoje rachunki często do transferów z rachunków pokrzywdzonych wykorzystywane są również rachunki bankowe osób, które wzięły udział w fikcyjnej rekrutacji i są przekonane o tym, że pracują zdalnie, np. na rzecz giełdy kryptowalut lub agenta rozliczeniowego[151]. Rekrutowane osoby są przekonywane, że praca jest legalna i że zostanie z nimi podpisana umowa. Podczas tzw. szkolenia osoby te muszą udowodnić, że umieją wykonywać elektronicznie operacje na własnym rachunku bankowym. W ramach szkolenia na własny rachunek bankowy otrzymują przelewy „testowe", następnie mają wygenerować kody BLIK. Kody BLIK przekazywane są następnie innej osobie biorącej udział w fikcyjnym szkoleniu, która wypłaca pieniądze w bankomacie.

Relatywnie łatwo również osobom zarządzającym przestępnym procederem rekrutować osoby, które zajmują się wypłatami środków w bankomatach i wpłacaniem ich w placówkach Poczty Polskiej, we wpłatomatach czy bitomatach. Osoby te co do zasady są świadome co do tego, że środki przez nie wypłacane pochodzą z przestępstwa i ich działanie wypełnia znamiona czynu z art. 299 § 1 kk, tj. przestępstwa prania pieniędzy. Wśród osób wypłacających bywają jednak również osoby, które wzięły udział w fikcyjnej rekrutacji i są przekonane o legalnym pochodzeniu środków.

[151] Szerzej o tym sposobie pozyskiwania rachunków: https://zaufanatrzeciastrona.pl/post/facebook-blik-gadu-gadu-bitbay-i-stado-nieswiadomych-mulow/ (dostęp 30.10.2020 r.).

szukam bankiera przez greenyogi	0	2020-09-27 PM przez greenyogi
Poszukiwany specjalista od leasingow, factoringow, dotacji itp przez roooj	0	2020-09-26 PM przez roooj
Szukam do pracy przez amirreihan	6	2020-09-26 AM przez casper666
KOSZ przez greenyogi	0	2020-09-23 PM przez greenyogi
Szukam współpracownika/partnera, AKTUALNE 20K+ PLN miesiecznie przez carterjimmy	0	2020-09-21 PM przez carterjimmy
Szukam bankiera z bramką przez unibelt	0	2020-09-21 PM przez unibelt
Zlece zalozenie konta na wskazane dane przez roooj	2	2020-09-19 PM przez roooj
Szukam wspolnika/programisty darkwebowego przez roooj	1	2020-09-19 PM przez Ricky_Lafleur
W poszukiwaniu ogarniętego bankiera przez Kazimierz Lux	0	2020-09-18 PM przez Kazimierz Lux
Spreader/botmaster. przez Ricky_Lafleur	0	2020-09-17 PM przez Ricky_Lafleur
Szukam telefonisty przez Conti44	0	2020-09-16 PM przez Conti44
Szukam współpracowników przez Kubus	0	2020-09-10 AM przez Kubus

Rys. 9. Przykładowe ogłoszenia na forum Cebulka dotyczące tzw. „fałszywej bramki płatności". Źródło: Materiały własne (dostęp 30.10.2020 r.).

Sprawców zarządzających „fałszywymi bramkami płatności" cechuje przestrzeganie zasad bezpieczeństwa operacyjnego - w tym w szczególności dbałość o zachowanie anonimowości. Współdziałające ze sobą osoby nie znają swoich danych osobowych, wizerunku, lokalizacji, nie wymieniają między sobą informacji dotyczących życia prywatnego. Komunikacja odbywa się z wykorzystaniem szyfrowanych komunikatorów (głównie jabber i Telegram). Ukrywają swoją tożsamość m.in. wykorzystując sieci TOR, VPN lub proxy. Aby uniknąć objęcia konta służącego do prania pieniędzy monitoringiem lub blokadą sprawcy włamań do bankowości elektronicznej łączą wykorzystanie sieci TOR z wykorzystaniem wcześniej przejętych urządzeń (botów), które wykorzystywane są jako proxy.

Dzięki stosowanemu podziałowi ról, osobami najbardziej narażonymi na ustalenie i zatrzymanie przez organy ścigania jest kolejno: osoba, która udostępniła swój rachunek bankowych („słup"), osoby, które kupują rachunki bankowe i następnie je dalej sprzedają, osoby dokonujące wypłat środków w bankomatach oraz osoby o randze tzw. „bankiera". Ponieważ

bez zapewnienia struktur do bezpiecznego transferowania środków przestępczy proceder nie byłby możliwy, należy eliminować poszczególne łańcuchy wykorzystane do prania pieniędzy. Podążanie za transferami pieniężnymi jest również najskuteczniejszą z metod ustalenia tożsamości osób stojących najwyżej w hierarchii grupy i nią kierujących. Aby ograniczyć dostępność rachunków służących do prania pieniędzy oraz transfery środków z rachunków pokrzywdzonych niezbędne jest podjęcie działań usprawniających wymianę informacji przez banki i instytucje finansowe. Niewątpliwą wymagającą monitoringu anomalią mogącą świadczyć o przygotowaniu do prania pieniędzy jest otworzenie jednego dnia lub w krótkich odstępach czasu wielu rachunków bankowych, w kilku lub kilkunastu bankach przez tą samą osobę. W sytuacji dokonania blokady rachunku wobec podejrzenia prania pieniędzy powinna nastąpić weryfikacja i objęcie monitoringiem również innych rachunków prowadzonych na dane tej samej osoby. Aby było to możliwe banki powinny między sobą przekazywać dane osób i rachunków wykorzystywanych do prania pieniędzy. Brak sprawnej wymiany informacji pomiędzy bankami sprawia, że pomimo dokonania przez bank blokady jednego rachunku, kolejne rachunki tego klienta w innych bankach są wykorzystywane do prania pieniędzy. Zatrzymanie i pociągnięcie do odpowiedzialności karnej sprawców prania pieniędzy lub przestępstwa bazowego wymaga również niezwłocznego przekazywania organom ściągania przez banki danych dotyczących rachunków i transakcji wraz z zawiadomieniem o podejrzeniu popełnienia przestępstwa lub w odpowiedzi na postanowienie o zwolnieniu z tajemnicy. Aktualnie nadmierny czas oczekiwania na dane z banku najczęściej prowadzi do niemożliwości zabezpieczenia nagrań z bankomatów lub monitoringu miejskiego z czasu i miejsca wypłat.

Ataki łączące dezinformację z przestępstwami przeciwko ochronie informacji i mieniu

Pandemia COVID-19 dała również początek dezinformacji związanej z epidemią, jej przyczynami, leczeniem czy zagrożeniami jakie powoduje. W mediach i literaturze coraz częściej analizowane jest zjawisko infodemii[152]. Użytkownicy Internetu przesyceni różnymi komunikatami oraz sensacyjnymi doniesieniami, przy jednoczesnym braku wiarygodnych źródeł

[152] Md Saiful Islam, Tonmoy Sarkar, Sazzad Hossain Khan, et al., COVID-19–Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis, The American Journal of Tropical Medicine and Hygiene 2020, DOI: https://doi.org/10.4269/ajtmh.20-0812, Catching the virus cybercrime, disinformation and the COVID-19 pandemic, Europol 2020, https://www.europol.europa.eu/newsroom/news/catching-virus (dostęp 24.10.2020 r.).

informacji stają się podatni na dezinformację i fałszywe wiadomości. Analiza zjawiska dezinformacji nie jest objęta artykułem z uwagi na inny cel i zakres badań. Przywołanie tego problemu niezbędne jest jednak z uwagi na widoczny związek z jedną ze strategii wykorzystywanych przez sprawców odpowiedzialnych do kampanie phishingowe, w których wyłudzane są dane dostępowe do portali społecznościowych. Drugim najpopularniejszym w Polsce scenariuszem ataku, w którym sprawcy wykorzystują COVID-19 jest atak polegający, w pierwszej fazie na uzyskaniu bez uprawnienia danych do logowania do portali społecznościowych, zaś w drugiej fazie – wykorzystaniu przejętych kont do przejmowania kont innych osób oraz dokonywania oszustw.

Cyberprzestępcy chcąc przyciągnąć na fałszywą stronę logowania użytkowników w pierwszym etapie tworzą stronę internetową podszywającą się pod portal informacyjny. Na stronie tej zamieszczana jest sensacyjna wiadomość dotycząca porwania (najczęściej dziecka), zgwałcenia, zuchwałej kradzieży, wypadku samochodowego. Pod opisem rzekomego zdarzenia znajduje się informacja o tym, że dostępne jest nagranie z monitoringu. Wraz z wprowadzaniem ograniczeń związanych z pandemią COVID-19 dotychczas wykorzystywane scenariusze socjotechniczne zostały zastąpione tworzonymi przez sprawców stronami internetowymi zawierającymi sensacyjne informacje na temat pandemii. Przykładowe nagłówki „*Wypowiedź doktora z jednego z warszawskich szpitali na temat namnażającej się liczby zakażonych w Polsce”*, „*Nowe fakty na temat koronawirusa [wideo]*”, „*Porwanie dziecka ze szpitala zakaźnego. [wideo]*”. Przykładowe domeny wykorzystywane w tym scenariuszu ataku: *efakty-koronawirus24.pl*, *fakty-koronawirus24.pl*, *koronainfo24.eu*, *koronanews.hekko24.pl*, *koronawirus-info24.pl*, *koronawirus.hekko24.pl*.

Rys. 10. Przykładowe strony portali informacyjnych służące do wyłudzenia danych do logowania do portali społecznościowych. Źródło: Materiały własne.

Z uwagi na to, że materiał ma być drastyczny i przeznaczony jedynie dla osób pełnoletnich, aby wyświetlić film, konieczne jest zweryfikowanie wieku. Weryfikacja ma zostać dokonana przez logowanie do portalu społecznościowego (np. Facebook.com). Po kliknięciu w ikonkę „zaloguj" ofiara jest przenoszona na stronę podszywającą się pod panel logowania. Po przejęciu danych ofiary, jej konto jest wykorzystywane między innymi do przejmowania

kolejnych kont przez wysyłanie linków do stron wyłudzających dane do logowania, publikowania fikcyjnych informacji o rekrutacji do pracy (w celu nieuprawnionego pozyskania danych osobowych lub pozyskania osób biorących udział w praniu pieniędzy pochodzących z przestępstwa) oraz do dokonywania oszustw.

Najczęstszy scenariusz oszustwa, w którym wykorzystuje się przejęte konta na portalach społecznościowych zakłada wysłanie do osób z kręgu znajomych takiej osoby prośby o pożyczenie niewielkiej kwoty pieniędzy lub opłacenie zamówienia. W tym celu ofiara jest proszona o wygenerowanie i przekazanie kodu BLIK, który umożliwi sprawcy wypłacanie środków w dowolnym bankomacie. Z uwagi na to, że wygenerowany kod BLIK należy wykorzystać w 2 minuty, sprawcy bądź osoby z nimi współpracujące, w czasie gdy przy pomocy komunikatora Messenger proszą o podanie kodu BLIK czekają już przy bankomacie. Czasem kod BLIK nie jest wykorzystywany do wypłaty środków w bankomacie lecz do opłacenia zamówienia zlecanego przez sprawcę (np. zakupów dokonywanych na portalach aukcyjnych). Osoba, która generuje kod BLIK, a następnie autoryzuje transakcję w aplikacji jest przekonana, że przekazuje pieniądze osobie zaufanej, która dokona zwrotu środków.

W scenariuszu tym sprawcy w celu osiągnięcia korzyści majątkowej doprowadzają do niekorzystanego rozporządzenia mieniem osobę, która generuje kod BLIK i autoryzuje transakcję w aplikacji bankowej poprzez wprowadzenie jej w błąd co do tożsamości osoby proszącej o pożyczenie pieniędzy oraz zwrotu środków w wyznaczonym terminie. Z uwagi na ukształtowanie znamion czynu z art. 190a § 2 kk jako przestępstwa, które może być popełnione wyłącznie w zamiarze bezpośrednim kierunkowym (*dolus directus coloratus*) wyrządzenia szkody osobie, pod którą się podszyto, sprawca co do zasady nie wypełni znamion przestępstwa kradzieży tożsamości, albowiem przejęcie konta na portalu społecznościowym jest jedynie środkiem do innego celu – to jest doprowadzenia innych osób do niekorzystnego rozporządzenia mieniem[153].

Za pozytywny krok w kierunku ochrony użytkowników Internetu przed opisanymi powyżej dwoma najczęstszymi scenariuszami ataków uznać należy porozumienie z 23.03.2020 r. o utworzeniu listy ostrzeżeń odnoszącej się do domen internetowych, które służą do wyłudzeń danych i środków finansowych, którego sygnatariuszami są MC, NASK - PIB, Orange Polska S.A., Polkomtel Sp. z o.o., P4 Sp. z o.o. oraz T-Mobile Polska S.A.

---

[153] Więcej: A. Gryszczyńska, Kradzieże tożsamości w sprawach z zakresu cyberprzestępczości, [w:] Rocznik Bezpieczeństwa Morskiego, Przestępczość Teleinformatyczna 2019, red. J. Kosiński, G. Krasnodębski, Gdynia 2020, s. 223-225.

W dniu 1.11.2020 r. na liście tej znajdowało się już 5 063 nazw domenowych, w tym 1 720 nazw z domeny .pl. Z uwagi na to, że lista ostrzeżeń jest rozwiązaniem prowadzonym zgodnie z § 1 pkt 1 porozumienia jedynie w okresach stanów nadzwyczajnych, stanu epidemii lub stanu zagrożenia epidemicznego należy rozważyć kontynuację prowadzenie listy ostrzeżeń również po zakończeniu pandemii, przy jednoczesnym oparciu dalszego prowadzenia listy i blokowaniu dostępu do stron wyłudzających dane o przepisy ustawowe.

Analiza listy ostrzeżeń pozwala na wyselekcjonowanie nazw domenowych wykorzystywanych przez sprawców odpowiedzialnych za „fałszywe bramki płatności" oraz sprawców tworzących strony z sensacyjnymi wiadomościami i przejmujących dane do logowania do portali społecznościowych. Dla pierwszej kategorii sprawców charakterystyczne ciągi znaków to: pay (197) – w tym dotpay (77), payu (37); poczta (169); kurier (128); inpost (107); paczka (91); dhl (67), dpd (54). Ciągi znaków charakterystyczne dla stron z sensacyjnymi wiadomościami to fakt (335), porwani (203), gwałt (156), news (107).

Z uwagi na to, że w części z omówionych powyżej ataków wykorzystano nazwy domenowe z domeny .pl lub domeny gdzie rejestratorami (pośrednikami) są podmioty mające siedzibę na terytorium Polski rozważyć należy dokonanie zmian w procesie pośrednictwa w rejestracji domen i nałożyć na rejestratorów obowiązki związane z weryfikacją tożsamości abonentów. Aktualnie rejestratorzy opierają się o dane deklarowane przez rejestrujących, co prowadzi do sytuacji w której cyberprzestępcy na potrzeby rejestracji domeny podają dane innych podmiotów (zarówno osób fizycznych jak i podmiotów prowadzących działalność gospodarczą) lub kreują nową tożsamość.

Podsumowanie

Przyspieszone przez tzw. *lockdown* wywołany pandemią COVID-19 procesy informatyzacji podmiotów publicznych i prywatnych unaoczniły problemy cyberbezpieczeństwa. Nagły wzrost aktywności on-line użytkowników jest nierozerwalnie sprzężony ze wzrostem aktywności cyberprzestępców czy grup zajmujących się dezinformacją. Do nowej rzeczywistości wśród różnych kategorii sprawców przestępstw najszybciej dostosowali się cyberprzestępcy, choć pandemia wpłynęła również na rynki dystrybucji narkotyków[154] czy na produkcję materiałów określanych jako CSAM[155].

[154] EU Drug Markets Impact of COVID-19, Europol 2020, https://www.europol.europa.eu/publications-documents/eu-drug-markets-impact-of-covid-19.

[155] Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. Europol 2020. https://www.europol.europa.eu/publications-documents/exploiting-isolation-

Skuteczność ataków w dużej mierze jest pochodną wymuszenia przez pandemię COVID-19 zdalnej pracy i zdalnej komunikacji na tych użytkownikach, którzy wcześniej nie byli na to dostatecznie przygotowani i wyposażeni w odpowiedzenie narzędzia. Nawet ataki źle przygotowane kończą się powodzeniem sprawców, dlatego szczególne istotne jest ponoszenie świadomości użytkowników i ich odporności na aktualne zagrożenia.

Równolegle należy dążyć do redukcji czynników ułatwiających popełnienie cyberprzestępstw oraz zwiększenia skuteczności organów ścigania. Sprawcy poddanych analizie ataków pozostają najczęściej nieuchwytni z uwagi na stosowanie przez nich różnych metod ukrycia własnej tożsamości, korzystanie z anonimowych usług, płatności (np. w kryptowalucie), czy łatwo dostępnych w Polsce rachunków bankowych założonych na dane tzw. „słupów". Nowe cyberzagrożenia wyeksponowane przez pandemię powinny skłonić do dyskusji nad zmianami regulacji prawnej cyberbezpieczeństwa i przeciwdziałania cyberprzestępczości – w tym również weryfikacją tożsamości użytkowników e-usług i abonentów domen czy zakresem obowiązków podmiotów świadczących usługi drogą elektroniczną.

Wykaz cytowanych publikacji

1. Buchanan B., The Legend of Sophistication in Cyber Operations, https://www.belfercenter.org/publication/legend-sophistication-cyber-operations, 2017.
2. Catching the virus cybercrime, disinformation and the COVID-19 pandemic, Europol 2020, https://www.europol.europa.eu/newsroom/news/catching-virus.
3. Check Point Blog 2020. Coronavirus update: not the type of CV you're looking for. https://blog.checkpoint.com/2020/06/04/coronavirus-update-not-the-type-of-cv-youre-looking-for/.
4. Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 10.9.2019 r, ZSPR.421.2.2019, https://uodo.gov.pl/decyzje/ZSPR.421.2.2019.
5. DePaula N., Sanjay G., A Sophistication Index for Evaluating Security Breaches, 11th Annual Symposium on Information Assurance, 2016, https://www.albany.edu/iasymposium/proceedings/2016/06_DePaula_Goel_ASIA2016.pdf.
6. EU Drug Markets Impact of COVID-19, Europol 2020, https://www.europol.europa.eu/publications-documents/eu-drug-markets-impact-of-covid-19.

offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic (dostęp: 12.8.2020), IOCTA 2020.

7. Exploiting isolation: Offenders and victims of online child sexual abuse during the COVID-19 pandemic. Europol 2020, https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic.
8. Gryszczyńska A., Kradzieże tożsamości w sprawach z zakresu cyberprzestępczości, [w:] Rocznik Bezpieczeństwa Morskiego, Przestępczość Teleinformatyczna 2019, red. J. Kosiński, G. Krasnodębski, Gdynia 2020.
9. H2 REPORT 2020. Email Fraud & Identity Deception Trends. Global Insights from the Agari Identity Graph. 2020. https://www.agari.com/cyber-intelligence-research/e-books/agari-h2-2020-email-fraud-report.pdf.
10. https://zaufanatrzeciastrona.pl/post/facebook-blik-gadu-gadu-bitbay-i-stado-nieswiadomych-mulow/.
11. https://zaufanatrzeciastrona.pl/post/jak-zlodzieje-chcieli-morele-net-szantazowac-z-nasza-pomoca/.
12. IC3 Internet Crime Report 2019, https://pdf.ic3.gov/2019_IC3Report.pdf.
13. Incident Classification/ Incident Taxonomy according to eCSIRT.net, International Version Don Stikvoort, 11 Jan – 19 Dec 2012 (version mkVI of 31 March 2015). https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf.
14. Internet Organised Crime Threat Assessment (IOCTA) 2020, Europol, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.
15. Kodeks karny z dnia 6 czerwca 1997 r., t.j. Dz.U. z 2020 r. poz. 1444
16. Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2018, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf.
17. Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska 2019, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.
18. Md Saiful Islam, Tonmoy Sarkar, Sazzad Hossain Khan, et al., COVID-19 – Related Infodemic and Its Impact on Public Health: A Global Social Media Analysis, The American Journal of Tropical Medicine and Hygiene 2020, DOI: https://doi.org/10.4269/ajtmh.20-0812.
19. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku, CSIRT GOV, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html.

20. Rozporządzenie Ministra Edukacji Narodowej z dnia 11 marca 2020 r. w sprawie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19 (Dz. U. poz. 410 z późn. zm.).
21. Rządowy projekt ustawy o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw, druk nr 299 z dnia 26.3.2020, http://sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=299.
22. Socjotechnika: praktyczne zastosowania socjologii, red. A. Podgórecki, Warszawa 1968
23. Wyrok WSA w Warszawie z 3.9.2020 r., II SA/Wa 2559/19.

ABSTRACT

USE OF COVID-19 IN SOCIAL ENGINEERING ATTACKS

Summary: The COVID-19 pandemic has considerably affected the methods of working, learning or carrying out public tasks. The widespread use of information and commu-nication technologies for remote work or education has exposed problems in the area of cybersecurity. The COVID-19 pandemic has become an opportunity for cyber-criminals to increase the effectiveness of attacks with the use of social engineering techniques, both in Poland and around the world. The existing attack scenarios have been adapted to the current situation involving the pandemic. Undoubtedly, the most frequent incidents in Poland basing on the fear of the disease executed by Polish cy-bercriminals are acts aiming at monetisation – fraud, Internet fraud and theft of mon-ey in a bank account. A great deal of activity has been reported with regard to groups that set up fake sites which mimic the websites of acquirers and banks. Numerous crimes have been committed also by cybercriminals who take hold of data necessary to log on to social media.

The new threats inspire debate on the anonymous use of electronic services and the methods of verifying the identity of people who wish to use them. The issue is inseparably linked to the ever more frequent practice of identity theft. Another problem, both legal and technical, is blocking Internet domains that serve to obtain data and money by deception.

This chapter discusses the most frequent scenarios of social engineering attacks in Poland carried out for the purpose of financial gains. The analysis covers the fac-tors which help the criminals execute an attack successfully and render it difficult to ascertain their identity.

Keywords: Cybersecurity, cybercrime, social engineering, phishing, identity theft.

ROZDZIAŁ 10

DZIAŁANIA W CYBERPRZESTRZENI JAKO PRZESŁANKA WPROWADZENIA STANU WOJENNEGO W POLSCE

dr Malwina Ewa KOŁODZIEJCZAK [156]

STRESZCZENIE: Rozdział dotyczy próby wskazania działań w cyberprzestrzeni, które mogłyby zostać uznane za przesłanki umożliwiające wprowadzenie stanu wojennego, stanu wyjątkowego, jak i stanu klęski żywiołowej. W rozdziale przedstawione zostały także najważniejsze akty prawne związane z cyberprzestrzenią, a także dokumenty strategiczne i analizy odnoszące się do tego zagadnienia. Biorąc pod uwagę trudności z definicjami i procedurami, mimo wdrożonego systemu cyberbezpieczeństwa, przy braku metodyki szacowania ryzyka, wskazanie takich działań w cyberprzestrzeni, które mogłyby zostać uznane za przesłanki do wprowadzenia stanu wojennego jest prawdopodobnie niemożliwe.

SŁOWA KLUCZOWE: cyberprzestrzeń, działania w cyberprzestrzeni, stan wojenny, stany nadzwyczajne.

Stany nadzwyczajne, zgodnie z *Konstytucją RP* wprowadzić można w określonych sytuacjach, gdy zwykłe środki konstytucyjne są niewystarczające. *Konstytucja RP* zapewniła trzy stany nadzwyczajne: stan wojenny, stan wyjątkowy i stan klęski żywiołowej. Mimo,

[156] Adiunkt, Instytut Bezpieczeństwa Państwa, Akademia Sztuki Wojennej; m.kolodziejczak@akademia.mil.pl, ORCID: 0000-0002-2624-4009.

iż zarówno akt ten, jak i odrębne ustawy[157], regulujące każdy ze stanów nadzwyczajnych szczegółowo je omawiają, nadal pojawiają się trudności w zakresie interpretacji prawnej, czy – co istotne – określenia i przyporządkowania poszczególnych przypadków odpowiedniemu stanowi.

Jedną z wartych szerszej analizy przesłanek, umożliwiających wprowadzenie każdego z trzech stanów nadzwyczajnych są działania w cyberprzestrzeni. W niniejszym rozdziale rozpatrzony zostanie stan wojenny. Toteż, problem główny zawarty został w pytaniu: Jaki obecnie jest stan regulacji dotyczących wprowadzenia stanu wojennego (na podstawie działań w cyberprzestrzeni)? Celem pracy jest charakterystyka i interpretacja przesłanki działania w cyberprzestrzeni oraz przepisów wprowadzających stan wojenny. Hipoteza stanowi przypuszczenie, że brak jest odpowiednich przepisów – z jednej strony pozwalających wskazać skalę i zakres działań w cyberprzestrzeni, pozwalających na uznanie ich za wystarczającą przesłankę do wprowadzenia stanu wojennego, a z drugiej – które umożliwiłyby w przejrzysty i płynny sposób wprowadzić stan wojenny. Jednak, przypuszczać można, że wyłonienie katalogu zamkniętego takich działań w cyberprzestrzeni jest niemożliwe.

1. Podstawy prawne

Zgodnie z art. 229 *Konstytucji RP,* stan wojenny można wprowadzić w razie zewnętrznego zagrożenia państwa, zbrojnej napaści na terytorium RP lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji. Ustawowa definicja została rozszerzona o możliwość wprowadzenia stanu wojennego w przypadku zewnętrznego zagrożenia spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni[158]. Zgodnie z art. 2 ust. 1a Ustawy z dnia 29 sierpnia 2002 r. o *stanie wojennym*

[157] Ustawa z dnia 18 kwietnia 2002 r. *o stanie klęski żywiołowej* (Dz.U. z 2017, poz. 1897), ustawa z dnia 21 czerwca 2002 r. o *stanie wyjątkowym* (Dz. U. z 2017, poz. 1928) oraz ustawa z dnia 29 sierpnia 2002 r. o *stanie wojennym i kompetencjach Naczelnego Dowódcy Sił Zbrojnych oraz jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2017, poz. 1932).

[158] Ustawa z dnia 29 sierpnia 2002 r. o *stanie wojennym...* art. 2 ust. 1 „W razie zewnętrznego zagrożenia państwa, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, zbrojnej napaści na terytorium Rzeczypospolitej Polskiej lub gdy z umowy międzynarodowej wynika zobowiązanie do wspólnej obrony przeciwko agresji, Prezydent Rzeczypospolitej Polskiej może, na wniosek Rady Ministrów, wprowadzić stan wojenny na części albo na całym terytorium państwa".

i kompetencjach Naczelnego Dowódcy... zagrożeniami zewnętrznymi dla państwa są „celowe działania, godzące w niepodległość, niepodzielność terytorium, ważny interes gospodarczy Rzeczypospolitej Polskiej lub zmierzające do uniemożliwienia albo poważnego zakłócenia normalnego funkcjonowania państwa, podejmowane przez zewnętrzne w stosunku do niej podmioty". Definicja ta przedstawia najważniejsze przesłanki i szczegółowo określa zewnętrzne zagrożenie. Wydaje się jednak, że jest to przykład zbyt szczegółowego zdefiniowania, gdyż zawężono możliwość wprowadzenia stanu wojennego tylko do zewnętrznego zagrożenia spowodowanego przez inne podmioty. Należy zastanowić się, czy stan ten „zarezerwowany" został jedynie dla zagrożeń *stricte* wojennych, pochodzących od innego państwa? Być może zatem, mimo iż zaistniałyby działania terrorystyczne czy też działania w cyberprzestrzeni i byłyby one zinterpretowane jako przesłanka do wprowadzenia stanu wojennego, jego wprowadzenie z racji pochodzenia od niepaństwowego podmiotu czy niezidentyfikowanej jednostki, w powyższych sytuacjach mogłoby okazać się niemożliwe[159]?

Dodano także definicję legalną cyberprzestrzeni, która rozumiana jest w każdej ustawie o poszczególnych stanach nadzwyczajnych, jako przestrzeń przetwarzania i wymiany informacji, która tworzona jest przez systemy teleinformacyjne wraz z powiązaniami między nimi oraz relacjami z użytkownikami[160]. Z kolei, system informatyczny określony został Ustawą z dnia 17 lutego 2005 roku o *informatyzacji działalności podmiotów realizujących zadania publiczne*[161] i zgodnie z art. 3 pkt 3 jest to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, który zapewnia przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego[162]. Wreszcie, wraz z Ustawą

---

[159] M. Kołodziejczak, *Działania w cyberprzestrzeni jako przesłanka do wprowadzenia stanów nadzwyczajnych w Polsce,* [w:] *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne,* red. nauk. W. Kitler, J. Taczkowska-Olszewska, Wyd. TWO, FINA, Warszawa 2017, s. 170-182.

[160] Ustawa z dnia 29 sierpnia 2002 r. o *stanie wojennym...* art. 2 ust. 1b.

[161] Ustawa z dnia 17 lutego 2005 r. *informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2020, poz. 346).

[162] Z kolei, zgodnie z art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – *Prawo telekomunikacyjne* (Dz.U. z 2019, poz. 2460) przez sieci telekomunikacyjne rozumie się systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju.

z dnia 5 lipca 2018 r.[163] *o krajowym systemie cyberbezpieczeństwa* ustanowiona została definicja cyberbezpieczeństwa. Zgodnie z art. 2 pkt 4 jest to „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". W ustawie wskazano również zróżnicowanie stopnia incydentów, jednak bez ich powiązania ze stanami nadzwyczajnymi.

Po pierwsze jednak, żeby w ogóle rozważać wprowadzenie któregokolwiek ze stanów nadzwyczajnych, muszą zostać wyczerpane środki, które zapewniają konstytucyjne i ustawowe przepisy, na co wskazuje norma art. 228 ust. 1 *Konstytucji RP*: „W sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny: stan wojenny, stan wyjątkowy lub stan klęski żywiołowej". Dopiero potem należy brać pod uwagę zaistniałe przesłanki, które mogą skutkować wprowadzeniem któregoś stanu nadzwyczajnego.

Toteż, należy wskazać, że sytuacja, która nie zmienia albo nie zmierza do zmiany istoty organizacji (np. państwa) nie może być uznana, nie tylko za przesłankę do wprowadzenia któregoś ze stanów nadzwyczajnych, ale nawet za kryzys. Jednak, jeśli nie nastąpi odpowiednia i skuteczna reakcja, być może koniecznym stanie się ich wprowadzenie[164]. W przypadku, gdy istnieje konkretne zagrożenie, powstaje sytuacja kryzysowa. Wówczas należy uruchomić procedurę wynikającą z reagowania kryzysowego, a gdy i te mechanizmy zawiodą nastąpi kulminacyjny moment – kryzys. Kryzys jednak nie trwa długo, gdyż albo uda się opanować (względnie) zaistniałą sytuację i nastąpi powrót do normalnego funkcjonowania organizacji (np. państwa), albo sytuacja zaogni się i wówczas

---

[163] Ustawa z dnia 5 lipca 2018 r. o *krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2019, poz. 2020, 2248).

[164] Do czasu nowelizacji ustawy z 26 kwietnia 2007 r. *o zarządzaniu kryzysowym,* sytuacją kryzysową była „sytuacja będącą następstwem zagrożenia i prowadząca w konsekwencji do zerwania lub znacznego naruszenia więzów społecznych przy równoczesnym poważnym zakłóceniu w funkcjonowaniu instytucji publicznych, jednak w takim stopniu, że użyte środki niezbędne do zapewnienia lub przywrócenia bezpieczeństwa nie uzasadniają wprowadzenia żadnego ze stanów nadzwyczajnych, o których mowa w art. 228 ust. 1 Konstytucji Rzeczypospolitej Polskiej", art. 3 pkt 1, (Dz. U. z 2007, nr 89, poz. 590). Co interesujące, po ostatniej nowelizacji sytuację kryzysową rozumie się inaczej – jako „sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków", art. 3 pkt 1, (Dz. U. z 2017, poz. 209).

konieczne będzie wprowadzenie stanów nadzwyczajnych[165]. Należy jednak zauważyć, że brak szczegółowych i kompletnych procedur reagowania w sytuacjach kryzysowych na wypadek działań w cyberprzestrzeni[166].

Dopiero wówczas będzie można uznać, że znamiona wskazane w art. 228 ust. 1 *Konstytucji RP* zostały wypełnione łącznie, a mianowicie:

1. istnieje szczególne zagrożenie;
2. zwykłe środki konstytucyjne okazały się niewystarczające;
3. środki konstytucyjne okazały się niewystarczające, bo zostały sprawdzone, wykorzystane i wyczerpane, a nie ominięte.

Co więcej, stany nadzwyczajne muszą charakteryzować się określonymi zasadami: wyjątkowości, legalności, proporcjonalności, celowości, ochrony podstaw systemu prawnego i ochrony organów przedstawicielskich[167].

Gdy znamiona art. 228 ust. 1 zostały wypełnione, w przypadku działań w cyberprzestrzeni należy sprawdzić czy istnieją dalsze przesłanki pozwalające na wprowadzenie stanu wojennego określone w art. 229 *Konstytucji RP oraz* w art. 2 Ustawy z dnia 29 sierpnia 2002 r. o *stanie wojennym...*

2. Wprowadzenie stanu wojennego

Zakładając, że w przypadku celowych działań w przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne, które zostałyby dokonane przez inne państwo a działania te miałyby olbrzymi i negatywny wpływ na funkcjonowanie organów władzy i godziłyby w niepodległość, Rada Ministrów będzie wnioskowała do Prezydenta RP o wprowadzenie stanu wojennego. Wprowadzenie stanu wojennego ma związek z regulacjami wewnątrzkrajowymi i docelowo ma umożliwić zabezpieczenie, z jednej strony państwa, a z drugiej obywateli, przed zagrożeniami zewnętrznymi.

---

[165] Szerzej: M. Kołodziejczak, *Różnica pojęć: wojna, konflikt zbrojny, kryzys, zagrożenie występujących w naukach o bezpieczeństwie – ujęcie prawne*, [w:] *Zagrożenia bezpieczeństwa narodowego Rzeczypospolitej Polskiej w XXI wieku. Pojęcie, zakres i kwalifikacja,* pod. red. W. Sójka, M. Kołodziejczak, Wyd. AON, Warszawa 2016.

[166] Tak też stwierdzono w raporcie NIK, vide: *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP,* Informacja o wynikach kontroli, Najwyższa Izba Kontroli, KPB-4101-002-00/2014, Warszawa 2015, s. 9.

[167] Więcej: K. Prokop, *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej*, Wyd. Temida, Białystok 2005.

Stan wojenny wprowadza rozporządzeniem Prezydent RP na wniosek Rady Ministrów, na części bądź całym terytorium. Prezydent Rzeczypospolitej Polskiej niezwłocznie rozpatruje wniosek, a następnie wydaje rozporządzenie o wprowadzeniu stanu wojennego (albo postanawia o odmowie). Rozporządzenie Prezydent RP przedstawia Sejmowi w ciągu 48 godzin od jego podpisania[168]. W samej procedurze wprowadzania rozporządzenia jest kilka niewiadomych, które sprowadzają się do podstawowego pytania: co w przypadku, gdy Rada Ministrów się nie zbierze? Kolejne dotyczy momentu opublikowania rozporządzenia w Dzienniku Ustaw (a co za tym idzie momentu rozpoczęcia stanu wojennego): czy zostaje ono opublikowane po podpisaniu przez prezydenta (i kontrasygnowaniu przez premiera), czy dopiero gdy Sejm nie podejmie uchwały o odrzuceniu? Wydaje się, że rozporządzenie powinno ukazać się niezwłocznie po podpisaniu, ale co w przypadku gdy Sejm uchyli rozporządzenie po kilku dniach[169]? Pozostaje jeszcze kwestia zebrania się Sejmu, gdyż być może ze względu na sytuację panującą w kraju będzie to niemożliwe. Pomijając, że cała procedura wprowadzenia może okazać się zbyt skomplikowana, w kontekście tego konkretnego zagrożenia prawdopodobne wydawać się mogą problemy czy wręcz brak funkcjonowania części systemów teleinformatycznych. Natomiast stan wojenny w Polsce obowiązuje od momentu – nie faktycznych działań ani wydania rozporządzenia, ale od dnia jego ogłoszenia w Dzienniku Ustaw[170]. Zatem, w przypadku problemów z funkcjonowanie systemów rządowych będzie, to kolejny element powodujący opóźnienie.

3. Cyberdziałania a zadania organów w stanie wojennym

Wprowadzenie przesłanki działań w cyberprzestrzeni w stanach nadzwyczajnych od samego początku budziło wątpliwości. Już w opinii prawnej projektu Andrzej Szmyt zauważał, że powtarzanie definicji cyberprzestrzeni w każdej ustawie o stanach nadzwyczajnych wydaje się zbędnym zabiegiem, natomiast wskazywał, że brakuje rozwinięcia pojęcia cyberprzestrzeni w perspektywie jej oddziaływania na społeczeństwo

---

[168] Ustawa z dnia 29 sierpnia 2002 r. o *stanie wojennym...* art. 3 ust. 1.

[169] Szczegółowo o kontroli decyzji o wprowadzeniu stanu wojennego i uchwaleniu uchylenia rozporządzenia pisał Krzysztof Prokop, vide: *Stany nadzwyczajne...,* op. cit., s. 64-69.

[170] Ustawa z dnia 29 sierpnia 2002 r. o *stanie wojennym...* art. 4: „Stan wojenny obowiązuje od dnia ogłoszenia rozporządzenia, o którym mowa w art. 3 ust. 1, w Dzienniku Ustaw Rzeczypospolitej Polskiej".

i ewentualnych ograniczeń wolności i praw człowieka występujących po wprowadzeniu stanu wojennego[171].

Jest to zagadnienie równie interesujące, co nieco kontrowersyjne w kontekście możliwości wprowadzenia stanu wojennego. Należy zatem zastanowić się, czy jeśli stan ten „zarezerwowany" został jedynie dla zagrożeń *stricte* wojennych, pochodzących od innego podmiotu, działania w cyberprzestrzeni wypełnią przesłankę wprowadzenia stanu wojennego? A jeśli jednak to by nastąpiło, jaka byłaby wówczas rola Naczelnego Dowódcy? Problematyczne jest także nieokreślenie skali, skutków, rozmiaru szkód wywołanych przez działania w cyberprzestrzeni, które pozwoliłyby na wprowadzenie któregoś ze stanów.

Wobec powyższego należy wskazać zadania i uprawnienia poszczególnych organów w czasie stanu wojennego w związku z działaniami w cyberprzestrzeni. I tu pojawiają się także problemy. Zadań odnoszących się bezpośrednio do tej sytuacji nie mają wyszczególnionych najważniejsze organy w systemie kierowania bezpieczeństwem narodowym, jak Prezydent RP, Rada Ministrów czy Prezes Rady Ministrów. Jednym z najważniejszych organów w stanie wojennym, po uprzednim mianowaniu przez Prezydenta RP na wniosek Prezesa Rady Ministrów, byłby także Naczelny Dowódca Sił Zbrojnych. Należy jednak wskazać na brak wyszczególnienia zadań Naczelnego Dowódcy odnoszących się do działań w cyberprzestrzeni. Skoro przesłanki te mogą dać podstawę do wprowadzenia stanu wojennego, powinno się wskazać udział zadaniowy Naczelnego Dowódcy, bądź jego brak.

Warto także zaznaczyć, że w raporcie NIK z 2015 roku nadal wskazywano, że: „nie zostały dotychczas opracowane plany reagowania kryzysowego i utrzymania ciągłości działania podstawowych procesów ekonomicznych oraz funkcji państwa, w sytuacjach zagrożeń związanych z cyberprzestrzenią. Tworzone w Polsce plany kryzysowe, w tym w szczególności Krajowy Plan Zarządzania Kryzysowego, odnosiły się wyłącznie do konwencjonalnych zdarzeń, takich jak, np. katastrofy naturalne i nie uwzględniały zmiany charakteru zagrożeń wynikającej, m.in. z postępu technologicznego"[172].

---

[171] A. Szmyt, *Opinia do przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw*, Druk sejmowy nr 4355, Warszawa 2011.

[172] *Realizacja przez podmioty państwowe…, op. cit.,* s. 14; 62-65.

Wskazać jednak należy, że w najnowszym *Krajowym Planie Zarządzania Kryzysowego* (2017)[173] uwzględniono już zagrożenia związane z cyberatakiem, które mogą wywołać zakłócenie funkcjonowania systemów i usług telekomunikacyjnych. W dokumentach tych wyszczególniono także zadania najważniejszych organów w tym zakresie, dzieląc je na fazy zapobiegania, przygotowania, reagowania i odbudowy. Mimo zasadniczo szczegółowo przedstawionych procedur, w przypadku zakłócenia funkcjonowania systemów i usług telekomunikacyjnych nie omówiono tego zagadnienia dokładnie[174].

W KPZK wskazano Szefa Agencji Bezpieczeństwa Wewnętrznego za podmiot odpowiedzialny za główne zadania związane z omawianą sytuacją. Na podstawie ustaw wypunktowano jego zadania, które dotyczyć mają: uruchomienia procesu koordynacji obiegu informacji w związku z wystąpieniem zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych, a następnie wnioskowanie do właściwych organów o wprowadzenie stopnia alarmowego CRP w związku z tą sytuacją. Kolejnym krokiem jest uruchomienie i nadzór nad realizacją zadań w przypadku ataku na infrastrukturę teleinformatyczną organów administracji rządowej oraz wydanie poleceń organom administracji publicznej, właścicielom i posiadaczom obiektów, instalacji, urządzeń infrastruktury administracji publicznej lub infrastruktury krytycznej w przypadku wystąpienia zdarzenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych, a następnie organizacja realizacji zadań na rzecz wsparcia procesu odtwarzania i zapewnienia ciągłości działania infrastruktury krytycznej[175].

Należy wskazać, że wraz z ustawą o *krajowym systemie cyberbezpieczeństwa* usystematyzowano zadania niektórych organów w tym zakresie. Wymienić należy tu obowiązki ministra obrony narodowej, który zgodnie z art. 51 zobowiązany jest do: współpracy Sił Zbrojnych RP z właściwymi organami NATO, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej w zakresie cyberbezpieczeństwa (w tym prowadzenie Narodowego Punktu Kontaktowego do współpracy z NATO)[176]; zapewnienia zdolności Sił Zbrojnych RP w układzie krajowym, sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa

---

[173] *Krajowy Plan Zarządzania Kryzysowego,* część A i B, Rządowe Centrum Bezpieczeństwa, Warszawa 2017.

[174] Z racji uchwalenia ustawy o *krajowym systemie cyberbezpieczeństwa* można przypuszczać, że w następnym KPZK zagadnienie to zostanie rozwinięte.

[175] *Krajowy Plan Zarządzania Kryzysowego,* część B, s. 56.

[176] Ustawa z dnia 5 lipca 2018 r. o *krajowym systemie cyberbezpieczeństwa…,* art. 52.

powodującego konieczność działań obronnych; rozwijania umiejętności Sił Zbrojnych RP w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych; pozyskiwania i rozwoju narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych RP.

Do najważniejszych zadań ministra względem omawianego tematu, wskazać należy przede wszystkim kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego; ocenę wpływu incydentów na system obrony państwa oraz ocenę zagrożeń cyberbezpieczeństwa w czasie stanu wojennego oraz przedstawienie właściwym organom propozycji dotyczących działań obronnych, a także koordynowanie we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa.

Jak wspomniano, w przedmiotowej ustawie wskazano incydenty, które podzielono na cztery kategorie: incydent krytyczny[177], incydent poważny[178], incydent istotny[179], incydent w podmiocie publicznym[180]. Jak dodaje Filip Radoniewicz, różnią się one: rodzajem podmiotu, który je identyfikuje, klasyfikuje, zgłasza (z wyjątkiem incydentu krytycznego) i zapewnia w związku z tym obsługę – zwykle jest to ten sam podmiot; CSIRT'em, do którego

---

[177] Zgodnie z art. 2 pkt 6 to incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV.

[178] Zgodnie z art. 2 pkt 7 to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.

[179] Zgodnie z art. 2 pkt 8 to incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UEL26 z31.01.2018).

[180] Zgodnie z art. 2 pkt 9 to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny (podmioty wymienione zostały w dalszych częściach ustawy).

incydent jest zgłaszany; stopniem oddziaływania[181]. Jednak w ustawie nie wskazano expressis verbis, że dany rodzaj incydentu będzie dawał możliwość wprowadzenia któregoś ze stanów nadzwyczajnych czy skutkował koniecznością jego wprowadzenia.

Pewien niedosyt w tym zakresie zostawia także *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*[182]. *W Strategii Cyberbezpieczeństwa* wskazano jedynie, że celem usprawnienia zarządzania bezpieczeństwem będą wdrażane działania polegające na wymianie informacji i uzgodnianie reakcji zarówno na poziomie strategicznym, jak i poziomie operacyjnym, w sferze cywilnej i wojskowej. Określono, że konieczna jest budowa systemu wymiany informacji odpornego na cyberzagrożenia dla potrzeb administracji publicznej, który będzie wykorzystany w różnych stanach nadzwyczajnych oraz stanach gotowości obronnej państwa[183]. Mimo innych niedociągnięć, w *Doktrynie cyberbezpieczeństwa RP* wyróżniono niektóre zagrożenia, które mogą wystąpić[184]. Oprócz istotnego stwierdzenia, że „operacje w cyberprzestrzeni stanowią dziś integralną część klasycznych kryzysów i konfliktów polityczno-militarnych (wojen)"[185], zwrócono uwagę, że cyberkryzysy i cyberkonflikty mogą powstawać przy udziale, tak podmiotów (państwowych), jak i niepaństwowych. Jest to szczególnie istotne wobec definicji ustawowej stanu wojennego, w której wskazuje się na zagrożenie zainicjowane przez zewnętrzne

[181] F. Radoniewicz, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa: komentarz,* red. W. Kitler, J. Olszewska-Taczkowska, F. Radoniewicz, Wyd. C. H. Beck, Warszawa 2019.

[182] *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024,* przyjęta uchwałą nr 125 Rady Ministrów z dnia 22 października 2019 w *sprawie przyjęcia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024,* (Dz.Urz. z 2019, poz. 1037). *Strategia Cyberbezpieczeństwa* zastąpiła *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022,* które zostały przyjęte uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. *w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.*

[183] *Strategia Cyberbezpieczeństwa RP*, s. 12.

[184] Wyróżniono: cyberszpiegostwo, ataki w cyberprzestrzeni o podłożu ideologicznym, politycznym, religijnym, biznesowym i kryminalnym, zainicjowane przez państwa, grupy terrorystyczne czy ekstremistyczne, vide: *Doktryna cyberprzestrzeni Rzeczypospolitej Polskiej,* BBN, Warszawa 2015, s. 13-14.

[185] Ibidem, s. 13.

podmioty[186]. Należy zgodzić się z Joanną Kuleszą[187], która podkreśla, że w powyższej sytuacji nie można jednoznacznie stwierdzić, czy państwo poszkodowane mogłoby skorzystać z samoobrony (zbrojnej), gdyż nie jest pewne, czy zagrożenie bezpieczeństwa poprzez działania w cyberprzestrzeni uznane zostałoby za spełniające przesłanki napaści zbrojnej, czy nawet agresji. Pomijając już zagadnienie podmiotowości, wątpliwości wywołuje konieczność „zewnętrzności" atakujących.

Niemniej jednak w ostatnim czasie podjęto szereg inicjatyw dotyczących przeciwdziałaniu cyberzagrożeniom, które mogłyby skutkować wprowadzeniem stanu wojennego. W lipcu 2019 roku pomiędzy NATO a Polską zostało podpisane porozumienie dotyczące współpracy w obszarze cyberbezpieczeństwa. Podjęto także decyzję o powołaniu **Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni** na bazie Narodowego Centrum Kryptologii i Inspektoratu Informatyki. Powołano **pełnomocnika MON ds. utworzenia wojsk obrony cyberprzestrzeni. Na** bazie **Centrum Operacji Cybernetycznych sformowane zostaną Siły Obrony Cyberprzestrzeni,** które docelowo zostaną przekształcone w wojska obrony cyberprzestrzeni.

4. Podsumowanie

Działania w cyberprzestrzeni są przesłanką do wprowadzenia stanu wojennego. O ile występuje tu podstawa prawna, istnieje dużo wątpliwości natury prawno-organizacyjnej odnośnie do ewentualnej sytuacji wprowadzenia tego stanu w przypadku cyberzagrożeń. Należy przecież wziąć pod uwagę zewnętrzny podmiot (czy aby na pewno uwzględniona byłaby grupa hackerska? organizacja terrorystyczna?), atak (na co? na kogo?), cel (przede wszystkim celowe działania godzące w niepodległość czy niepodzielność RP)… Ale może jeszcze bardziej istotny jest skutek[188], wymiar i zasięg takiego działania. Te elementy

---

[186] Jak już wskazano autorka uważa, że wyrażenie „zewnętrzne w stosunku do niej podmioty" należy rozpatrywać w świetle prawa międzynarodowego publicznego. Co więcej, także w *Uzasadnieniu do projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw* (2011), *nie* odniesiono się do kwestii, co uznawać należy za zewnętrzny podmiot.

[187] *Analiza prawna działań w cyberprzestrzeni,* Raport Fundacji im. K. Pułaskiego, opracowanie przygotowane na zamówienie Centrum Doktryn i Szkolenia Sił Zbrojnych w Bydgoszczy, Warszawa 2015, s. 14.

[188] O skutkach jakie mogą wywołać działania w cyberprzestrzeni wspomniano już w uzasadnieniu do projektu ustawy, nie zdecydowano się jednak na ich umieszczenie w samej ustawie ze względu

nie są uregulowane i wprowadzenie stanu wojennego jest aktem bardziej politycznym, niż praktycznym. Wszak nie ma obecnie regulacji, które na ten konkretny przypadek porządkowałyby zadania najważniejszych organów państwowych. Mimo podjętych działań w tym zakresie, „brak jest kompleksowych procedur reagowania kryzysowego i utrzymania ciągłości działania podstawowych procesów ekonomicznych oraz funkcji państwa w sytuacji zagrożeń lub zakłócenia działania infrastruktury państwa spowodowanych zdarzeniami występującymi w cyberprzestrzeni”[189].

Co więcej, podkreślić należy, że zanim jednak wprowadzony zostanie, którykolwiek ze stanów nadzwyczajnych konieczne jest wypełnienie znamion z artykułu 228, a mianowicie – muszą zostać wyczerpane wszelkie konstytucyjne środki. W tym wypadku koniecznym jest wykorzystanie procedury zarządzania kryzysowego oraz mechanizmów zagwarantowanych przez ustawę o krajowym systemie cyberbezpieczeństwa.

Jak wynika z dokumentów strategicznych, już kilka lat temu zaczęto zauważać problem związany z brakiem regulacji w cyberprzestrzeni i konsekwentnie powtarzane są uwagi o konieczności wprowadzenia zmian proceduralno-organizacyjnych i legislacyjnych w tym obszarze.

Należy zatem wziąć pod uwagę konieczne, ale dostępne zabiegi natury legislacyjnej, które dotyczyłyby po pierwsze zmiany (uproszczenia) procedury wprowadzenia stanu wojennego. Po drugie, problematyczne jest także nieokreślenie skali, skutków, rozmiaru szkód wywołanych przez działania w cyberprzestrzeni, które pozwoliłyby na wprowadzenie któregoś ze stanów nadzwyczajnych, co wskazywałoby na konieczność doregulowania tego

na decyzję prezydenta i Rady Ministrów o konieczności wprowadzenia stanów nadzwyczajnych: „W tym kontekście należy podkreślić, że rozporządzenia Prezydenta RP i Rady Ministrów o wprowadzeniu określonego stanu nadzwyczajnego mają charakter fakultatywny, a ich wydanie uzależnione jest zawsze od oceny stopnia zagrożenia w sferze zewnętrznego bądź wewnętrznego bezpieczeństwa państwa. Zatem ustawowe nadanie bezpieczeństwu w cyberprzestrzeni rangi istotnego segmentu bezpieczeństwa narodowego znajduje pełne uzasadnienie. W ten sposób bowiem wskazana ocena dokonywana będzie także przez pryzmat skutków naruszeń bezpieczeństwa w przestrzeni wirtualnej, dając w efekcie Prezydentowi RP i Radzie Ministrów poszerzony obraz skali występujących zagrożeń”, vide: *Uzasadnienie do przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw*, 2011.

[189] *Realizacja przez podmioty państwowe…,* op. cit., 62-65.

obszaru. Być może, warto byłoby znowelizować ustawę o *krajowym systemie cyberbezpieczeństwa* rozszerzając ją o powyższe zagadnienia.

5. Bibliografia

Akty prawne i dokumenty strategiczne:

1. *Doktryna cyberprzestrzeni Rzeczypospolitej Polskiej,* BBN, Warszawa 2015.
2. *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022,* które zostały przyjęte uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. *w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.*
3. *Krajowy Plan Zarządzania Kryzysowego,* część A i B, Rządowe Centrum Bezpieczeństwa, Warszawa 2017.
4. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024,* przyjęta uchwałą nr 125 Rady Ministrów z dnia 22 października 2019 w *sprawie przyjęcia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024,* (Dz. Urz. z 2019, poz. 1037).
5. Ustawa z dnia 16 lipca 2004 r. – *Prawo telekomunikacyjne* (Dz.U. z 2019, poz. 2460).
6. Ustawa z dnia 17 lutego 2005 r. *informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2020, poz. 346).
7. Ustawa z dnia 18 kwietnia 2002 r. *o stanie klęski żywiołowej* (Dz.U. z 2017, poz. 1897).
8. Ustawa z dnia 21 czerwca 2002 r. o *stanie wyjątkowym* (Dz. U. z 2017, poz. 1928).
9. Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. z 2007, nr 89, poz. 590).
10. Ustawa z dnia 26 kwietnia 2007 r. *o zarządzaniu kryzysowym* (Dz. U. z 2017, poz. 209).
11. Ustawa z dnia 29 sierpnia 2002 r. o *stanie wojennym i kompetencjach Naczelnego Dowódcy Sił Zbrojnych oraz jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2017, poz. 1932).
12. Ustawa z dnia 5 lipca 2018 r. o *krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2019, poz. 2020, 2248).

Publikacje zwarte i artykuły naukowe:

1. *Analiza prawna działań w cyberprzestrzeni,* Raport Fundacji im. K. Pułaskiego, opracowanie przygotowane na zamówienie Centrum Doktryn i Szkolenia Sił Zbrojnych w Bydgoszczy, Warszawa 2015
2. Kołodziejczak M., *Działania w cyberprzestrzeni jako przesłanka do wprowadzenia stanów nadzwyczajnych w Polsce,* [w:] *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne,* red. nauk. W. Kitler, J. Taczkowska-Olszewska, Wyd. TWO, FINA, Warszawa 2017.
3. Kołodziejczak M., *Różnica pojęć: wojna, konflikt zbrojny, kryzys, zagrożenie występujących w naukach o bezpieczeństwie – ujęcie prawne*, [w:] *Zagrożenia bezpieczeństwa narodowego Rzeczypospolitej Polskiej w XXI wieku. Pojęcie, zakres i kwalifikacja,* pod. red. W. Sójka, M. Kołodziejczak, Wyd. AON, Warszawa 2016.
4. Prokop K., *Stany nadzwyczajne w Konstytucji Rzeczypospolitej Polskiej*, Wyd. Temida, Białystok 2005.
5. *Ustawa o krajowym systemie cyberbezpieczeństwa: komentarz,* red. W. Kitler, J. Olszewska-Taczkowska, F. Radoniewicz, Wyd. C. H. Beck, Warszawa 2019.

Opinie prawne, uzasadnienia, raporty:

1. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP,* Informacja o wynikach kontroli, Najwyższa Izba Kontroli, KPB-4101-002-00/2014, Warszawa 2015.
2. Szmyt A., *Opinia do przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw*, Druk sejmowy nr 4355, Warszawa 2011.
3. *Uzasadnienie do przedstawionego przez Prezydenta Rzeczypospolitej Polskiej projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw*, 2011.

ABSTRACT

ACTIONS IN CYBERSPACE AS A PREMISE FOR THE INTRODUCTION OF MARTIAL LAW IN POLAND

Summary: In this paper author is trying to identify cyberspace activities that could be considered as premise for introducing martial law – the one of the extraordinary measures in Poland. In the Republic of Poland, action in cyberspace is considered a premise for introducing both state of natural disaster, state of emergency and even martial law.

Given the difficulties with definitions and procedures, despite the implemented cybersecurity system, the lack of estimated risk methodology, indicating such activities in cyberspace that could be considered as premises for introducing martial law is probably impossible.

Keywords: cyberspace, action in cyberspace, martial law, extraordinary measure.

ROZDZIAŁ 11

HACKING W KODEKSIE KARNYM - WYBRANE ZAGADNIENIA TECHNICZNE I KARNE

dr Filip RADONIEWICZ [190]

STRESZCZENIE: Głównym celem niniejszego rozdziału jest przedstawienie technicznych aspektów hackingu i kryminalizacji tego zjawiska w polskim Kodeksie karnym. Składa się on z trzech części. Pierwsza stanowi krótkie wprowadzenie do omawianego zagadnienia. W drugiej części omówiono przepisy art. 267 § 1 oraz 267 § 2 Kodeksu karnego kryminalizujące hacking, jak również aspekty techniczne tego zjawiska - opisano w niej metody uzyskania nieuprawnionego dostępu do systemów i sieci informatycznych. Ostatnia część – podsumowanie - jest próbą dokonania oceny obowiązującej regulacji.

SŁOWA KLUCZOWE: cyberprzestępczość, nieuprawniony dostęp, hacking, spoofing, malware.

1. Uwagi wstępne

Na wstępie należy poczynić kilka uwag dotyczących znaczenia terminów hacker i hacking. Początkowo pod pojęciem „hacker"[191] rozumiano po prostu zdolnego programistę.

---

[190] Adiunkt, Wydział Bezpieczeństwa Narodowego Akademii Sztuki Wojennej, f.radoniewicz@akademia.mil.pl, ORCID: 0000-0002-7917-4059.

[191] Termin „hacker" pochodzi od ang. hack, którego używali w latach 60. studenci Massachusetts Institute of Technology na określenie pomysłowych żartów przez nich płatanych (za przykład podaje się modyfikację panelu kontrolnego w windzie, w wyniku której po wciśnięciu przycisku odnoszącego się do wybranego numeru piętra winda jechała na zupełnie inne). Zob. S.W. Brenner, Cybercrime and the Law. Challenges. Issues, and Outcomes, Boston 2012, s. 16.

Później, po zlaniu się w latach 70. subkultury hackerów z phreakerami (od angielskiego określenia phone freak, czyli „telefoniczny maniak", osoba włamującą się do sieci telekomunikacyjnych w celu nawiązywania darmowych połączeń) zaczął nabierać innego znaczenia – kogoś działającego w podziemiu, parającego się hackingiem, czyli włamującego się do komputerów i sieci, często ze szlachetnych pobudek, a czasami po prostu dla zabawy i zdobycia sławy. Takie rozumienie pojęć „hacker" i „hacking" utrwaliły filmy (zwłaszcza „Gry wojenne" J. Badhama z 1983 r., czy „Hakerzy" I. Softleya z 1995 r.)[192]. Obecnie jednak „hackerem" potocznie nazywa się przestępcę „siejącego zamęt" w Internecie, czyli zarówno włamującego się do sieci teleinformatycznych i komputerów, jak i działającego w celu zakłócenia ich pracy[193]. Czasami nawet określa się tak wszystkich przestępców działających w sieci, w tym internetowych oszustów. W związku z powyższym zakres pojęcia „hacking" również bywa rozszerzany i używany dla określenia przestępczej działalności, polegającej nie tylko na włamywaniu się do systemów informatycznych, ale również, np. zakłócania ich pracy[194]. Przedmiotem niniejszego rozdziału jest jednak hacking *sensu stricto* – czyli zachowanie polegające na uzyskaniu nieuprawnionego dostępu do systemu informatycznego lub sieci teleinformatycznej.

2. Nieuprawniony dostęp do danych komputerowych i systemów informatycznych – art. 267 § 1 i § 2 k.k.

W treści art. 267 § 1 k.k. przewidziano odpowiedzialność karną za uzyskanie przez sprawcę bez uprawnienia dostępu do informacji dla niego nieprzeznaczonej, przez otwarcie zamkniętego pisma, podłączenie się do sieci telekomunikacyjnej lub przełamanie albo omi-

[192] Por. S. Bukowski, Przestępstwo hackingu, Przegląd Sądowy, 2006, nr 4, s. 134–137; B. Fischer, Przestępstwa komputerowe i ochrona informacji, Kraków 2000, s. 53–58; D.L. Shinder, E. Tittel, Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci, Gliwice 2004, s. 65–78; J.W. Wójcik, Przestępstwa komputerowe. Część 1 Fenomen cywilizacji, Warszawa 1999, s. 187–189.

[193] Obecnie nie ma już konieczności, by sprawca posiadał zaawansowane umiejętności. Wystarczy, że pobierze z sieci odpowiedni program, który wszystkie czynności wykona za niego. Ukuty został nawet termin dla określenia takich osób – ang. script kiddies – czyli „dzieciaki skryptowe" (skrypt – program napisany w języku skryptowym, który wykonuje pewne działania wewnątrz innego programu – w uproszczeniu jest to niesamodzielny program, np. skrypty JavaScript na stronach WWW, makra w dokumentach MS Office).

[194] F. Radoniewicz, Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warszawa 2016, s. 31-32.

nięcie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia. Czyn ten zagrożony jest karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat dwóch.

Przepis art. 267 § 1 k.k. kryminalizuje trzy zachowania będące zamachami na bezpieczeństwo systemów informatycznych, jeżeli ich skutkiem jest nieuprawnione uzyskanie dostępu do informacji: podłączenie się do sieci telekomunikacyjnej; przełamanie elektronicznego, magnetycznego, informatycznego lub innego szczególnego jej zabezpieczenia oraz ominięcie takiego zabezpieczenia.

W literaturze wskazuje się, że trudno jest rozgraniczyć to znamię od użytego w art. 267 § 3 k.k. – „zakładania lub posługiwania się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem". Zdaniem B. Kunickiej-Michalskiej nie jest to istotne, gdyż w obu wypadkach grozi taka sama sankcja i oba czyny ścigane są w tym samym trybie[195]. Zauważyć jednak trzeba, że między tymi typami przestępstw zachodzą istotne różnice – czyn z art. 267 § 1 k.k. dokonany jest tylko wtedy, gdy sprawca uzyskał dostęp do informacji, natomiast w przypadku występku z art. 267 § 3 k.k. wystarcza, by działał w celu jej uzyskania. Przede wszystkim jednak o tym, który z tych przepisów znajdzie zastosowanie, decydują okoliczności danej sprawy. Nie należy bowiem zapominać, że przepis art. 267 § 3 k.k. kryminalizuje tzw. podsłuch komputerowy, czyli przechwytywanie danych podczas ich przesyłania, natomiast przepis art. 267 § 1 k.k. penalizuje przy użyciu wskazanego wyżej znamienia zachowania polegające na uzyskaniu nieuprawnionego dostępu do informacji przechowywanej w systemie komputerowym. Kryminalizowane zachowanie będzie bowiem polegać na uzyskaniu fizycznego dostępu do sieci, np. poprzez podłączenie się przez sprawcę do serwera i pobranie w ten sposób przechowywanych danych[196].

Drugie z kryminalizowanych w przepisie zachowań polega na przełamaniu elektronicznego, magnetycznego, informatycznego lub innego szczególnego zabezpieczenia. Podkreślić należy, iż przepis art. 267 § 1 k.k. chroni tylko takie informacje przechowywane w systemach informatycznych, które zostały przez ich dysponenta zabezpieczone przed nieuprawnionym dostępem. Przez zabezpieczenia należy rozumieć „wszelkie formy utrudnienia dostępu do informacji, których usunięcie wymaga wiedzy specjalistycznej lub posiadania

---

[195] B. Kunicka-Michalska, [w:] Kodeks karny. Część szczególna. Komentarz do artykułów 222–316. T. II, red. A. Wąsek, R. Zawłocki, Warszawa 2010, s. 694.

[196] F. Radoniewicz, Odpowiedzialność karna…, s. 290-292.

szczególnego urządzenia lub kodu"[197]. Jak wskazuje P. Kardas, z punktu widzenia przestępstwa nie są istotne technologiczne aspekty zabezpieczeń. O ich charakterze (magnetycznym, elektronicznym czy informatycznym) decydują ich właściwości technologiczne. Natomiast doprecyzowanie zakresu tych pojęć ma pewne znaczenie dla interpretacji zakresu przedmiotowego - mającego charakter dopełniający - pojęcia czwartej, niedookreślonej postaci zabezpieczenia („inne szczególne zabezpieczenie"). Będzie to bowiem środek niemożliwy do zakwalifikowania, do któregoś z określonych w przepisie rodzajów zabezpieczeń, a którego neutralizacja przez sprawcę będzie się wiązała z co najmniej takimi trudnościami, jak przełamanie zabezpieczenia elektronicznego, magnetycznego lub informatycznego[198].

Przez przełamanie zabezpieczeń rozumie się bezpośrednie oddziaływanie sprawcy na zabezpieczenie, prowadzące do zniwelowania jego funkcji ochronnej, które nie musi się wiązać z jego zniszczeniem[199]. Dla bytu przestępstwa określonego w przepisie art. 267 § 1 k.k. niezbędne jest, by zabezpieczenie to było realne oraz aktywne w momencie ataku hackera. W przeciwnym wypadku nie dojdzie do wypełnienia znamion przestępstwa[200].

Najpowszechniejszym sposobem zabezpieczenia dostępu do systemu jest wymóg potwierdzenia tożsamości użytkownika za pomocą loginu i hasła (inne metody weryfikacji polegają, np. na wykorzystaniu kart chipowych, czy danych biometryczych). Istnieje kilka metod pokonania tego zabezpieczenia. Jeżeli hasła przesyłane są siecią, sprawca może próbować je przechwycić, tak jak inne dane, za pomocą tzw. sniffera[201]. Może również użyć w tym celu

---

[197] W. Wróbel, [w:] Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k., red. A. Zoll, Warszawa 2013, s. 1502.

[198] P. Kardas, Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego, Czasopismo Prawa Karnego i Nauk Penalnych, 2000, nr 1, s. 71.

[199] P. Kardas, Prawnokarna ochrona..., s. 71–72; P. Kozłowska-Kalisz [w:] Kodeks karny. Praktyczny komentarz, M. Mozgawa (red.), Warszawa 2012, s. 621; W. Wróbel [w:] Kodeks karny…, s. 1502-1503.

[200] Por. S. Bukowski, Przestępstwo hackingu…, s. 142–143; P. Kardas, Prawnokarna ochrona..., s. 64.

[201] Program komputerowy lub urządzenie, którego zadaniem jest przechwytywanie i ewentualnie analizowanie danych przepływających w sieci (nazwa pochodzi od ang. *sniff* - węszyć).

keyloggera[202] lub trojana[203] umieszczonego w komputerze ofiary[204]. Poza tym może je po prostu wyłudzić (omówiona w dalszej części socjotechnika).

Najmniej skomplikowaną metodą złamania hasła jest metoda siłowa (ang. *brute force*), polegająca po prostu na próbowaniu jego odgadnięcia poprzez wpisywanie kolejnych kombinacji. Skuteczna jest zwłaszcza w sytuacjach, gdy hacker ma do czynienia z systemem należącym do prywatnego użytkownika i zna jego dane, których ten mógł użyć przy konstruowaniu hasła (np. data urodzin, imię kota). Istnieją specjalne programy, które dysponują słownikiem (stąd można się spotkać z nazwą „atak słownikowy") wyręczającym sprawcę we wpisywaniu kolejnych kombinacji znaków. Im bardziej skomplikowany jest system zabezpieczeń, tym bardziej złożony musi być program do złamania hasła. Najlepsze z nich umożliwiają łamanie haseł przy pomocy kilku komputerów, np. poprzez podział hasła na części i wykorzystanie do pracy nad każdą z nich oddzielnego komputera. Hasła bardzo często są zapamiętane w systemie. Wystarczy wiedzieć, gdzie i jak ich szukać. Wynika to z tego, że przeciętny użytkownik zazwyczaj korzysta z wielu haseł – do logowania, do skrzynki pocztowej, do logowania się na witrynach WWW itd. Dlatego też zazwyczaj „zleca" ich zapamiętanie systemowi[205].

Ostatnim zachowaniem kryminalizowanym w przepisie art. 267 § 1 k.k. jest ominięcie zabezpieczeń. Pamiętać bowiem należy, że przełamanie zabezpieczeń jest tylko jedną z wielu

---

[202] Program odczytujący i zapisujący wszystkie znaki wpisywane przez użytkownika za pomocą klawiatury. W ten sposób gromadzi cenne informacje, np. loginy i hasła.

[203] Trojany (konie trojańskie) to nieszkodliwe na pierwszy rzut oka programy, w których zapisano dodatkowe instrukcje. Wykonują one działania, o których użytkownik nie wie. Czasami wyróżnia się wśród nich kategorię back doors - czyli programy „tylne drzwi", „furtki", wśród których najsłynniejszym był „Back Orifice", umożliwiające „wejście" do systemu z pominięciem zabezpieczeń (inne znaczenie tego terminu – furtka świadomie pozostawiona przez autora programu, umożliwiająca swobodne „wchodzenie" do systemu). Mogą wykonywać takie czynności, jak usuwanie danych lub ich modyfikacja, przesyłanie plików do osoby, która go umieściła w systemie, czy zakłócanie pracy komputera. Zob. D.L. Shinder, E. Tittel, Cyberprzestępczość..., s. 283; M. Tomaszewski [w:] D. Lisiak, I. Politowska, M. Szmit, M. Tomaszewski, 13 najpopularniejszych ataków na twój komputer – wykrywanie, usuwanie skutków, zapobieganie, Gliwice 2011, s. 78.

[204] Wymienione programy należą do grupy tzw. *malware* (od ang. *malicious software* – oprogramowanie złośliwe), czyli programów i skryptów szkodliwych dla funkcjonowania komputerów i sieci oraz przetwarzanych w nich danych. Do tej kategorii zalicza się ponadto, m.in. wirusy (programy instalujące się bez wiedzy i zgody użytkownika, wykonujące różne działania, które mogą polegać np. na zakłócaniu pracy systemu lub na niszczeniu danych), oprogramowanie szpiegujące (ang. *spyware*), a także omówione w dalszej części *exploity* i boty.

[205] D. L. Shinder, E. Tittel, Cyberprzestępczość…, s. 291-293. Zob. szerzej J. Erickson, Hacking Sztuka…, s. 201-215.

technik (i to nawet nie najczęściej spotykaną) używanych przez hackerów do penetracji systemów komputerowych. Pozostałe sprowadzają się do ich ominięcia, a polegają na:

• wprowadzeniu w błąd człowieka (*social engineering*, czyli tzw. socjotechnika);

• wprowadzeniu w błąd systemu – wśród metod polegających na ominięciu zabezpieczeń w ten sposób należy wskazać tzw. *spoofing* (maskarada);

• wykorzystaniu luk (błędów) w systemach operacyjnych, aplikacjach czy protokołach (są to zbiory zasad określających procesy komunikacyjne odpowiadające, m.in. za identyfikację komputerów w sieci), czemu często służą programy zwane *exploitami* (umożliwiające wykorzystanie konkretnej luki w określonej aplikacji).

Jedną z metod najczęściej używanych przez hackerów jest tzw. socjotechnika lub inżynieria społeczna (ang. *social engineering*). Polega ona na uzyskiwaniu poufnych informacji poprzez interakcje z ludźmi. W przeciwieństwie do pozostałych omówionych metod, nie polega na wykorzystaniu środków technicznych, ale ludzkich słabości – na uzyskaniu dostępu do systemu, czy to przez zdobycie zaufania i wyłudzenie haseł od uprawnionych osób, czy wykorzystanie czyjejś beztroski i braku uwagi, bądź przez skorzystanie z podstępu. Może przykładowo polegać na skontaktowaniu się z pracownikiem firmy i – po przedstawieniu się jako informatyk lub osoba z obsługi technicznej – wyłudzeniu haseł[206].

Socjotechnika stanowi element bardzo wielu ataków. Często bowiem zdarza się, że dla przeprowadzenia ataku środkami technicznymi konieczne jest wymuszenie pewnych działań ze strony potencjalnej ofiary. Może to być namówienie do kliknięcia linka na stronie internetowej, co skutkuje zainstalowaniem się w komputerze użytkownika programu typu *spyware*, czy otwarcie załącznika do wiadomości e-mail, a w rezultacie „zawirusowanie komputera" (jak to miało miejsce, np. w przypadku wirusa „*I love You*")[207].

Z kolei *spoofing* polega na podszywaniu się pod coś lub kogoś, np. fałszowaniu adresów, czyli wprowadzeniu w błąd systemu. Najczęściej fałszowane są adresy IP w nagłówkach pakietów (czyli „porcji" na jakie dzielone są dane w celu przesłania siecią), ale możliwe jest fałszowanie również adresów WWW, poczty elektronicznej oraz wpisów w tablicach ARP i serwerach DNS. W związku z tym możemy mówić o *spoofingu* jako o[208]:

---

[206] Zob. szerzej E. Casey, C. Daywalt, Computer Intrusions, [w:] E. Casey (red.), Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet, Academic Press 2011, s. 375; K. Krysiak, Sieci komputerowe. Kompendium, Gliwice 2005, s. 475-476; D. L. Shinder, E. Tittel, Cyberprzestępczość…, s. 297-299.

[207] Hack Proofing Your Network. Edycja Polska, red. R. Russell, Gliwice 2002, s. 43.

[208] F. Radoniewicz, Odpowiedzialność karna…, s. 92-94.

• fałszowaniu adresów IP (IP spoofing, maskarada), które ma na celu oszukanie atakowanego systemu co do miejsca nadania komunikatów, by przemycić je przez firewall bądź router. Polega na odpowiedniej modyfikacji nagłówków pakietów, by wskazywały zaufany adres. Obecnie nie ma możliwości eliminacji zjawiska IP spoofingu. Można jednak ograniczyć je poprzez odpowiednio skonfigurowaną zaporę sieciową (firewall);

• fałszowaniu ARP (ang. ARP *spoofing*, ARP *poisonning* – „zatruwanie" ARP) – protokół ARP (ang. *Address Resolution Protocol*) jest odpowiedzialny za odwzorowanie adresów IP na adresy fizyczne MAC. Komputery w dynamicznej tablicy ARP mają zapisane adresy IP oraz odpowiadające im adresy MAC hostów ze swojej sieci. W sytuacji gdy komputer wysyłający dane nie ma w swojej tablicy adresu MAC odpowiadającego adresowi IP hosta, do którego chce wysłać dane, protokół ARP wysyła do wszystkich komputerów danej sieci (podsieci) komunikat z żądaniem, by komputer o danym adresie IP podał swój adres MAC. Gdy udzielona zostaje odpowiedź, protokół dokonuje odpowiedniego „wpisu" w tablicy ARP. Fałszowanie ARP polega na wysyłaniu przez atakującego nieprawidłowych odpowiedzi, wskazujących fałszywy adres MAC (np. adres sprawcy), co prowadzi do tworzenia nieprawdziwych wpisów w tablicy. Rezultatem tego jest przesyłanie danych do nieodpowiedniego komputera (wskazanego przez sprawcę);

• fałszowaniu DNS (ang. *DNS spoofing*, *DNS poisonning* – „zatruwanie" DNS) – system nazw domen (DNS – ang. *Domain Name System*) odpowiada za odwzorowanie nazw domen (mnemonicznych, np. www.google.pl) na odpowiednie adresy IP (np. 173.194.116.184). Użytkownik, chcąc uzyskać dostęp do określonej witryny internetowej, wpisuje jej adres w postaci mnemonicznej. Następnie system operacyjny wysyła zapytanie do serwera DNS w celu uzyskania adresu IP tej witryny. Jeżeli hacker zastąpi w serwerze DNS prawidłowy adres innym, sprawi, że użytkownik, wpisując nazwę interesującej go strony, trafi na zupełnie inną. Może to być, np. strona utworzona przez hackera, imitująca „oryginalną" stronę serwisu internetowego banku;

• fałszowaniu adresów poczty elektronicznej (ang. *e-mail spoofing*), czyli działaniu mającemu na celu ukrycie prawdziwego nadawcy wiadomości lub podszycie się pod cieszącą się zaufaniem adresata osobę lub instytucję (np. bank, w którym ma on konto). Technika ta używana jest przy próbach wyłudzenia poufnych danych (np. danych dostępowych do kont bankowości elektronicznej) oraz przy rozsyłania tzw. spamu, jak potocznie nazywa się niechciane wiadomości.

Ostatnią wspomnianą grupą technik hackerskich, mogących umożliwić uzyskanie nieuprawnionego dostępu, są metody polegające na wykorzystaniu luk. Internet stanowi zbiór

aplikacji pełniących określone funkcje (routing pakietów, udostępnianie informacji czy zasobów). Aby pełnić swoją rolę, muszą współpracować one z użytkownikiem[209]. Proces ten może polegać, np. na naciśnięciu klawisza lub „kliknięciu" kursorem w odpowiednie pole, czy wprowadzeniu ciągu znaków. Użytkownik może w sposób zamierzony lub nieświadomy wprowadzić do aplikacji dane, których ta się nie spodziewa, tj. takie, których nie przewidzieli programiści, a w związku z tym nie określili, co się dzieje, gdy pojawią się takie nieoczekiwane (nieprawidłowe) wartości. W rezultacie może dojść do zawieszenia systemu lub otwarcia drogi do niego[210]. Klasycznym przykładem takiej sytuacji jest tzw. przepełnienie bufora (ang. *buffer overflow*), bądź też nadpisanie bufora (ang. *buffer overrun*). Bufory to obszary pamięci operacyjnej, w których programy przechowują dane przed skopiowaniem ich na dysk. Ich przepełnienie następuje w sytuacji, gdy liczba bajtów lub wprowadzonych znaków przekracza maksymalną, tj. przewidzianą przez programistę dopuszczalną liczbę, np. jeżeli przewidziano 25 bajtów, a zostanie wprowadzone 27, dojdzie do nadpisania obszarów pamięci bezpośrednio sąsiadujących z buforem, które mogą być innym buforem, innymi zmiennymim bądź też danymi odpowiedzialnymi za przepływ sterowania wykonywanego programu. W rezultacie może dojść do zakłócenia lub nawet unieruchomienia programu. Hacker, może w ten sposób uzyskać dostęp do systemu poprzez nadpisanie danych w taki sposób, że program zacznie wykonywać jego polecenia[211].

Inną grupą ataków z tej grupy, o jakiej należy wspomnieć, są ataki polegające na wprowadzeniu odpowiednio spreparowanych danych wejściowych, których wykonanie przez zaatakowaną aplikację pozwala, np. na ominięcie mechanizmów uwierzytelnienia, nieautoryzowane uzyskanie lub modyfikację danych czy wykonanie poleceń systemowych. Za ilustrację posłuży tzw. *SQL injection* (dosłownie „wstrzyknięcie SQL" lub „zastrzyk SQL"). Większość stron internetowych zbudowana jest z wykorzystaniem baz danych, w których przechowywane są dane zgodnie z określonymi regułami. Mogą to być informacje wszelkiego rodzaju, w zależności od charakteru danego serwisu (strona sklepu internetowego, banku, biblioteki itd.). Język *Structured Query Language* (SQL) jest z kolei najpopularniejszym, niezależnym od bazy danych językiem służącym do przekazywania poleceń do bazy danych i prezentowania wyników w zrozumiałym dla użytkownika formacie. Aby aplikacja (pełniąca

[209] Hack Proofing…, s. 191.
[210] K. Krysiak, Sieci komputerowe…, s. 492–493. Zob. szerzej J. Erickson, Hacking. Sztuka penetracji, Gliwice 2004, s. 31–36.
[211] F. Radoniewicz, Odpowiedzialność karna…, s. 97-99.

rolę pośrednika między użytkownikiem a serwisem, czyli np. klientem sklepu internetowego, a tym sklepem) mogła funkcjonować, musi posiadać dostęp do bazy danych (zawierającej zarówno np. asortyment sklepu, jak i dane klientów) z uprawnieniami niezbędnymi do wykonywania określonych czynności w tej bazie (np. przeglądania asortymentu sklepu). Jest zatem uprawniona do korzystania z jej zasobów. Jeżeli atakujący zmodyfikuje polecenia przekazywane przez aplikację (zwykle za pośrednictwem formularza czy okna dialogowego)[212] do serwera bazy danych, zmodyfikowane zapytania będą wykonywane z uprawnieniami przynależnymi aplikacji. W tym wypadku atakujący nie przechodzi żadnego procesu uwierzytelniającego. Nie zatrzyma go również żadna zapora sieciowa, odgradzająca aplikację i serwer bazy danych. Jeżeli bowiem aplikacja może z tej bazy korzystać, to może to czynić za jej pośrednictwem również atakujący[213].

Z popełnieniem przestępstwa z art. 267 § 1 k.k. mamy do czynienia, gdy sprawca w wyniku podłączenia się do sieci telekomunikacyjnej lub przełamania albo ominięcia zabezpieczeń bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej[214]. W związku z tym dla bytu przestępstwa z art. 267 § 1 k.k. nie jest istotne, czy uzyskana przez sprawcę informacja jest tą, której poszukiwał, a także to, czy jest dla niego w jakikolwiek sposób przydatna[215]. Karalne jest samo uzyskanie dostępu do informacji, co wiąże się z uzyskaniem dostępu do danych procedowanych przez ten system (co jest równoznaczne

---

[212] Inną metodą ataku SQL Injection jest, np. użycie zmodyfikowanych odpowiednio plików cookies.

[213] F. Radoniewicz, Odpowiedzialność karna…, s. 100-101. Zob. szerzej np. M. Bąbol, M. Miłosz, Współczesne technologie…, s. 97-117; Hack Proofing…, s. 196-199.

[214] Bezkarne pozostają czynności przygotowawcze do uzyskania dostępu, takie np. jak skanowanie portów (port jest to przyporządkowane każdej usłudze lub aplikacji miejsce, z którego i do którego docierają „jej" dane). Działanie to wiąże się już z wejściem w interakcje z atakowanym systemem (komputerem, serwerem czy routerem), ale nie ma jeszcze charakteru inwazyjnego. Polega ono na sprawdzeniu, które porty w danym systemie są otwarte. Skanowanie pozwala na ustalenie, które urządzenia w sieci są podatne na atak, jakie usługi TCP/IP są uruchomione, a następnie na zbadanie ich pod kątem luk w zabezpieczeniach. Służą temu programy nazywane po prostu skanerami. Są one dostępne w Internecie (np. AngryIP, NSAuditor), często jako aplikacje służące administratorom do sprawdzenia bezpieczeństwa sieci (np. Microsoft Baseline Security Analyzer). Pociągnięcie do odpowiedzialności karnej za skanowanie portów umożliwia regulacja angielska (Computer Misuse Act z 1990 r.), czy stanowiąca jej recepcję singapurska. Zob. też Zob. szerzej C. Easttom, J. Taylor, Computer Crime, Investigation, and the Law, Boston 2011, s. 425–432; J. Erickson, Hacking. Sztuka…, s. 166–167; K. Krysiak, Sieci komputerowe..., s. 477–489; F. Radoniewicz, Odpowiedzialność karna…, s. 77-79, 408-410; D.L. Shinder, E. Tittel, Cyberprzestępczość..., s. 281–283.

[215] M. Kalitowski [w:] Kodeks karny. Komentarz, red. M. Filar, Warszawa 2012, s. 1207.

z uzyskaniem dostępu do systemu informatycznego lub jego części)[216]. Aby było możliwe postawienie sprawcy zarzutów, nie musi on uzyskać władztwa nad informacją[217]. Występek ten można popełnić tylko umyślnie, działając z zamiarem bezpośrednim[218].

Nowelizacją z 2008 r.[219], mającą implementować postanowienia decyzji ramowej 2005/222 w sprawie ataków na systemy informatyczne[220], dodano do art. 267 k.k. – jako § 2 – przepis kryminalizujący działanie sprawcy polegające na uzyskaniu bez uprawnienia dostępu do całości lub części systemu informatycznego. Przedmiotem ochrony, podobnie jak w przepisie art. 267 § 1 k.k., jest poufność przetwarzanych w systemie informatycznym danych informatycznych. Choć nie wynika to wprost z jego treści, przepis chroni również dwa pozostałe aspekty bezpieczeństwa danych, tj. ich integralność i dostępność. Wskazuje na to jednoznacznie uzasadnienie nowelizacji z 2008 r., w którym stwierdza się, że „przepis art. 267 § 2 k.k. penalizuje czyn skutkujący uzyskaniem, bez uprawnienia, dostępu do systemu informatycznego lub jego części, nawet bez złamania jakiegokolwiek zabezpieczenia zainstalowanego w komputerze użytkownika lub zabezpieczenia systemowego. Czyn taki może polegać, np. na wprowadzeniu do systemu informatycznego oprogramowania, które umożliwia sprawcy przejęcie zdalnej kontroli nad komputerem w celu wykonania z jego wykorzystaniem zmasowanych ataków na określone strony internetowe. Sprawca w takim przypadku nie działa w celu uzyskania informacji znajdującej się w zasobach przejętego systemu lub dostępu do niej, lecz w celu przejęcia kontroli nad systemem jako narzędziem do bezprawnego wykorzystywania. Przewidując omawiany nowy typ przestępstwa, projekt ustawy usuwa istotną lukę w obowiązującym prawie, gdy tego rodzaju szkodliwe działania pozostają obecnie

---

[216] Zob. też A. Adamski, Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?, Prawo Teleinformatyczne, 2007, nr 3, s. 6–7.

[217] Krytycznie do tego rozwiązania odniosła się B. Kunicka-Michalska [w:]System prawa karnego. Tom 8. Przestępstwa przeciwko państwu i dobrom zbiorowym, red. L. Gardocki, Warszawa 2012, s. 931.

[218] Tak też A. Marek, Kodeks karny. Komentarz, Warszawa 2010, s. 571; P. Kozłowska-Kalisz [w:] Kodeks karny. Praktyczny komentarz, red. M. Mozgawa, s. 622; W. Wróbel [w:] Kodeks karny…, s. 1503.

[219] Ustawa z 24 października 2008 r. o zmianie ustawy - Kodeks karny i niektórych innych ustaw (Dz. U. z 2008 r. Nr 214, poz.1344).

[220] Decyzja ramowa Rady 2005/222/WSiSW z 24.02.2005 r. w sprawie ataków na systemy informatyczne (Dz. Urz. UE 2005 L 69/67), zastąpiona przez Dyrektywę Parlamentu Europejskiego i Rady 2013/40/UE z 12.08.2013 r. dotyczącą ataków na systemy informatyczne i uchylającą decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE 2013 L 218/8).

poza zakresem penalizacji"[221]. Autorzy projektu słusznie wskazali, że celem uzyskania nieuprawnionego dostępu do systemu może być nie tylko uzyskanie dostępu do informacji, ale czyn ten może stanowić niejako wstęp do innych działań. Trafnym zobrazowaniem takiej sytuacji jest przytoczony w uzasadnieniu przykład umieszczenia w komputerze programu (często nazywanego botem), umożliwiającego uzyskanie nad nim kontroli, celem stworzenia sieci takich przejętych komputerów, tzw. botnetu[222], za pomocą którego sprawca ma zamiar przeprowadzić rozproszony atak odmowy usługi (DDoS)[223]. Nie do końca zgadzam się jednak z tezą, że zachowanie takie pozostawało całkowicie bezkarne. Umieszczenie w systemie programu służącego przejęciu nad nim kontroli (czy innej szkodliwej aplikacji) stanowi nieuprawnioną modyfikację danych komputerowych, a co za tym idzie może być kwalifikowane jako czyn z art. 268a § 1 k.k[224]. Ponadto przepis art. 267 § 2 k.k. znajdzie zastosowanie, gdy celem sprawcy, który uzyskuje nieuprawniony dostęp, jest popełnienie innego, „pospolitego" przestępstwa. Jego zachowanie może bowiem polegać, np. na uzyskaniu dostępu do konta innego użytkownika w serwisie aukcyjnym, w celu wykorzystania go do dokonywania oszustw.

Przez dostęp do całości lub części zarówno systemu informatycznego, jak i komputerowego należy rozumieć uzyskanie możliwości korzystania z jego zasobów, czyli – w zasadzie – przetwarzanych w nim danych. To, na ile sprawca może sobie pozwolić w zaatakowanym systemie, zależy od zakresu uprawnień, jakie uda mu się uzyskać. Jeżeli zdobędzie on uprawnienia administratora, będzie mógł dokonywać w zasadzie wszystkich czynności w ramach całego systemu. W przypadku uzyskania uprawnień zwykłego użytkownika jego możliwości będą ograniczone do korzystania z fragmentów zasobów systemu lub do dokonywania określonych operacji na danych informatycznych.

---

[221] Druk sejmowy nr 458, Sejm VI kadencji, Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, s. 5–6, http://orka.sejm.gov.pl/Druki6ka.nsf/WWW-wszystkie/0458?OpenDocument, dostęp 30.09.2020 r.

[222] Zob. szerzej A. Adamski, Botnety jako zagadnienie prawno-kryminologiczna na tle doświadczeń amerykańskich, Prokuratura i Prawo, 2013, nr 11, s. 68-69.

[223] Ataki DoS (ataki odmowy usług, *Denial of Service*) mają zazwyczaj na celu zakłócenie pracy sieci (łącznie z jej zablokowaniem). W zasadzie można przyjąć, iż polegają na wywołaniu dużego ruchu sieciowego lub ruchu określonego rodzaju, prowadzącego do zawieszenia serwera, przeciążenia routera lub urządzeń sieciowych. Ich „wzmocnionymi" wariantem są ataki DDoS (rozproszone ataki DoS, *Distributed Denial of Service*), często wykorzystujące w tym celu botnety.

[224] F. Radoniewicz, Odpowiedzialność karna…, s. 319.

Przez dostęp nieuprawniony należy rozumieć dostęp bez uprawnień lub z ich przekroczeniem, np. gdy ktoś wprawdzie ma prawo do korzystania z systemu jako zwykły użytkownik, ale w wyniku błędu systemu operacyjnego uzyska prawa administratora. Kwestia praw dostępu do zasobów systemu informatycznego regulowana jest w większości wypadków przez przepisy „miękkiego prawa" – regulaminy wewnętrzne sieci. O nadaniu użytkownikowi uprawnień oraz o ich zakresie decyduje zwykle administrator systemu.

Czyn zabroniony stypizowany w art. 267 § 2 k.k. jest przestępstwem materialnym – skutkiem działania sprawcy jest uzyskanie dostępu do całości lub części systemu informatycznego. Jest to przestępstwo powszechne. Dopuścić się go można jedynie umyślnie, w zamiarze bezpośrednim.

W świetle art. 269c k.k. nie podlega karze za przestępstwo określone w art. 267 § 2 k.k. sprawca działający wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia pod warunkiem niezwłocznego powiadomienia dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, o ile jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody.

Sprawcy omawianego przestępstwa korzystają oczywiście z tych samych metod i narzędzi, co w przypadku występku z art. 267 § 1 k.k.

Rozwiązanie przyjęte przez ustawodawcę w przepisie art. 267 § 2 k.k. spotkało się z uzasadnioną krytyką z trzech zasadniczych powodów. Po pierwsze, jest to niejako automatyczne i dosłowne przekopiowanie treści art. 2 decyzji ramowej 2005/222. Należy podkreślić, że decyzje ramowe były instrumentami prawnymi służącymi do zbliżania przepisów prawnych państw członkowskich. Określały rezultat, jaki ma zostać osiągnięty, natomiast dobór środków ku temu prowadzących pozostawiano państwom członkowskim. W przypadku decyzji ramowych z dziedziny prawa karnego materialnego ustawodawca krajowy miał obowiązek wprowadzenia takich zmian w porządku prawnym, by na podstawie przepisów karnych możliwe było kryminalizowanie opisanych w tych decyzjach czynów. W związku z tym ich postanowienia sformułowane są bardzo ogólnie. W pewnym uproszczeniu – ustawodawca krajowy powinien dokonać implementacji norm prawnych, a nie przepisów. Co za tym idzie, decyzje ramowe harmonizujące prawo karne materialne nie nadawały się do dosłownej trans-

pozycji. Natomiast polski ustawodawca treść art. 2 decyzji ramowej 2005/222 dosłownie przepisał. Andrzej Adamski zastosowaną „technikę legislacyjną" trafnie określił jako *copy and paste*[225].

Po drugie, w związku z powyższym, przepis art. 267 § 2 k.k. jest niezwykle pojemny treściowo. Znamiona czynu w nim opisanego wypełni sprawca, który „uzyskuje nielegalny dostęp" do danych, bo na tym w zasadzie polega – o czym była już mowa – uzyskanie dostępu do systemu, przy czym by odpowiadać karnie, nie musi w tym celu ani łamać zabezpieczenia, ani go omijać. Jedynym warunkiem jest, by dostęp ów był nieuprawniony. Przykładem może być uzyskanie dostępu do niezabezpieczonej sieci wi-fi. Można by się zastanawiać, czy ustawodawca w ten sposób usiłował stworzyć swego rodzaju typ podstawowy przestępstwa (art. 267 § 2 k.k.) oraz jego typ kwalifikowany (art. 267 § 1 k.k.), wymagający działania polegającego na pokonaniu zabezpieczeń, a co za tym idzie – bardziej szkodliwego społecznie? Zważywszy jednak na okoliczność, że oba występki zagrożone są identyczną sankcją – karą pozbawienia wolności do lat dwóch – koncepcję tę wypada wykluczyć. Przyjąć należy, że przepis art. 267 § 2 k.k. będzie znajdował zastosowanie w przypadkach, gdy głównym elementem czynu sprawcy było uzyskanie dostępu do systemu informatycznego, a nie uzyskanie dostępu do informacji (z sytuacją taką mamy do czynienia, np. w wypadku włamania się na konto w serwisie aukcyjnym w celu wykorzystania go do popełnienia przestępstwa oszustwa) lub gdy nie doszło do naruszenia zabezpieczeń.

Po trzecie, jedynym warunkiem, który musi zostać spełniony, aby możliwe było postawienie sprawcy zarzutu naruszenia przepisu art. 267 § 2 k.k., jest uzyskanie przez niego dostępu do systemu bez uprawnień. Natomiast kwestię uprawnień użytkowników sieci komputerowych regulują przede wszystkim – jak była mowa wyżej – takie „akty" jak regulaminy, a nie przepisy o randze ustawowej. To swego rodzaju odesłanie przez ustawodawcę do norm pozaprawnych jest niebezpieczne i trudne do pogodzenia z zasadą określoności przestępstwa[226].

3. Podsumowanie

Kwestie odpowiedzialności karnej za przestępstwo hackingu unormowano w przepisach art. 267 § 1 k.k. (uzyskanie nieuprawnionego dostępu do informacji) oraz art. 267 § 2

---

[225] A. Adamski, Nowe ujęcie cyberprzestępstw..., s. 7–8.

[226] Zwraca na to uwagę A. Adamski (zob. A. Adamski, Nowe ujęcie cyberprzestępstw..., s. 8).

(uzyskanie nieuprawnionego dostępu do całości lub części systemu informatycznego). Głównym narzędziem do walki z hackingem, jako czynu nienakierowanego na uzyskanie informacji, ale na zdobycie samego dostępu do systemu jest art. 267 § 2 k.k. Jednocześnie jednak pozostawiono art. 267 § 1 k.k. (w zmodyfikowanej wersji). Efektem opisanej sytuacji jest fakt, że niektóre zachowania teoretycznie mogą być kryminalizowane przez trzy przepisy – art. 267 § 1, art. 267 § 2 oraz art. 267 § 3 k.k. Wydaje się, że najlepszym rozwiązaniem tej kwestii, które pozostawałoby jednocześnie w zgodzie z postanowieniami dyrektywy 2013/40 dotyczącej ataków na systemy informatyczne, byłoby ograniczenie przepisu art. 267 § 1 k.k. do kryminalizacji przypadków naruszenia tajemnicy korespondencji, przy jednoczesnym przyznaniu głównej roli w walce z hackingiem sensu stricto przepisowi art. 267 § 2 k.k., po uzupełnieniu go o wymóg, by sprawca zniwelował lub ominął magnetyczne, elektroniczne, informatyczne lub inne szczególne zabezpieczenie[227].

4. Bibliografia

1. Adamski A., Botnety jako zagadnienie prawno-kryminologiczna na tle doświadczeń amerykańskich, Prokuratura i Prawo, 2013, nr 11
2. Adamski A., Nowe ujęcie cyberprzestępstw w kodeksie karnym – ale czy lepsze?, Prawo Teleinformatyczne, 2007, nr 3
3. Bąbol M., Miłosz M., Współczesne technologie informatyczne. Zagrożenia i ochrona aplikacji internetowych, Lublin 2014
4. Brenner S.W., Cybercrime and the Law. Challenges. Issues, and Outcomes, Boston 2012
5. Bukowski S., Przestępstwo hackingu, Przegląd Sądowy, 2006, nr 4
6. Casey E., Daywalt C., Computer Intrusions, [w:] E. Casey (red.), Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet, Academic Press 2011
7. Decyzja ramowa 2005/222/WSiSW z 24.02.2005 r. w sprawie ataków na systemy informatyczne (Dz. Urz. UE 2005 L 69/67)

[227] Zob. szerzej F. Radoniewicz, Ujęcie przestępstw przeciwko ochronie informacji w Kodeksie karnym a postanowienia dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne – aspekty wybrane [w:] Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017, s. 313-316.

8. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z 12.08.2013 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW (Dz. Urz. UE 2013 L 218/8)
9. Easttom C., Taylor J., Computer Crime, Investigation, and the Law, Boston 2011
10. Erickson J., Hacking. Sztuka penetracji, Gliwice 2004
11. Fischer B., Przestępstwa komputerowe i ochrona informacji, Kraków 2000
12. Hack Proofing Your Network. Edycja Polska, red. R. Russell, Gliwice 2002
13. Kalitowski M., [w:] Kodeks karny. Komentarz, red. M. Filar, Warszawa 2012
14. Kardas P., Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego, Czasopismo Prawa Karnego i Nauk Penalnych, 2000, nr 1
15. Kozłowska-Kalisz P., [w:] Kodeks karny. Praktyczny komentarz, red. M. Mozgawa, Warszawa 2012
16. Krysiak K., Sieci komputerowe. Kompendium, Gliwice 2005
17. Kunicka-Michalska B., [w:] System prawa karnego. Tom 8. Przestępstwa przeciwko państwu i dobrom zbiorowym, red. L. Gardocki. Warszawa 2012
18. Kunicka-Michalska B., [w:] Kodeks karny. Część szczególna. Komentarz do artykułów 222–316. T. II, red. A. Wąsek, R. Zawłocki, Warszawa 2010
19. Marek A., Kodeks karny. Komentarz, Warszawa 2010
20. Radoniewicz F., Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym, Warszawa 2016
21. Radoniewicz F., Ujęcie przestępstw przeciwko ochronie informacji w Kodeksie karnym a postanowienia dyrektywy 2013/40/UE dotyczącej ataków na systemy informatyczne – aspekty wybrane, [w:] W. Kitler, J. Taczkowska-Olszewska (red.), Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne, Warszawa 2017
22. Shinder D.L., Tittel E., Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci, Gliwice 2004
23. Tomaszewski M., [w:] D. Lisiak, I Politowska, M. Szmit, M. Tomaszewski, 13 najpopularniejszych ataków na twój komputer – wykrywanie, usuwanie skutków, zapobieganie, Gliwice 2011
24. Ustawa z dnia 24 października 2008 r. o zmianie ustawy - Kodeks karny i niektórych innych ustaw (Dz. U. z 2008 r. Nr 214, poz.1344)
25. Ustawa z dnia 6.06.1997 r. – Kodeks karny (t.j. Dz. U.2018r., poz. 1600 ze zm.)

26. Uzasadnienie rządowego projektu ustawy o zmianie ustawy - Kodeks karny oraz niektórych innych ustaw, druk nr 458, http://orka.sejm.gov.pl/Druki6ka.nsf/WWW-wszystkie/0458?OpenDocument, dostęp 29.09.2020 r.
27. Wójcik J.W., Przestępstwa komputerowe. Część 1. Fenomen cywilizacji, Warszawa 1999
28. Wróbel W., [w:] Kodeks karny. Część szczególna. Tom II. Komentarz do art. 117-277 k.k., red. A. Zoll, Warszawa 2013

ABSTRACT

HACKING IN THE POLISH CRIMINAL CODE - SELECTED TECHNICAL AND CRIMINAL ISSUES

Summary: The main purpose of the article is to present the technical aspects of hacking and describe criminalizing this phenomenon in the Polish Criminal Code. It consists of three parts. The first of these is the concise introduction to the discussed issues. The second part discusses provisions of art. 267 § 1 and 267 § 2 of the Criminal Code, which criminalize hacking. It also describes the technical aspects of this phenomenon - it presents the methods of obtaining unauthorized access to information systems. The last one - summary - is an attempt to make an assessment of current regulation.

Keywords: cybercrime, unauthorised access, hacking, spoofing, malware.

ROZDZIAŁ 12

O PEWNYM NOWYM PRZEPISIE I JEDNYM PRECEDENSOWYM WYROKU

dr inż. Maciej SZMIT [228]

STRESZCZENIE: Rozdział zawiera próbę analizy niektórych skutków nowelizacji Kodeksu Wykroczeń polegającej na wprowadzeniu artykułu 107a oraz wyroku Sądu Apelacyjnego w Katowicach z dnia 29 listopada 2019 r. sygn. akt V ACa 266/18 z punktu widzenia ich możliwego wpływu na opiniowanie sądowo-informatyczne.

SŁOWA KLUCZOWE: Tarcza 4.0, informatyka sądowa, odpowiedzialność biegłego.

1. Wstęp

Czas pandemii choroby COVID-19 jest – jak na razie – czasem ograniczonej aktywności ustawodawcy w zakresie interesującym biegłych zajmujących się informatyką śledczą i sądową. Również ograniczenie procedowania sądów nie sprzyja powstawaniu nowych wykładni czy praktyk orzeczniczych. Niemniej warto odnotować przynajmniej dwa zdarzenia z ostatnich 12

[228] Uniwersytet Łódzki, maciej.szmit@uni.lodz.pl; ORCID: 0000-0002-6115-9213.

miesięcy, które mogą mieć wpływ na praktykę opiniowania sądowo-informatycznego: nowelizację Kodeksu Wykroczeń (art. 107a) oraz wyrok Sądu Apelacyjnego w Katowicach z dnia 29 listopada 2019 r. sygn. akt V ACa 266/18.

2. Z tarczą na zoombombing – nowelizacja Kodeku Wykroczeń

Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 (Dz.U. z 2020 r. poz. 1086 ze zm., tzw. Tarcza 4.0), wprowadziła – między innymi – w artykule 26 ust. 1 nowy rodzaj wykroczenia (art. 107a Kodeksu Wykroczeń):

Art. 107a. § 1. Kto nie będąc do tego uprawnionym, włączając się w transmisję danych prowadzoną przy użyciu systemu teleinformatycznego, udaremnia lub utrudnia użytkownikowi tego systemu przekazywanie informacji, podlega karze ograniczenia wolności albo grzywny nie niższej niż 1000 złotych.

§ 2. Jeżeli sprawca czynu określonego w § 1 używa słów powszechnie uznanych za obelżywe lub w inny sposób dopuszcza się nieobyczajnego wybryku, podlega karze aresztu, ograniczenia wolności albo karze grzywny nie niższej niż 3000 złotych.

Uchwalenie tego przepisu (co zresztą było podane w uzasadnieniu[229]) było skutkiem pojawiającego się zjawiska zakłócania (głównie przez uczniów) spotkań internetowych,

[229] Z uzasadnienia do projektu ustawy: *„W art. 25 dodaje się art. 107a w ustawie z dnia 20 maja 1971 r. – Kodeks wykroczeń. Przepis ma na celu ochronę niezakłóconego przebiegu zdalnej komunikacji, prowadzonej za pomocą systemów teleinformatycznych. Nowe technologie informatyczne umożliwiają bowiem „włamania" m.in. na internetowe czaty, wideokonferencje, transmisje lub zdalnie prowadzone formy nauczania i edukacji on-linie. Takie zachowania nie tylko zaburzają prawidłowy tok transmisji, często ją opóźniając lub uniemożliwiając ale także, w przypadku „włamań" połączonych z prezentowaniem treści obraźliwych, obscenicznych, niecenzuralnych lub dyskryminujących, zaburzają porządek społeczny i deprawują małoletnich uczestników transmisji. Należy podkreślić, że rozpowszechnianie za pośrednictwem środków komunikacji elektronicznej tego typu treści w celu zyskania poklasku w danej grupie (najczęściej złożonej z małoletnich) albo wręcz osiągnięcia wymiernej korzyści majątkowej, jest zjawiskiem coraz bardziej powszechnym. Poważnym i pogłębiającym się problemem jest tzw. patostreaming, tj. rozpowszechnianie za pomocą serwisów internetowych zachowań powszechnie uznawanych za dewiacje społeczne, tj. libacje alkoholowe, przemoc, treści pornograficzne lub quasi pornograficzne. O ile dotychczasowy „model" tego typu działalności opierał*

w szczególności zdalnych lekcji, poprzez udostępnianie ekranu zawierającego nieprzyzwoite treści[230].

Wprowadzony przepis spotkał się z krytyką w literaturze przedmiotu. Podkreślano, że tego rodzaju zachowania mogą być karane w oparciu o istniejące przepisy, w szczególności o art. 141 KW[231] bądź art. 51 KW[232]; że – choć w uzasadnieniu mowa o zakłócaniu zdalnych lekcji przez młodzież – ustawodawca nie zdecydował się na ograniczenie oddziaływania nowego przepisu tylko do tej grupy uczestników transmisji[233]. Co więcej – wobec braku poszerzenia w ustawie z 26 października 1982 r. o postępowaniu w sprawach nieletnich (t. jedn.: Dz.U. z 2018 r. poz. 969 ze zm.) katalogu wykroczeń, za popełnienie których mogą odpowiadać nieletni przed sądem rodzinnym – za popełnienie czynu z art. 107a KW, nieletni

---

się na dobrowolnym dostępie użytkowników do platformy streamingowej używanej przez patostreamera i czerpaniu korzyści za pomocą systemów monetyzacji (zamiany ruchu internetowego na danej witrynie na korzyść majątkową), to nie można wykluczyć również aktywnego włączania się takich osób w transmisje prowadzone przez innych użytkowników. Działanie takie może bowiem służyć jako swoista reklama działalności patostreamera, który prezentuje w ten sposób przykłady udostępnianych przez siebie treści szerszej publiczności i zwiększa rozpoznawalność swojej „marki". Należy również uwzględnić ryzyko, jakie niesie za sobą działalność tzw. trolli internetowych, tj. osób, które utrudniają korzystanie z Internetu, kierując się jedynie wewnętrzną potrzebą wywołania negatywnych emocji u innych użytkowników przez szeroki wachlarz antyspołecznych zachowań. Osoby takie będą włączać się do prowadzonych transmisji i zakłócać ich przebieg bez względu na ewentualne obiektywne korzyści majątkowe. Mając powyższe na względzie projektodawca stanął na stanowisku, że niezwykle mało prawdopodobna jest samoregulacja w przedmiotowym zakresie, co rodzi potrzebę penalizacji zachowań określonych w dodawanym art. 107a Kodeksu wykroczeń". Druk sejmowy nr 382 Rządowy projekt ustawy o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19 oraz o zmianie niektórych innych ustaw, http://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=382

[230] Zjawisko takie nazywane bywa zoombombingiem, co jest związane ze złośliwym wykorzystywaniem domyślnego ustawienia w aplikacji Zoom umożliwiającego udostępnianie ekranu bez zgody administratora transmisji. Podobne zjawiska miały miejsce na publicznie dostępnych chatach Discorda również wykorzystywanych w zdalnym nauczaniu.

[231] Warto w tym kontekście zwrócić uwagę na postanowienie SN z 17 kwietnia 2018 r., sygn. akt IV KK 296/17, przyznające Internetowi status „miejsca publicznego" w kontekście art. 141 KW.

[232] Zob. Tarcza antykryzysowa 4.0: Kary za włamanie na e-lekcje, https://www.infor.pl/prawo/wykroczenia/charakterystyka-wykroczen/4590849,Tarcza-antykryzysowa-40-Kary-za-wlamanie-na-elekcje.html

[233] Zob.: Sewastianowicz M.: Grzywną w nieproszonego gościa na Zoom party, Prawo.pl, https://www.prawo.pl/oswiata/grzywna-za-przerywanie-zdalnych-lekcji-wykroczenie,500657.html

odpowiadać będą jedynie wtedy, gdy zachowanie takie przybierze znamiona demoralizacji[234] i będzie miało charakter powtarzalny[235].

Wielu komentatorów wskazuje na podobieństwo ustawowych znamion czynów zabronionych określonych w dyspozycji nowego artykułu oraz w artykułach 268 i 268a KK. Rzeczywiście – rozróżnienie pomiędzy sytuacją, w której działania podejrzanego doprowadziły do udaremnienia lub utrudnienia użytkownikowi systemu przekazywania informacji a sytuacją, w której podejrzany włączając się w transmisję (a zatem – literalnie rzecz biorąc – w sposób inny niż przez zniszczenie, uszkodzenie, usunięcie lub zmianę zapisu istotnej informacji, które to sformułowanie użyte zostało w dyspozycji art. 268 § 1 KK) udaremnił lub znacznie utrudnił osobie uprawnionej zapoznanie się z informacją, będzie niekiedy skrajnie trudne. Ponadto każde, w zasadzie, udaremnienie wysyłania informacji będzie skutkowało udaremnieniem możliwości zapoznania się z nią przez osoby uprawnione do jej odbioru, trudno bowiem zapoznać się z informacją, która nie została wysłana, z kolei utrudnienie wysyłania informacji albo będzie nieskuteczne (można więc będzie rozważać usiłowanie nieudolne) albo w jakiś sposób będzie skuteczne (informacja zostanie wysłana później, wolniej, czy z zakłóceniami), a więc będzie to znowu wiązać się z utrudnieniem zapoznania się z nią. Na dodatek większość ataków typu Denial of Service prowadzona jest zazwyczaj w ten sposób, aby zaatakowanym był nadawca wysyłający informację (w szczególności, gdy mowa o atakach typu rozproszonej odmowy usług DDoS), nie zaś jej odbiorca, uchwalenie omawianego przepisu może więc doprowadzić do problemów ze ściganiem sprawców tego typu ataków. Podobnie, a nawet jeszcze gorzej, wygląda sytuacja z „zakłóceniem w istotnym stopniu lub uniemożliwianiem przekazywania danych informatycznych" z art. 268a § 1 KK i „udaremnianiem lub utrudnianiem przekazywania informacji" z art. 107a § 1 KW.

---

[234] W części komentarzy (zob. np. Szymaniak P.: Areszt za włamanie na e-lekcje, „Gazeta Prawna" z 26.05.2020 r., https://prawo.gazetaprawna.pl/artykuly/1479115,zaklocenie-transmisji-e-lekcje-kara-laczna-areszt-grzywna.html; Tarcza antykryzysowa 4.0: Kary za…, op. cit.) przywoływano przykłady wysyłania w ten sposób treści pornograficznych. Warto przypomnieć, że czyn taki byłby penalizowany z art. 202 § 1 KK.

[235] Zob. Uwagi Helsińskiej Fundacji Praw Człowieka do ustawy z dnia 4 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19, druk senacki nr 142, https://www.hfhr.pl/wp-content/uploads/2020/06/druk-senacki-nr-142-uwagi-HFPC-1.pdf

Warto również rozważyć jeszcze kwestię sformułowania ustawowych znamion czynu zabronionego. Obejmują one: włączenie się w transmisję danych prowadzoną przy użyciu systemu teleinformatycznego oraz udaremnienie lub utrudnienie użytkownikowi tego systemu przekazywanie informacji. Osoba, która dokonuje powyższych czynności, musi być osobą nieuprawnioną do nich, przy czym konstrukcja przepisu pozostawia wątpliwości, czy chodzi o brak uprawnienia do włączania się w transmisję[236], czy o brak uprawnienia do udaremniania bądź utrudnienia użytkownikowi przekazywania informacji, tj. czy osoba uprawniona do włączenia się w transmisję danych, ale nieuprawniona do udaremniania czy utrudniania przekazywania informacji (czyli np. „legalny" uczestnik zdalnego spotkania, ale niemający praw administratora) mogłaby, w razie takiego udaremniania bądź utrudniania, również odpowiadać za naruszenie tego przepisu. Ustawodawca nie użył formy „bez uprawnienia włącza się w transmisję danych i udaremnia bądź utrudnia", która byłaby odpowiednia, gdyby przepis miał karać czynności przyłączenia się bez uprawnienia i zakłócenia, ale „nie będąc do tego uprawnionym, włączając się w transmisję danych (…) udaremnia bądź utrudnia".

3. Odpowiedzialność deliktowa biegłego – wyrok Sądu Apelacyjnego w Katowicach z dnia 29 listopada 2019 r. (V ACa 266/18)

Kwestia odpowiedzialności biegłych za wydaną opinię była przedmiotem wielu rozważań w literaturze przedmiotu. O ile nie ulegała wątpliwości kwestia odpowiedzialności karnej za sfałszowanie opinii, o tyle możliwość odpowiedzialności cywilnej biegłego była niejednokrotnie podawana w wątpliwość. Podnoszono, że nie można przekładać wykładni prawa podatkowego dokonywanej przez TK[237] i NSA[238] (przy okazji ustalania, czy biegły jest płatnikiem VAT) na grunt prawa cywilnego, bowiem biegły nie działa samodzielnie, ale na polecenie i pod kierownictwem organu procesowego, zaś w takiej sytuacji przepisy prawa cywilnego przypisują odpowiedzialność zwierzchnikowi, a nie bezpośredniemu wykonawcy[239]; że biegły ponosić miałby odpowiedzialność zarówno karną[240], jak i cywilną,

---

[236] Zob. np. Sewastianowicz M., op. cit.
[237] Wyrok TK z dnia 12 czerwca 2008 r., sygn. akt 50/05.
[238] Uchwała składu siedmiu sędziów NSA z 12 stycznia 2009 r., sygn. akt I FPS 3/08.
[239] Zob. Jędruszczyk Ł.: Odpowiedzialność cywilna biegłego sądowego, [w:] Temidium.pl, 2014-09-09 https://www.temidium.pl/artykul/odpowiedzialnosc_cywilna_bieglego_sadowego-270.html
[240] Zob.: Nowak M.: Wątpliwości związane z odpowiedzialnością prawną biegłego sądowego w świetle znowelizowanego art. 233 § 4A KK, [w:] „Zeszyty Prawnicze" Nr 17.2 / 2017 s. 76–102,

a nawet pewną formę odpowiedzialności dyscyplinarnej[241] (zwolnienie z funkcji biegłego czy niepowołanie na kolejną kadencję); wreszcie że możliwość skutecznego pozywania biegłego przez stronę prowadzić musi do jego wyłączenia ze sprawy (trudno bowiem uznać za bezstronną osobę znajdującą się w sporze sądowym ze stroną postępowania) i w konsekwencji uznania opinii za niebyłą[242], co – jako konsekwentnie stosowana taktyka – może być skuteczną formą obstrukcji procesowej.

Odnośnie odpowiedzialności cywilnej można było zapewne zgodzić się, że biegły może ponosić odpowiedzialność wobec osób trzecich za niektóre szkody powstałe w związku z wykonywaniem funkcji biegłego (np. za uszkodzenie bądź zniszczenie badanych urządzeń), natomiast wątpliwości budziły możliwości pociągnięcia biegłego do odpowiedzialności cywilnej wobec osób trzecich za przeprowadzone zgodnie z poleceniem organu procesowego czynności badawcze, czy – tym bardziej – za decyzje podejmowane przez organ procesowy w postępowaniach z wykorzystaniem opinii biegłego[243]. Podkreślano, że to na sądzie

---

http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ojs-doi-10_21697_zp_2017_17_2_04/c/2057-1922.pdf

[241] Zob.: Bojarski M.: Problemy odpowiedzialności karnej i dyscyplinarnej biegłego, „Jurisprudencja" T. 18(10)/2000, s. 24−28.

[242] Zob. Wyrok Sądu Najwyższego z dnia 27 maja 1976 r. I PR 64/76

[243] Ryzyko pociągnięcia do takiej odpowiedzialności będzie skłaniać biegłych do wątpliwych zachowań. Zob.: Widła T.: VAT-em w biegłego, wystąpienie na 1. Kongresie Nauk Sądowych, http://www.ptrm.pl/praktyka/warsztat-wyce ny/informacja-z-przebiegu-pierwszego-kongresu-nauk-sadowych-w-warszawie):

„Bez jednoznacznego wskazania w postanowieniu (przez zaznaczenie, że organ procesowy zleca te czynności na własną odpowiedzialność) nie podejmować żadnych czynności badawczych, które mogłyby łączyć się ze zniszczeniem, uszkodzeniem, a nawet jakimkolwiek pomniejszeniem wartości (rynkowej, emocjonalnej) badanego przedmiotu.

W przypadku lekarzy, psychologów, etc.: nie podejmować żadnych czynności pozostających w niezgodzie z ustawami regulującymi prowadzenie działalności zawodowej - np. bez zgody badanego nie pobierać krwi na obecność środków odurzających, bez zgody badanych nie poddawać ich testom lub obserwacjom, etc.

Najlepiej nie podejmować żadnych działań z własnej inicjatywy; a wyłącznie wyraźnie wskazane w postanowieniu - przebadać tylko obiekty wyraźnie wskazane w postanowieniu, nie wahać się z opisem wszystkich, nawet najdrobniejszych zastrzeżeń odnośnie materiału badawczego i tylko odpowiadać na pytania wyraźnie tam postawione (nawet jeżeli przedłożony materiał pozwalałby na więcej, nawet jeżeli miałoby to znaczenie dla sprawy!).

Jeżeli sądy będą konsekwentne; to - w świetle np. wyroku w sprawie o sygn.: I ACa 1875/04 - powinno to zapobiec ewentualnemu orzeczeniu na niekorzyść biegłego.

orzekającym ciąży obowiązek oceny całości materiału dowodowego, a więc i środka dowodowego, jakim jest opinia, że ma on możliwość konwalidacji opinii niepełnej, bądź niejasnej (w tym – za zawierającej sprzeczności: wewnętrzne lub z istniejącym stanem wiedzy) w drodze zobowiązania biegłego do uzupełnienia opinii bądź powołania innych biegłych itd.[244]. W literaturze pojawiały się wprawdzie opinie dopuszczające odpowiedzialność cywilną biegłego za wydanie opinii fałszywej[245], podnoszono jednak szereg

---

Unikać wydawania tzw. opinii kategorycznych (w efekcie rozstrzygnięcie kwestii - odpowiedzialność - spadnie wyłącznie na organ procesowy).
Tam - ale tylko tam - gdzie możliwe są do uzyskania wyliczenia prawdopodobieństwa (np. wg teorematu Bayesa), wnioski wyrażać przy użyciu wykładników liczbowych.
Tam, gdzie biegły odwołuje się do prawdopodobieństwa w sensie psychologicznym (pewność psychologiczna jest tu najwyższym stopniem prawdopodobieństwa), używać wykładników o treści: >>prawdopodobnie ...<<, >>nie wykluczam ...<<, itp. Nie używać zwrotów jednoznacznych (>>osoba badana jest ...<<, >>testament sporządzono pod wpływem choroby ...<<, itp.).
Wzorem zachodnich ekspertów można stosować wykładniki leksykalne o treści: >>literatura przedmiotu (środowisko naukowe) zbiory takich cech, jak znalezione w toku tu opisywanych badań, uznaje za znamienne dla ...<<, itp.
Zaproponowane środki nie kłócą się z ciążącą na biegłym powinnością sumienności i uczciwości; bo pozostają w zgodzie z obecnym paradygmatem metodologicznym! Oczywiście niektórzy prokuratorzy lub sędziowie mogą być z tego powodu niezadowoleni; ale czy biegli powinni się kierować ich interesem, czy też własnym?".

[244] W kontekście znowelizowanego art. 233 § 4 A KK, w którym mowa o nieumyślnym przedstawieniu fałszywej ekspertyzy, podnoszono absurdalność istniejących konstrukcji ustawowych odnośnie do karania biegłego: *„biegły, który po raz kolejny, >>uporczywie podtrzymuje opinię niepełną<<, odmawiając przy tym uzupełnienia nieistniejących jego zdaniem nieścisłości czy nieuwzględniający materiału dowodowego, który w jego ocenie nie posiada wartości poznawczej, może być najpierw ukarany karą finansową (w oparciu o art. 285 § 1a w zw. z § 1), następnie aresztowany na okres do 30 dni (w oparciu o art. 287 § 2 k.p.k.), jego wynagrodzenie może być zmniejszone (w oparciu o art. 618f § 4b), a następnie może być pociągnięty do odpowiedzialności karnej na podstawie art. 233 § 4a k.k. i skazany na karę pozbawienia wolności do lat 3. Niedorzeczność takiej konstrukcji zdaje się wręcz razić, co nie zmienia faktu, że jest ona, jak się zdaje, możliwa pod rządami aktualnie obowiązujących przepisów".* Nowak M.: Wątpliwości…., op. cit.

[245] Zob. Pachnik K.: Prawne uwarunkowania odpowiedzialności cywilnej i karnej biegłych w polskim systemie prawnym, „Edukacja Prawnicza" Nr 10(118)/ 2010, http://www.edukacjaprawnicza. pl/artykuly/artykul/a/pokaz/c/artykul/art/prawne-uwarunkowania-odpowiedzialnosci-cywi lnej-i-karnej-bieglych-w-polskim-systemie-prawnym.html Autor słusznie zauważa, że warunkiem odpowiedzialności jest bezprawność czynu, przy czym owa „bezprawność" może być interpretowana dość szeroko: *„Zaznaczyć trzeba, że czyn biegłego musi być bezprawny. Bezprawność – jako przedmiotowa cecha czynu sprawcy – tradycyjnie ujmowana jest jako sprzeczność z obowiązującym porządkiem prawnym. Pojęcie »porządek prawny« obejmuje przy tym nakazy i zakazy wynikające z normy prawnej, lecz*

wątpliwości, poczynając od tego, że szkodę strona procesowa ponosi nie na skutek wydania opinii, ale na skutek decyzji organu procesowego[246], aż do tego, że ponowna ocena opinii, na której oparł się sąd wydając orzeczenie, mogłaby prowadzić do naruszenia powagi rzeczy osądzonej i stać się przesłanką do podważenia prawomocnych wyroków[247]. Rozważano też pojęcie „opinii fałszywej", o ile bowiem łatwo można mówić o fałszywości zeznań świadka, który zeznaje co do faktów, o tyle opinia biegłego nie jest źródłem materiału faktycznego, a jedynie wyjaśnia fakty przy wykorzystaniu wiadomości specjalnych, przy czym samo słowo „opinia" zdaje się wskazywać, że dopuszczalny jest w jej obrębie pewien subiektywizm[248], choć w literaturze przedmiotu pojawiły się i głosy przeciwne[249].

---

także nakazy i zakazy wynikające z norm moralnych i obyczajowych (…). Przy tym wedle orzecznictwa sam fakt sporządzenia przez biegłych opinii na polecenie sądu nie usuwa ewentualnej bezprawności ich działania, polegającej na nierzetelnym wykonaniu obowiązków biegłych". Z punktu widzenia biegłego informatyka takimi, ryzykownymi, sytuacjami są na przykład: prowadzenie badań niszczących (np. zawartości pamięci ulotnej) czy uzyskiwanie dostępu do informacji chronionej, związane z przełamywaniem bądź omijaniem zabezpieczeń (zob. Szmit M.: Wybrane zagadnienia opiniowania sadowo-informatycznego, PTI, Warszawa 2014, s. 44).

246 Zob. np. Słowik P.: Odszkodowanie od biegłego sprawy nie załatwi, „Gazeta Prawna" z 14.01.2020 r., https://prawo.gazetaprawna.pl/artykuly/1448462,sad-wyrok-odszkodowanie-od-bieglego.html.

247 Zob. np. wyrok SA w Białymstoku z 9 marca 2018 r., sygn. akt I ACa 905/17.

248 Wyrok Sądu Najwyższego z 7 grudnia 2001 r. (IV KKN 563/97): „Odpowiedzialność karna biegłego za przestępstwo tzw. fałszu intelektualnego dotyczy poświadczenia faktów, które poddają się weryfikacji z punktu widzenia ich prawdziwości lub fałszu, natomiast nie obejmuje samych ocen".

249 *„Zagadnienie fałszywej opinii wystąpi w sytuacjach:*

- *gdy ocena formułowana w opinii będzie wyraźnie sprzeczna z aktualnym stanem wiedzy w dziedzinie, której opinia dotyczy;*
- *gdy ocena formułowana w opinii będzie wyraźnie sprzeczna z rzeczywistym stanem faktycznym, możliwym do wyinterpretowania z akt sprawy;*
- *gdy ocena będzie oparta na wyraźnie błędnej metodzie badawczej.*

Istotną okolicznością jest, że ocena musi być też od strony subiektywnej (świadomie) nieprawdziwa, a ów element świadomości zachodzić będzie we wszystkich wskazanych sytuacjach". Pachnik K.: Prawne uwarunkowania…, op. cit. Warto zwrócić uwagę, że stanowisko to dotyczyło zapisów KK sprzed nowelizacji artykułu art. 233 § 4a KK, a więc sprzed wprowadzenia pojęcia nieumyślnego przedstawienia fałszywej ekspertyzy. Obecnie należałoby, zapewne, mówić raczej o świadomej zgodzie na możliwą nierzetelność opinii. Por. wyrok Sądu Najwyższego z dnia 7 grudnia 2001 r., sygn. akt IV KKN 563/97: „Biegły sądowy lub rzeczoznawca, z racji pełnionej funkcji i posiadanych uprawnień, nie działa we własnym imieniu i we własnej sprawie, a w sytuacji, gdy wydaje on opinię, co najmniej godząc się z jej nierzetelnością, tym samym poświadcza w niej nieprawdę co do okoliczności mającej znaczenie prawne. Może więc być podmiotem przestępstwa określonego w art. 271 § 1

W tym kontekście za nie tylko precedensowy, ale być może i rewolucyjny, należy uznać wyrok, który zapadł w dniu 29 listopada 2019 r. przed Sądem Apelacyjnym w Katowicach (sygn. akt V ACa 266/18). Sprawa dotyczyła opinii biegłej dotyczącej prawidłowości wykonania robót budowlanych wydanej na potrzeby postępowania cywilnego. Biegła kwestię tę rozstrzygnęła na korzyść wykonawcy, który ostatecznie wygrał spór z inwestorem. Pismo procesowe obejmujące powództwo przeciwko biegłej wniesione zostało do sądu 28 stycznia 2012 r. Pozwana biegła domagała się oddalenia powództwa argumentując, że biegły nie jest samodzielnym bytem procesowym, a za jego działania na zasadzie art. 430 KC odpowiada organ procesowy, który zlecił mu dokonanie czynności oraz – niezależnie od tego – podniosła zarzut przedawnienia roszczenia[250]. Zarówno SO w Gliwicach, jak i SA w Katowicach oddaliły powództwo uznając, że powód nie wykazał bezprawności działania pozwanej i jej winy, stanowiących niezbędne przesłanki odpowiedzialności deliktowej oraz uznały za zasadny zarzut przedawnienia roszczenia na skutek upływu terminu przewidzianego w art. 442 KC. W ocenie Sądu Apelacyjnego, w sprawie nie miał zastosowania art. 442^1 § 2 KC, gdyż pozwanej nie można przypisać zbrodni lub występku.

Na skutek skargi kasacyjnej powoda wyrok Sądu Apelacyjnego został uchylony, a sprawę przekazano do ponownego rozpoznania z zaleceniem uzupełnienia postępowania dowodowego o przeprowadzenie dowodu z opinii instytutu na okoliczność zarzuconej opinii wady. Sąd Najwyższy argumentował także, że zarzucona przez skarżącego wada opinii mogła być skutkiem przestępstwa (wydania fałszywej opinii), a więc ocena spornej kwestii przedawnienia dochodzonego roszczenia na podstawie art. 442^1 § 2 KC wymaga uwzględnienia całego materiału sprawy, zgromadzonego po jego uzupełnieniu. Z tych właśnie przyczyn, celem rozpoznania istoty sprawy, Sąd Apelacyjny w ponownym postępowaniu uchylił zaskarżony wyrok i przekazał sprawę do ponownego rozpoznania Sądowi Okręgowemu. W toku postępowania przed tym sądem do sprawy przystąpił Prokurator, który poparł stanowisko powoda. Po ponownym rozpoznaniu sprawy wyrokiem z 26 kwietnia 2018 r. Sąd Okręgowy w Gliwicach oddalił powództwo, uznając wprawdzie, że opinia biegłej

---

KK (art. 266 § 1 KK z 1969 r.), jeżeli swoim zachowaniem wyczerpuje jego znamiona, a jednocześnie nie bierze bezpośredniego udziału w postępowaniu sądowym lub w innym postępowaniu prowadzonym na podstawie ustawy".

[250] Jak napisano w wyroku Sąd I instancji wydał wyrok w dniu 31 grudnia 2002 r., a orzeczenie sądu odwoławczego zapadło 19 marca 2002 r., zapewne miała miejsce pomyłka odnośnie do roku wydania wyroku, apelacja bowiem musi być później niż wyrok sądu I instancji.

zawierała szereg błędów, jednak z materiału dowodowego nie można było wysnuć wniosków, że godziła się na nie i przewidywała, że w związku z tym jej oświadczenia mogą być nieprawdziwe. Biegła wskazywała nawet w swojej opinii, jakimi dokumentami nie dysponowała przy jej wydawaniu. Sąd Okręgowy wskazał też, że powód nie złożył żadnych wniosków dowodowych, które odnosiłyby się strony woluntatywnej pozwanej dotyczącej realizacji znamion strony przedmiotowej czynu zabronionego z art. 233 § 4 KK. Sąd Okręgowy przyjął, że z braku umyślności zachowanie biegłej nie wyczerpało również znamion czynu zabronionego z art. 271 § 1 KK i w konsekwencji uznał, że wobec skutecznego podniesienia zarzutu przedawnienia powództwo podlegało oddaleniu. Wyrok w całości zaskarżyli powód i Prokurator, zaś Sąd Apelacyjny uwzględnił obie apelacje argumentując, że:

- ustalone przez Sąd Okręgowy uchybienia w opinii świadczą o naruszeniu przez biegłą wymogów, które sprowadzają się do oczekiwania, że opinia zostanie sporządzona z całą sumiennością i bezstronnością, zgodnie z zasadami wiedzy i standardami badawczymi obwiązującymi w dziedzinie, której dotyczy opinia i że obowiązki te były pozwanej znane, skoro pełniła funkcję stałego biegłego sądowego;
- sporządzenie fałszywej opinii pozostawało w adekwatnym związku przyczynowym z poniesieniem przez powoda szkody i że bez znaczenia jest, że opinia została zaakceptowana przez Sąd orzekający w sprawie II C 70/01, a powód nie wnosił do niej zastrzeżeń oraz, że biegły odpowiada za swój delikt, niezależnie od tego czy działanie sądu podjęte w postępowaniu, dla potrzeb którego sporządzono opinię, było prawidłowe czy nie;
- rolą Sądu Okręgowego było stwierdzenie, czy pozwana poprzez sporządzenie opinii naruszyła przepisy ustawy karnej (art. 233 § 4 KK, art. 271 § 1 KC), a jeśli tak, czy w tym czasie miała nastawienie psychiczne uzasadniające przypisanie jej zamiaru popełnienia przestępstwa (co było konieczne do ustalenia długości terminu przedawnienia);
- do stwierdzenia winy umyślnej wystarczające jest, aby sprawca czynu przewidując możliwość jego popełnienia, na to się godził, zaś pozwana będąc stałym biegłym sądowym miała świadomość ciążących na niej obowiązków, znała także swoje obowiązki w przedmiotowej sprawie, ponieważ zostały one określone w tezie dowodowej. Winna zatem podjąć wszystkie możliwe, a zarazem konieczne czynności tak, aby udzielić odpowiedzi na postawione jej pytanie w sposób odpowiadający standardom wiedzy budowlanej. Obowiązków tych biegła nie dopełniła.

W konsekwencji Sąd Apelacyjny uznał, że działając w opisany wyżej sposób pozwana co najmniej godziła się na to, że wnioski przedstawione w jej opinii nie są prawdziwe i tym samym dopuściła się przestępstwa z art. 233 § 4 KK popełnionego z zamiarem ewentualnym. W konsekwencji roszczenie powoda nie było przedawnione, Sąd Apelacyjny zmienił zaskarżony wyrok w ten sposób, że zasądził od pozwanej na rzecz powoda dochodzoną kwotę.

Zapewne wyrok sądu Apelacyjnego doczeka się wielu glos. Niezależnie jednak od tego należałoby się zastanowić nad jego potencjalnymi konsekwencjami dla praktyki orzeczniczej i opiniodawczej. Pomijając nawet nietypowy tryb uznania pozwanej za przestępcę wyrokiem zapadłym w postępowaniu cywilnym odwoławczym (a więc bez gwarancji procesowych właściwych dla procesu karnego) warto zauważyć, że otwarta została w ten sposób droga do kwestionowania wszystkich opinii w postępowaniach zakończonych prawomocnymi wyrokami z ostatnich dwudziestu lat[251], a w konsekwencji, w ewentualnym przypadku stwierdzenia winy biegłego, do szerokiego stosowania nadzwyczajnych środków odwoławczych, trudno bowiem nie uznać ich za zasadne, gdy mowa o orzeczeniach, wyrokach czy decyzjach opartych na fałszywej opinii wydanej przez przestępcę.

Niepokojąca jest konstrukcja, w myśl której biegły, który nie podjął wszystkich możliwych, a zarazem koniecznych czynności tak, aby udzielić odpowiedzi na postawione pytania w sposób odpowiadający standardom, automatycznie staje się przestępcą. Błąd opiniodawczy jest zjawiskiem bardzo częstym[252], podobnie jak zjawiskiem bardzo częstym są błędne wyroki wydawane przez sądy[253]. Składa się na to szereg przyczyn, omówienie których

---

[251] Pozostaje kwestią otwartą, czy taki sposób działania dotyczyć będzie tylko spraw cywilnych, biegli bowiem wydają opinie również w sprawach karnych, ale i w postępowaniach administracyjnych, jak również w szeregu innych sytuacji, na przykład w sprawach dotyczących zamówień publicznych.

[252] W pracy habilitacyjnej Kunz J.: Błąd w opiniach sądowo-lekarskich w sprawach przestępstw przeciwko zdrowiu i życiu, Katedra Medycyny Sądowej Collegium Medicum UJ, Kraków 1999, Autor przeanalizował szereg opinii sądowo-lekarskich znajdując błędy w kilkudziesięciu procentach z nich. Zob. też Marek Z.: Błąd medyczny, Wydawnictwo Medyczne, Kraków 2007, passim.

[253] W badaniach przeprowadzonych przez Instytut Wymiaru Sprawiedliwości w 2000 r. w sprawach cywilnych odsetek postępowań, w których w apelacji uchylono zaskarżony wyrok i sprawę przekazano do ponownego rozpoznania oscylował w niektórych sądach (Gdańsk, Poznań, Warszawa) wokół 20%, w sprawach gospodarczych w Warszawie przekraczał zaś 30%. Zob.: Warzocha E.: Orzecznictwo apelacyjne sądów okręgowych w sprawach cywilnych – sprawozdanie z badania aktowego, IWS, Warszawa 2003.

wykraczałoby znacznie poza ramy niniejszego artykułu, poczynając od aspektów osobowych (niewiedzy, omylności, podatności na wpływy, problemów komunikacyjnych i interpretacyjnych itd.), poprzez ograniczenia natury technicznej, ekonomicznej[254] i organizacyjnej, zarówno po stronie dyscypliny, którą reprezentuje biegły (często bowiem nie istnieją sformalizowane „standardy" postępowania w danej dziedzinie, albo istnieją różne drogi działania, wybór pomiędzy którymi nie musi być wcale oczywisty[255]), jak i po stronie systemu prawnego[256]. I choć oczywiście należy dążyć do minimalizacji błędnych opinii i niesprawiedliwych wyroków, to wydaje się, że multiplikacja rodzajów odpowiedzialności, zaostrzanie kar, czy otwieranie kolejnych dróg do podważania opinii i zapadłych na ich podstawie wyroków może nie być najlepszą drogą do tego celu.

4. Podsumowanie

Oba omawiane zdarzenia: nowelizację KW oraz powołany wyrok, z punktu widzenia biegłych zajmujących się informatyką sądową, należy ocenić jako niefortunne. Wprowadzenie nowego artykułu w KW zagmatwało jeszcze bardziej i tak już trudne do zrozumienia i interpretacji przepisy dotyczące ochrony informacji. Można spodziewać się, że subsumcja czynów zabronionych, w szczególności odnośnie ataków DoS, będzie teraz jeszcze trudniejsza i bardziej czasochłonna. Przedstawiony powyżej wyrok SA w Katowicach wybitnie zwiększa ryzyko związane z opiniowaniem sądowym (nawet jeśli mowa tylko o ryzyku spędzania czasu w sądach w roli pozwanego). Może okazać się, że taki poziom ryzyka jest dla części biegłych niemożliwy do zaakceptowania.

---

[254] „Wiadomo przecież, że najczęściej sądy kierują się zasadą WIELOBE (Pobocha: byle kto, byle szybko, byle tanio!; a w zamian: byle co, wykonane byle jak!)". Widła T.: VATem w biegłych…, op. cit.

[255] W informatyce śledczej na przykład: czy dokonać na miejscu akwizycji danych (wykonać kopię bitową nośnika), czy zabrać cały komputer i kopię wykonać w laboratorium; czy przeprowadzić pełną analizę wszystkich zapisów na nośniku, czy posłużyć się podejściem triage do wytypowania tyko tych zapisów, które – z dużym prawdopodobieństwem – będą zawierać interesujące dane. W niektórych przypadkach wybór sposobu postępowania będzie prosty, w innych – nie.

[256] Biegły bowiem, szczególnie w postępowaniu cywilnym, nie ma swobody żądania uzupełnienia materiału dowodowego, sama zaś konstrukcja postępowania przyjmująca zasadę „prawdy formalnej" może prowadzić biegłego, choćby działającego jak najstaranniej, do niezgodnych z rzeczywistością wniosków, wyprowadzonych z nieprawdziwych – materialnie – przesłanek. Odnośnie tego, czy biegły może żądać uzupełnienia materiału dowodowego (czy będzie to już brak bezstronności), a także tego czy biegły może podejmować pewne czynności (w szczególności tzw. „oględziny przez biegłego") panują rozbieżności zarówno w literaturze, jak i w praktyce.

5. Bibliografia

1. Bojarski M.: Problemy odpowiedzialności karnej i dyscyplinarnej biegłego, „Jurisprudencja" T. 18(10)/200.
2. Jędruszczyk Ł.: Odpowiedzialność cywilna biegłego sądowego, [w:] Temidium.pl, 2014-09-09 https://www.temidium.pl/artykul/odpowiedzialnosc_cywilna_bieglego_sadowego-270.html
3. Kunz J.: Błąd w opiniach sądowo-lekarskich w sprawach przestępstw przeciwko zdrowiu i życiu, Katedra Medycyny Sądowej Collegium Medicum UJ, Kraków 1999.
4. Nowak M.: Wątpliwości związane z odpowiedzialnością prawną biegłego sądowego w świetle znowelizowanego art. 233 § 4A K.K, [w:] Zeszyty Prawnicze 17.2 / 2017, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.ojs-doi-10_21697_zp_2017_17_2_04/c/2057-1922.pdf.
5. Sewastianowicz M.: Grzywną w nieproszonego gościa na Zoom party, Prawo.pl, https://www.prawo.pl/oswiata/grzywna-za-przerywanie-zdalnych-lekcji-wykroczenie,500657.html.
6. Słowik P.: Odszkodowanie od biegłego sprawy nie załatwi, Gazeta Prawna 14.01.2020, https://prawo.gazetaprawna.pl/artykuly/1448462,sad-wyrok-odszkodowanie-od-biegłego.html.
7. Szmit M.: Wybrane zagadnienia opiniowania sadowo-informatycznego, PTI, Warszawa 2014.
8. Szymaniak P.: Areszt za włamanie na e-lekcje, Gazeta prawna z 26.05.2020, https://prawo.gazetaprawna.pl/artykuly/1479115,zaklocenie-transmisji-e-lekcje-karalaczna-areszt-grzywna.html.
9. Tarcza antykryzysowa 4.0: Kary za włamanie na e-lekcje, https://www.infor.pl/prawo/wykroczenia/charakterystyka-wykroczen/4590849,Tarcza-antykryzysowa-40-Kary-za-wlamanie-na-elekcje.html.
10. Uwagi Helsińskiej Fundacji Praw Człowieka do ustawy z dnia 4 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19, Druk sencki nr 142, https://www.hfhr.pl/wp-content/uploads/2020/06/druk-senacki-nr-142-uwagi-HFPC-1.pdf.
11. Warzocha E: Orzecznictwo apelacyjne sądów okręgowych w sprawach cywilnych - sprawozdanie z badania aktowego, IWS, Warszawa 2003.

12. Widła T.: VAT-em w biegłego, wystąpienie na 1. Kongresie Nauk Sądowych, http://www.ptrm.pl/praktyka/warsztat-wyce ny/informacja-z-przebiegu-pierwszego-kongresu-nauk-sadowych-w-warszawie.
13. Ustawa z dnia 20 maja 1971r. Kodeks wykroczeń, Dz. U. 1971 Nr 12 poz. 114, tekst jednolity: Dz. U. z 2019 r. poz. 821 z późn. zm.
14. Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich, tekst jednolity: Dz. U. z 2018 r. poz. 969.
15. Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19, Dz.U. z 2020 r. poz. 1086.
16. Ustawa dnia 6czerwca 1997 r. Kodeks karny, tekst jednolity: Dz.U. z 2019 r. poz. 1950 z późn. zm.
17. Wyrok Sądu Apelacyjnego w Białymstoku z 9 marca 2018 r., sygn. I ACa 905/17.
18. Wyrok Sądu Apelacyjnego w Katowicach z 29 listopada 2019 r., sygn. V ACa 266/18.
19. Wyrok Sądu Najwyższego z 7 grudnia 2001 r., sygn. IV KKN 563/97.
20. Postanowienie Sądu Najwyższego z 17 kwietnia 2018 roku, sygn. IV KK 296/17.
21. Wyrok Trybunału Konstytucyjnego z 12 czerwca 2008 r., sygn. K. 50/05.
22. Wyrok Sądu Najwyższego z dnia 27 maja 1976 r. I PR 64/76.
23. Uchwała składu siedmiu sędziów Naczelnego Sądu Administracyjnego z 2009-01-12, sygn. I FPS 3/08.
24. Druk sejmowy nr 382 Rządowy projekt ustawy o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19 oraz o zmianie niektórych innych ustaw, http://www.sejm.gov.pl/Sejm9.nsf/druk.xsp?nr=382.

ABSTRACT

ABOUT A NEW REGULATION AND ONE PRECEDENT-SETTING JUDGMENT

Summary: This chapter attempts to analyze some of the effects of the amendment to the Offences Code consisting of the introduction of Article 107a and the judgment of the Court of Appeal in Katowice of 29 November 2019, ref. V ACa 266/18, from the point of view of their possible impact on forensic IT.

Keywords: Shield 4.0 (Tarcza 4.0), forensic informatics, expert witness liability.

ROZDZIAŁ 13

KRYMINOLOGICZNE I PRAWNE ASPEKTY FUNKCJONOWANIA TOKENÓW INWESTYCYJNYCH – IDENTYFIKACJA ZJAWISKA ORAZ PRZECIWDZIAŁANIE ZAGROŻENIOM

dr Jacek CHARATYNOWICZ [257]

STRESZCZENIE: W rozdziale przedstawiono uwarunkowania terminologiczne i prawne rynku kryptoaktywów i tokenów. Scharakteryzowano najczęściej występujące ryzyka związane z obrotem kryptoaktywami, jak również podjęto próbę identyfikacji metod przeciwdziałania ustalonym zagrożeniom.

SŁOWA KLUCZOWE: kryptoaktywa, tokeny, zagrożenia, przepisy prawne, przeciwdziałanie zagrożeniom.

1. Wstęp

Rynek kryptoaktywów podlega ewolucyjnym przemianom prawnym, ekonomicznym i technologicznym. Rozwój nowatorskiego projektu blockchain, pandemia związana z rozprzestrzenianiem się Covid-19, malejące znaczenie tradycyjnych rynków finansowych[258],

[257] mł. insp. Jacek Charatynowicz, Centralne Biuro Śledcze Policji, j.charatynowicz@gmail.com.

[258] Zgodnie z materiałem informacyjnym zawartym w Pulsie Biznesu, *Inwestorzy stawiają na jachty motorowe*, atrakcyjna forma inwestowania to zaangażowanie finansowe w jachty, które może przynieść zyski w kwotach 8-12 % w skali roku. https://www.pb.pl/inwestorzy-stawiaja-na-jachty-motorowe-1005716, dostęp 25.10.2020 r.

wpływa na zachowania inwestorów indywidualnych i instytucjonalnych. Coraz istotniejszymi formami lokowania kapitału i pozyskiwania środków przez przedsiębiorców są, m. in. inwestycje w obligacje, rynek forex, ale również kryptoaktywa, w tym tokeny inwestycyjne.

W kontekście rozwoju rynku aktywów cyfrowych, wskazać należy dokumenty Europejskiego Nadzoru Bankowego (EBA) czy Europejskiego Nadzoru Rynku Kapitałowego (ESMA) z 2019 r., w których zdefiniowano termin kryptoaktywa (*crypto assets*) jako „rodzaj majątku prywatnego, który zależy przede wszystkim od kryptografii i technologii rozproszonej księgi rozrachunkowej". Dokumenty te wskazują również na możliwość, po spełnieniu pewnych przesłanek i warunków, wykorzystywania kryptoaktywów w charakterze usług o charakterze płatniczym oraz inwestycyjnym[259].

Zgodnie z raportem Financial Conduct Authority, Guidance on Cryptoassets, Consultation Paper CP19/3, ze stycznia 2019 r., kryptoaktywa najczęściej są wykorzystywane:

- jako środek wymiany, zwykle funkcjonujący jako zdecentralizowane narzędzie umożliwiające kupno i sprzedaż towarów oraz usług lub ułatwiające regulację zasad działania usług płatniczych;
- jako inwestycja, w której firmy i konsumenci są bezpośrednio narażeni na ryzyko związane z posiadaniem i handlem kryptoaktywami lub pośrednio narażeni poprzez posiadanie lub handel instrumentami finansowymi, które odnoszą się do kryptoaktywów;
- wspieranie pozyskiwania kapitału i/lub tworzenia zdecentralizowanych sieci poprzez Iinitial Coin Offering lub inne mechanizmy dystrybucji[260].

Rozróżnienie kryptoaktywów, z uwagi na skomplikowany charakter infrastruktury tego systemu, nie jest zadaniem prostym. Zgodnie z cytowanym już Raportem ESMA, Advice Initial Coin Offerings and Crypto-Assets, kryptoaktywa możemy podzielić na waluty cyfrowe, kryptowaluty oraz tokeny. W dokumentach Amerykańskiego Financial Crimes Enforcement Network zbiorczą nazwą – wymienialna waluta wirtualna (*convertible virtual currency*) określa się: walutę cyfrową (*digital currency*), kryptowaluty (*crypto-currency*), wartości oparte

[259] Raport European Banking Authority z 9 stycznia 2019 r., *With advice for the European Commissionon on crypto-assets.* Raport European Securities and Markets Authority z 9 stycznia 2019 r., *Advice Initial Coin Offerings and Crypto-Assets*.

[260] Financial Conduct Authority, *Guidance on Cryptoassets, Consultation Paper CP19/3*, January 2019, s. 9.

na kryptografii (*cryptoasset*) oraz aktywa cyfrowe (*digital asset*)[261]. Natomiast w polskojęzycznej literaturze naukowej oraz literaturze praktycznej można wyróżnić pojęcia: kryptowaluty, waluty wirtualne oraz waluty cyfrowe[262].

Już sama próba prawidłowego sklasyfikowania i uporządkowania kryptoaktywów, powoduje problemy nawet dla podmiotów i autorów profesjonalnie, jak również i naukowo zajmujących się przedmiotowym zagadnieniem. Uwzględniając jednak rozwój rynku tych aktywów, dotychczasowe doświadczenia w zakresie praktyki i technologii ich funkcjonowania, oraz na potrzeby przedmiotowego opracowania możemy przyjąć następujący podział kryptoaktywów: wirtualne waluty, kryptowaluty, waluty cyfrowe oraz tokeny.

Celem przedmiotowego rozdziału jest analityczne i naukowe przybliżenie zagrożeń związanych z obrotem tokenami, ze szczególnym uwzględnieniem tokenów o charakterze inwestycyjnym, jak również przedstawienie instytucjonalnego i operacyjnego im przeciwdziałania.

2. Definicja i rodzaje tokenów

„Kryptoaktywa to cyfrowe odwzorowanie istniejącej w rzeczywistości wartości ekonomicznej, bądź wartości nieznajdującej odzwierciedlenia w realnym instrumencie bazowym, ale przyjmowanej umownie pomiędzy stronami transakcji ustalonej, zapisane z wykorzystaniem zabezpieczeń kryptograficznych, przy wykorzystaniu technologii blockchain”[263]. Tokeny natomiast, to jednostki rozliczeniowe funkcjonujące w ramach zbudowanego już łańcucha blockchain. „Można je traktować jako żeton, bilet, los, kupon, punkt lojalnościowy, dowód, akcję, obligację, papier dłużny, głos w wyborach, prawo własności a nawet monetę kolekcjonerską”[264].

---

[261] P. Opitek, *Pranie pieniędzy i finasowanie terroryzmu z wykorzystaniem walut wirtualnych*, Instytut Kościuszki, Brief Programowy, s. 5. https://ik.org.pl/wp-content/uploads/ik_brief_programowy_ pranie-pieniedzy-i-finasowanie-terroryzmu-z-wykorzystaniem-walut-wirtualnych.pdf, dostęp: 4.11.2020r.

[262] S. Bela, T. Kopyściański, W. Srokosz, *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomicznej i prawne*, Wrocław 2016, s. 52

[263] Stanowisko Urzędu Komisji Nadzoru Finansowego z dnia 16 lipca 2020 r.w sprawie wydawania i obrotu kryptoaktywami, s. 6, https://www.knf.gov.pl/knf/pl/komponenty/img/Stanowisko_UKNF_ws_wydawania_i_obrotu_kryptoaktywami_70296.pdf, dostęp: 24.10.2020 r.

[264] M. Grzybkowski, Sz. Bentyn, *Kryptowaluty*, Wydawnictwo Crypto-logic Sp. z o.o., Poznań 2018, s. 64.

Prezentowana definicja pokazuje w jak szerokim ujęciu może być przedstawiany ten instrument. Cytowany dokument Financial Conduct Authority, *Guidance on Cryptoassets, Consultation Paper CP19/3*, wyróżnia następujące rodzaje tokenów:

- tokeny służące do wymiany: nie są emitowane ani nadzorowane przez żaden organ centralny i są przeznaczone i zaprojektowane do wykorzystania jako środek wymiany. Zwykle są zdecentralizowanym narzędziem do kupowania i sprzedawania towarów i usług bez tradycyjnych pośredników. Tokeny te funkcjonują zwykle poza obszarem rynku regulacyjnego;
- tokeny jako papier wartościowy: to tokeny o określonych cechach, które spełniają definicję instrumentu finansowego, takiej jak akcja lub instrument dłużny;
- tokeny użytkowe: tokeny te zapewniają dostęp do aktualnego lub przyszłego produktu lub usługi, ale nie dają posiadaczom takich samych praw, jak instrumenty finansowe. Chociaż tokeny użytkowe nie są inwestycjami, mogą w pewnych okolicznościach spełniać definicję pieniądza elektronicznego (podobnie jak inne tokeny), natomiast w takim przypadku wymagają stosownego zezwolenia właściwego organu[265].

Natomiast w literaturze możemy spotkać szersze podejście do klasyfikacji tych kryptoaktywów, która wyróżnia następujące rodzaje tokenów:

- walutowe, które reprezentują cechy typowe dla walut i środków płatniczych;
- mające cechy papierów wartościowych – reprezentują prawa własności, udziały, dług przedsiębiorstwa lub organizacji, prawo głosu lub kontroli;
- tokeny użytkowe – tokeny rozliczeniowe projektów, posiadające określoną funkcję w danym zamkniętym ekosystemie, np. będące jednostką rozliczeniową wewnątrz aplikacji internetowej lub innego zamkniętego ekosystemu;
- tokeny reprezentujące dobra fizyczne – stanowią cyfrową reprezentację dóbr materialnych, np. konkretnych egzemplarzy kamieni szlachetnych;
- tokeny reputacyjne – stosowane jako rodzaj nagrody w grach komputerowych, mediach społecznościowych, a także działaniach marketingowych;
- tokeny osobiste, tokeny autorów mogą mieć wartość kolekcjonerską, np. reprezentować popularność danej osobistości, ale także i biznesową. Za tokeny danego celebryty można wykupować jego czas pracy, udział w reklamach lub zaangażowanie w konkretne działania;

[265] Financial Conduct Authority, op. cit. s 5.

– tokeny identyfikowalne, które zawierają specyficzne informacje, indywidualnie określone informacje[266].

3. Zagrożenia związane z obrotem tokenami

Kryptoaktywa, w legalnym obrocie mogą być wykorzystywane przede wszystkim jako usługi o charakterze płatniczym i inwestycyjnym. Posiadają jednak pewne cechy, które predestynują ich wykorzystanie do działań przestępczych, m.in. takie jak: anonimowy charakter, szybkość realizowanej transakcji, również w obrocie międzynarodowym, niskie koszty transakcyjne, bezpieczeństwo obrotu dla znających uwarunkowania technologiczne i kryptograficzne uświadomionych uczestników rynku, czy też brak ingerencji organów państwowych.

Zagrożenia związane z obrotem kryptowalutą zostały już zidentyfikowane i opisane zarówno przez środowisko naukowe, przedstawicieli instytucji publicznych i prywatnych, jak również instytucje europejskie. Do najczęściej występujących zagrożeń związanych z obrotem kryptowalutą, w tym również i tokenami, należy zaliczyć:

– pranie pieniędzy pochodzących z różnych form przestępczości pospolitej, poważnej, jak również z przestępczości zorganizowanej;
– oszustwa związane z emisją kryptoaktywów;
– ukrywanie mienia pochodzącego z różnych form przestępczości, w tym przestępczości zorganizowanej;
– nabywanie mienia, którym legalny obrót jest zabroniony (środki odurzające i substancje psychotropowe, broń);
– do transakcji towarzyszących zjawiskom wymuszeń rozbójniczych, porwań, szantażów komputerowych;
– manipulacja wartością, przy czym metody wykorzystywane przez sprawców są analogiczne do stosowanych działań przestępczych na rynku kapitałowym;
– ataki hackerskie na giełdy/kantory kryptoaktywów, jak również na podmioty gospodarcze oferujące emisję/wymianę kryptoaktywów w ramach usług o charakterze inwestycyjnym.

Z raportów Europolu dotyczących aktywności zorganizowanych grup przestępczych

[266] S. Bentyn, *Kryptowaluty*, op. cit., s. 65.

(tzw. raport SOCTA) wynika, że wśród najczęściej wykorzystywanych metod do prania pieniędzy, oprócz przemytu gotówki, działalności gospodarczej, działalności wyspecjalizowanych grup, należą również nowe metody płatności finansowych wykorzystujące możliwość ukrywania faktycznego beneficjenta transakcji, w tym również kryptowaluty[267].

Europol wyróżnia trzy najczęściej występujące mechanizmy w kontekście wykorzystania rynku kryptowalut do prania pieniędzy[268]:

- wykorzystanie prowadzonej działalności gospodarczej – giełdy kryptowalutowej w procesie legalizowania środków finansowych pochodzących z przestępczości zorganizowanej. W tym celu wykorzystywane są również mechanizmy wymiany gotówkowej na kryptowalutę, w tym bankomaty kryptowalutowe;
- wykorzystanie transakcji smurfingowych polegających na rozdrabnianiu wpłat gotówkowych na kontrolowane przez grupę przestępczą rachunki bankowe, następnie mieszanie i transferowanie do giełd lub innych instytucji rynku kryptowalutowego;
- transfer środków finansowych w celu ich zalegalizowania w zagranicznych giełdach kryptowalutowych.

Istnieją pewne podobieństwa w funkcjonowaniu, modelu i architekturze kryptowalut i tokenów, choć można również wskazać na pewne różnice. Jednak zarówno kryptowaluty, jak i tokeny, oprócz wykorzystania do legalnych transakcji, mogą być wykorzystywane do działań przestępczych, w tym również zagrażać bezpieczeństwu finansowemu indywidulanych i instytucjonalnych uczestników obrotu.

22 listopada 2017 r. Komisja Nadzoru Finansowego opublikowała Komunikat w sprawie sprzedaży tzw. monet lub tokenów (*Initial Token Offerings* – ITOs lub *Initial Coin Offerings* – ICOs). Emisja publiczna kryptowalut jest nowym sposobem pozyskiwania środków w sposób publiczny, z zastosowaniem tzw. tokenów lub monet. Poprzez zakup tokena nabywca uzyskuje określone uprawnienia, najczęściej związane z obietnicą emisji unikalnej kryptowaluty.

W tym przypadku wykorzystywane jest podobieństwo pomiędzy wymienioną procedurą emisji publicznej kryptowalut do funkcjonującej na rynku kapitałowym publicznej emisji akcji. W kontekście realizowanych w tym zakresie nadużyć wykorzystywana jest niewiedza potencjalnych inwestorów wynikająca z następujących czynników:

---

[267] *Raport Europolu SOCTA*, https://www.europol.europa.eu/sites/default/files/documents/report_socta2017_1.pdf s. 19, dostęp: 13.01.2019 r.

[268] https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-criminal-organisation-arrested-in-spain, dostęp: 15.05.2019 r.

- brak możliwości uzyskania informacji o emitencie oraz dostępnych narzędzi weryfikacji posiadanych informacji;
- brak rzetelnych źródeł informacji o okolicznościach i dostatecznie wiarygodnych dokumentów rzetelności i wiarygodności dokumentów na podstawie, których dochodzi do emisji kryptowalut;
- brak podstaw faktycznych dających gwarancję zwrotu powierzanych środków;
- brak podstaw prawnych do ochrony prawnej inwestorów;
- brak nadzoru publicznego organu, który zatwierdza dokument informacyjny (w przypadku publicznej emisji akcji spółek notowanych na GPW w Warszawie SA lub alternatywnym rynku NewConnect w procedurze tej uczestniczy regulator, czyli Komisja Nadzoru Finansowego).

Komisja Nadzoru Finansowego w przedmiotowym komunikacie do zidentyfikowanych ryzyk zaliczyła:

- emisję podejmowaną w ramach ICO, która nie jest uregulowana przez polskie i międzynarodowe prawodawstwo, w związku z czym procedura ta narażona jest na wiele nadużyć, w tym oszustwa na szkodę inwestorów indywidualnych. Emisja przeprowadzona w tym trybie, nie gwarantuje w oparciu o polskie prawo żadnej gwarancji inwestorom. Ponadto może sprzyjać legalizowaniu środków finansowych;
- wysokie ryzyko utraty części lub całości zainwestowanych środków – w tym przypadku inwestorzy, w związku z wysokim ryzykiem tych inwestycji, mogą utracić w całości lub w części zainwestowane środki;
- inwestycję w ICO realizowaną na podstawie dokumentu informacyjnego, tzw. white papers, który jednak nie spełnia wymogów dokumentów opracowywanych na potrzeby dopuszczenia do obrotu na rynku regulowanym – prospektu emisyjnego lub alternatywnego rynku obrotu – memorandum informacyjnego. Ponadto z uwagi na rejestrację emitentów poza granicami RP w zagranicznych jurysdykcjach prawno-podatkowych brak jest rzetelnej informacji na temat faktycznej działalności emitenta oraz projekcie inwestycyjnym;
- wysoka zmienność wartości oraz brak możliwości wyjścia z inwestycji, które polega na braku prawnych gwarancji zwrotu inwestycji, jak również jej wysokości.

Rynek kryptoaktywów nieustannie się rozwija i na rynku obrotu tymi aktywami możemy mieć do czynienia zarówno z omówioną wyżej procedurą ICO, ale również IEO (*initial exchange offering*) oraz ITO.

Komisja Nadzoru Finansowego wskazuje na następujące rodzaje zagrożeń i nieprawidłowości mogące wystąpić w obrocie kryptoaktywami, w których występują procedury ICO, IEO lub ITO:

1. W związku z emisją tokenów, których wydawca zobowiązuje się do ich wykupu, istnieje możliwość naruszenia przepisów ustawy Prawo bankowe, poprzez obciążanie ryzykiem uzyskanych w ten sposób środków finansowych, pod jakikolwiek tytułem zwrotnym. Pod terminem obciążanie ryzykiem rozumie się w szczególności udzielanie pożyczek z pozyskanych środków pieniężnych, czy też dalsze ich inwestowanie w sposób, który potencjalnie zagraża zwrotowi pierwotnej kwoty[269].
2. Należy zwrócić uwagę, iż pomimo funkcjonowania tokenów poza obszarem regulacji rynku kapitałowego, podmioty zajmujące się ich emisją/wydawaniem zobowiązane są do zapewnienia interesów majątkowych inwestorów, jak również realizowania w oparciu o pozyskane w ten sposób środki inwestycje, zgodnie z dokumentem, na podstawie którego je pozyskano. Emisja tokenów inwestycyjnych, realizowana z zamiarem niewywiązania się z tego zobowiązania może skutkować odpowiedzialność karną[270].
3. Istnieje również możliwość uznania przez właściwe organy działalności związanej z emisją tokenów, która polega na lokowaniu, m.in. w prawa majątkowe aktywów osób fizycznych, osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej, zebranych w związku z emisją tokenów inwestycyjnych, jako czyn zabroniony[271].

---

[269] Zgodnie z art. 171 ust. 1 i 3 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe, „prowadzenie bez zezwolenia działalności polegającej na gromadzeniu środków pieniężnych innych osób fizycznych, osób prawnych lub jednostek organizacyjnych niemających osobowości prawnej, w celu udzielania kredytów, pożyczek pieniężnych lub obciążania ryzykiem tych środków w inny sposób, podlega grzywnie do 10 000 000 zł i karze pozbawienia wolności do lat 5".

[270] Zgodnie z art. 286 § 1 ustawy z dnia 6 czerwca 1997 r. Kodek karny: „Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania podlega karze pozbawienia wolności od 6 miesięcy do lat 8.".

[271] Zgodnie z art. 287 ust.1 Ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi: „Kto bez wymaganego zezwolenia lub wbrew warunkom określonym w Ustawie wykonuje działalność polegającą na lokowaniu w papiery wartościowe, instrumenty rynku pieniężnego lub inne prawa majątkowe, aktywów osób fizycznych, osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej, zebranych w drodze propozycji zawarcia umowy, której przedmiotem jest udział w tym przedsięwzięciu podlega grzywnie do 10 000 000zł i karze pozbawienia wolności do lat 5".

4. Ponadto, warto zauważyć, iż w sytuacji, gdy brak jest stosownego zezwolenia na działalność związaną z obrotem instrumentami finansowymi oraz uznania tokenów inwestycyjnych za instrumenty finansowe osoba prowadząca taką działalność zagrożona jest karą grzywny[272].

4. Uwarunkowania prawne tokenów

Od początku funkcjonowania kryptoaktywów, dla opisania tego systemu transakcyjnego używano określeń: anonimowy, zdecentralizowany, funkcjonujący poza obszarem regulacji rynku finansowego i usług płatniczych, dodając jednocześnie przymiotnik – [nieuregulowany. Nie ulega wątpliwości, iż kryptoaktywa funkcjonują poza regulacjami ustawy o obrocie instrumentami finansowymi, czy ustawy o usługach płatniczych w kontekście ich opisu jako instrument finansowy, czy pieniądz elektroniczny. Obserwując jednak ten rynek i analizując obowiązujące rozwiązania prawne należy podkreślić, iż istnieją już w polskim systemie prawnym rozwiązania legislacyjne dla przedmiotowego obszary rynku.

Kryptoaktywa, w tym tokeny, zgodnie z interpretacją, m.in. Izby Skarbowej w Warszawie z 25 lutego 2014 r. – uznawane są jako prawo majątkowe – prawo podmiotowe pozostające w ścisłym związku z ekonomicznym interesem uprawnionego. Jest to uprawnienie określonego podmiotu, które związane jest z jego majątkiem. Prawami majątkowymi są te aktywa, które są bezpośrednio uwarunkowane interesem ekonomicznym podmiotu prawa[273]. Ponadto, podlegają zasadom swobodnego obrotu cywilnego i gospodarczego, wymianie i dziedziczeniu.

Konstatując, nie ulega wątpliwości, iż kryptoaktywo w sensie prawa cywilnego, jest prawem o charakterze majątkowym. Ponadto, prawne regulacje tego obszaru rynku obejmują trzy perspektywy:

- przeciwdziałania wykorzystywania rynku kryptoaktywów do prania pieniędzy oraz finansowania terroryzmu;
- włączenia uczestników rynku kryptoaktywów do systemu skutecznego opodatkowania i eliminacji tzw. szarej strefy;

---

[272] Zgodnie z art. 178 Ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi: „Kto bez wymaganego zezwolenia lub upoważnienia zawartego w odrębnych przepisach albo nie będąc do tego uprawnionym w inny sposób określony w ustawie, prowadzi działalność w zakresie obrotu instrumentami finansowymi, podlega grzywnie do 5 000 000 zł".

[273] A. Wolter, J. Ignatowicz, K. Stefaniuk, *Prawo cywilne,* Wydawnictwo Lexis Nexis 2001, s. 138

– w związku z wykorzystaniem kryptoaktywów jako usługa płatnicza, objęcie regulacją tego segmentu rynku na podstawie ustawy konstytuującej rynek usług płatniczych.

Podstawowym elementem regulacyjnym w Ustawie z dnia 1 marca 2018 r. o przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu[274] było wprowadzenie do porządku prawnego definicji waluty wirtualnej[275] oraz definicji rachunku wirtualnej waluty[276]. Ponadto, podmioty prowadzące działalność gospodarczą, polegającą na świadczeniu usług w zakresie:

a) wymiany pomiędzy walutami wirtualnymi i środkami płatniczymi;
b) wymiany pomiędzy walutami wirtualnymi;
c) pośrednictwa w wymianie;
d) prowadzenia rachunku;

zakwalifikowano do katalogu instytucji obowiązanych.

Instytucje obowiązane[277] to oprócz Generalnego Inspektora Informacji Finansowej, jednostek współpracujących, elementy systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Do ich zasadniczych zadań należy:

– stosowanie wobec klientów tzw. środków bezpieczeństwa finansowego;

---

[274] DzU z 2019 r., poz. 723.

[275] Zgodnie z art. 2 ust. 1 pkt 12 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu wirtualne waluty to „cyfrowe odwzorowanie wartości, które nie jest:
a) prawnym środkiem płatniczym emitowanym przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,
b) międzynarodową jednostką rozrachunkową ustanawianą przez organizację międzynarodową i akceptowaną przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
c) pieniądzem elektronicznym w rozumiem u ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych,
d) instrumentem finansowym w rozumieniu ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi,
e) wekslem lub czekiem;
oraz jest wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany, a także może być elektronicznie przechowywane lub przeniesione albo może być przedmiotem handlu elektronicznego."

[276] prowadzony w formie elektronicznej zbiór danych identyfikacyjnych zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany

[277] Obowiązująca ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu charakteryzuje 25 kategorii instytucji obowiązanych.

- rejestracji i raportowania do GIIF informacji o transakcjach stanowiących równowartość 15 000 euro, transakcji podejrzanych,
- prowadzenie analizy ryzyka w zakresie identyfikowania transakcji podejrzanych,
- stworzenie technologicznych możliwości do wstrzymania transakcji/blokady rachunku.

Stosowanie przez instytucje obowiązane środków bezpieczeństwa finansowego polega na:

- identyfikacji klienta i weryfikacji jego tożsamości;
- podejmowaniu działań w celu identyfikacji beneficjenta rzeczywistego;
- ustalaniu charakteru prowadzonych przez klienta stosunków gospodarczych;
- bieżące monitorowanie transakcji z klientem w zakresie jego zgodności z dotychczasową działalnością.

Kolejną płaszczyzną regulacyjną dla kryptoaktywów był sposób i zakres opodatkowania transakcji z ich udziałem, mając na uwadze osiągane z tego tytułu dochody, zarówno przez osoby fizyczne i prawne, jak również eliminowania zagrożeń związanych z szara strefą.

Zgodnie z Ustawą z dnia 23 października 2018 r. o zmianie ustawy o podatku dochodowym od osób fizycznych[278], przychody z obrotu walutami wirtualnymi zakwalifikowano do przychodów z kapitałów pieniężnych lub zysków kapitałowych. Zgodnie z taką interpretacją do tej kategorii przychodu zalicza się: sprzedaż, zapłatę kryptowalutą, regulowanie innych zobowiązań, sprzedaż na wolnym rynku, giełdzie lub kantorze.

Natomiast w kontekście dochodów wykazanych z obrotu kryptowalutą w związku z prowadzoną działalnością gospodarczą to zastosowanie mają przepisy art. 7B ustawy z 15 lutego 1992 r. o podatku dochodowym od osób prawnych, *w* których przychody określono jako: sprzedaż, zapłatę kryptowalutą, regulowanie innych zobowiązań, sprzedaż na wolnym rynku, giełdzie, kantorze.

Zarówno podatek od osób fizycznych jak i prawnych wynosi 18 lub 32% zgodnie z obowiązującą aktualnie skalą podatkową.

Inną kwestią jest możliwość stosowania dla obrotu kryptoaktywami Ustawy z dnia 9 września 2000 r. o podatku od czynności cywilnoprawnych. Przedmiotowe rozwiązania zostały poddane krytyce przez środowisko związane z nowoczesnymi technologiami i kryptoaktywami. W związku z powstałymi wątpliwościami w kontekście przedmiotu opodatkowania opublikowano Obwieszczenie Ministra Finansów z dnia 29 kwietnia 2020 r.

[278] DzU. z 2018 r., poz. 2193.

w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Finansów w sprawie zaniechania poboru podatku od czynności cywilnoprawnych od umowy sprzedaży lub zamiany waluty wirtualnej[279]. Ponadto, w kontekście opodatkowania kryptoaktywów podatkiem od czynności cywilnoprawnych, od 1 lipca 2020 r., zgodnie z art. 9 ust. 1a ustawy o podatku od czynności cywilnoprawnych, z obowiązku tego zwolniono, m.in. sprzedaż i zamianę walut wirtualnych[280].

Zasadniczą kwestią dla rynku obrotu kryptoaktywów pozostaje jednak forma prowadzenia działalności gospodarczej, wymagania kapitałowe, techniczne, organizacyjne, czy też posiadane zabezpieczenia finansowe. Aktywne działania Komisji Nadzoru Finansowego polegające na ujawnianiu i składaniu do prokuratur zawiadomień o uzasadnionym podejrzeniu popełnienia przestępstwa prowadzenia działalności gospodarczej w zakresie wymiany kryptowalut wbrew przepisom art. 150 ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych, de facto wskazały na optymalny model takiej działalności. Nie bez znaczenia były również prace Zespołu roboczego ds. rozwoju innowacji finansowych (FinTech), który przygotował propozycję optymalnego modelu działalności gospodarczej dla giełd/platform obrotu kryptowalutą w ramach przedmiotowej ustawy – małą instytucję płatniczą.

Najistotniejszymi wymogami dla tej działalności są:

- uzyskanie wpisu do rejestru prowadzonego przez Komisję Nadzoru Finansowego małej instytucji płatniczej;
- średnia całkowita kwota transakcji płatniczych z poprzednich 12 miesięcy wykonanych przez małą instytucję płatniczą, w tym przez agentów, za pośrednictwem których świadczy ona usługi płatnicze, nie może przekraczać kwoty stanowiącej równowartość 1 500 000 euro miesięcznie;
- posiadanie rozwiązań organizacyjnych pozwalających na wyliczenie całkowitej miesięcznej kwoty transakcji płatniczych;
- posiadanie rozwiązań w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Mała instytucja płatnicza świadcząca usługę może przechowywać środki pieniężne użytkowników na rachunkach płatniczych użytkowników, których łączna wysokość środków przyjętych dla jednego użytkownika w każdym czasie nie może przekroczyć równowartości w walucie polskiej 2 000 Euro.

---

[279] DzU. z 2020 r., poz. 793.
[280] DzU. z 2020 r., poz. 695.

Z uwagi na zdecentralizowany i niezaprzeczalny charakter łańcucha blockchain jest on coraz częściej wykorzystywany w instytucjach finansowych do kontaktów z klientem, co wskazuje, iż ten innowacyjny projekt odgrywa coraz większą role w życiu gospodarczym. Pewnym przykładem są zmiany podjęte w Ustawie z dnia 15 września 2000 r. Kodeks spółek handlowych[281], które wprowadzają nowy rodzaj instytucji, tzw. prostą spółkę akcyjną[282] oraz instytucję rejestru akcjonariuszy. W ramach tego rejestru będzie miała zastosowanie technologia rozproszonych rejestrów, a wraz z nią również, token.

Warto również przedstawić założenia projektu Rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptograficznych oraz zmieniająca dyrektywę UE 2019/1937 dnia 24 września 2020 r. COM (2020) 593[283], w którym zawarto propozycję regulacji kryptoaktywów, w tym tokenów. Przedmiotowa koncepcja regulacyjna ma przełomowy charakter dla uczestników tego rynku, jak również perspektyw rozwoju tego rynku.

Już we wstępie tego projektu wskazano, na ważny charakter kryptoaktywów w kontekście rozwoju gospodarczego krajów Unii Europejskiej oraz jej sektora finansowego.

Istotną kwestią w tym dokumencie jest określenie usługi aktywów kryptograficznych, która oznacza dowolną z usług w odniesieniu do dowolnego zasobu kryptograficznego:

- przechowywanie i administrowanie kryptowalutami w imieniu osób trzecich;
- prowadzenie platformy handlowej dla aktywów kryptograficznych;
- wymiana aktywów kryptograficznych na walutę fiducjarną będącą prawnym środkiem płatniczym;
- wymiana aktywów kryptograficznych na inne aktywa kryptograficzne;
- realizacja zamówień na kryptoaktywa w imieniu osób trzecich;
- umieszczanie aktywów kryptograficznych;
- przyjmowanie i przesyłanie zamówień na aktywa kryptograficzne w imieniu osób trzecich;
- udzielanie porad dotyczących kryptowalut.

Zatem zakres przedmiotowych usług aktywów kryptograficznych projektodawca określił w sposób bardzo szeroki.

---

[281] DzU. z 2020 r., poz. 1526.

[282] Przepisy w tym zakresie wejdą w życie 1 marca 2021 r.

[283] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593, dostęp 31.10.2020 r.

Rozporządzenie określa również właściwych dla tego rynku regulatorów, tj. organy właściwe w zakresie nadzoru nad rynkiem kryptoaktywów na poziomie europejskim, czyli ESMA (European Supervisory Market Authority) i EBA (*European Banking Authority*), przyznając tym instytucjom określone uprawnienia o charakterze administracyjnym i dochodzeniowym. Ponadto, rozporządzenie posługuje się terminem właściwy organ kraju członkowskiego. W związku z nowymi zadaniami tych instytucji wskazano również potencjalne ich koszty, które winny być przewidziane w przyszłym budżecie.

Rozporządzenie wprowadza przepisy dotyczące nadużyć na rynku, w tym związanych z działalnością na szkodę inwestora, uczestnika obrotu, jak również zakaz dokonywania działań przestępczych typowych dla rynku kapitałowego, czyli: ujawnienia i wykorzystania informacji poufnej oraz manipulacji wartością kryptoaktywów.

Ponadto, dla emitentów rynku, w zależności od zakresu wykonywanych usług, projekt wprowadza określone wymogi kapitałowe, jak również posiadanie funduszy własnych oraz konieczność opracowania, zgłoszenia do właściwego organu krajowego oraz opublikowanie dokumentu informacyjnego, tzw. *white paper*. Ponadto członkowie zarządu, udziałowcy posiadający 20% udziałów w spółce prowadzącej działalność usługi aktywów kryptograficznych nie mogą być karani za przestępstwa prania pieniędzy oraz finansowania terroryzmu lub inne przestępstwa finansowe.

5. System przeciwdziałania zagrożeniom

Rynek kryptoaktywów z uwagi na tworzenie w tym środowisku nowych instrumentów, możliwości ich wykorzystania w różnych aspektach prowadzonej działalności, innowacyjny i atrakcyjny z punktu widzenia nowych inwestorów charakter, nieustannie się rozwija. Powstaje i ewoluuje rynek tokenów, w tym tokenów o charterze inwestycyjnym. W kontekście rynku kryptoaktywów powstają regulacje, nie tylko dotyczące aspektów przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu, form i regulacji prowadzonej działalności gospodarczej, czy określających zasady opodatkowania obrotu kryptoaktywami, ale również projekty aktów prawnych dotyczące sposobu emisji kryptoaktywów, wymogów kapitałowych, czy też sposobu i wartości zabezpieczenia tych emisji. Przedmiotem projektu regulacyjnego jest również dokument emisyjny, tzw. *white paper*, w którym zawarte będą takie informacje jak dane o emitencie, zasady emisji, zabezpieczenia prawne i finansowe, informacje o ryzykach, termin zapadalności.

W związku z powyższym, pierwszy z aspektów przeciwdziałania zagrożeniom, czyli regulacja rynku, na poziomie prac Parlamentu UE został już zainicjowany. Oczywiście inną kwestią pozostaje, jaki będzie ostateczny kształt tej regulacji.

Ponadto, w związku z takim ukształtowaniem regulacji kryptoaktywów istnieje potrzeba działań szkoleniowych z tego zakresu skierowanych do przedstawicieli instytucji publicznych, w kontekście realizowania przyszłych obowiązków nadzorczych i regulacyjnych, oraz ich stosowania w praktyce, jak również pozostałych uczestników rynku obrotu kryptoaktywami.

Kolejnym aspektem jest multidyscyplinarny i transgraniczny charakter tego zjawiska, który dotyczy obszarów ekonomicznych i technologicznych. Przeciwdziałanie i zwalczanie tego typu zagrożeń wymaga współpracy służb zajmujących się zwalczaniem przestępczości, instytucji nadzoru finansowego, w zakresie przeciwdziałania praniu pieniędzy, finansowania terroryzmu oraz służb skarbowych. Nie tylko na poziomie krajowym, ale również międzynarodowym. Warto przypomnieć, jako przykład multidyscyplinarnego podejścia, prace powołanego przez Prezesa Rady Ministrów w 2018 r. Zespołu Roboczego ds. Analizy Istotnych Zagrożeń Bezpieczeństwa oraz Interesów Konsumentów i Państwa w Sferze Gospodarczej i Finansowej w celu dokonania przez właściwe organy analizy zagrożeń dla bezpieczeństwa finansowego państwa oraz wypracowania rekomendacji skutecznych działań ograniczających te ryzyka.

Ponadto, istotną kwestią jest podejmowanie przez podmioty gospodarcze (banki, instytucje płatnicze, podmioty zajmujące się obrotem kryptoaktywami) niezbędnych środków w zakresie przeciwdziałania ich potencjalnego wykorzystania do prania pieniędzy, finansowania terroryzmu oraz przestępczości finansowej. W tym celu rekomendowana jest współpraca pomiędzy wymienionymi podmiotami, w szczególności, w zakresie wymiany i weryfikacji informacji o klientach i realizowanych przez te podmioty transakcjach[284].

Z uwagi na wskazany już transgranicznych charakter zjawiska istotna jest również współpraca międzynarodowa, nie tylko na poziomie państw Unii Europejskiej, ale również z państwami, w których obrót tymi aktywami jest powszechny oraz identyfikowana jest działalność podmiotów gospodarczych, co do których istnieją wątpliwości w zakresie rzetelności i legalności działania.

Przedmiotowa współpraca ma charakter multilateralny i wielopłaszczyznowy i jest realizowana przez:

– Policję, oraz inne służby w ramach międzynarodowej współpracy;

---

[284] Więcej na ten temat w Guidance For A Risk-Based Approach, Virtual Assets And Virtual Asset Service Providers, FATF, June 2019 r. http://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf [Dostęp 04.11.2020r.]

- nadzór finansowy;
- jednostki analityki finansowej;
- organy skarbowe.

Istotna jest również współpraca instytucji publicznych z przedstawicielami środowiska naukowego oraz prywatnej przedsiębiorczości, przede wszystkim może ona dotyczyć następujących kwestii:

- organizacja wspólnych konferencji naukowych i szkoleń[285],
- tworzenie wspólnych zespołów zadaniowych do zbadania określonego problemu oraz wypracowania metod przeciwdziałania zidentyfikowanym zagrożeniom;
- prowadzenie wielostronnych i wieloaspektowych badań naukowych;
- wymiana doświadczeń i dobrych praktyk;
- tworzenie projektów technologicznych w zakresie analizy blockchain, jego stabilności, podatności na ataki hackerskie.

W kontekście wypracowania platformy do analizy blockchain, która istotnie wpłynęłaby na pracę służb zaangażowanych w nadzór, monitorowanie transakcji, czy też przeciwdziałanie zagrożeniom na rynku obrotu kryptoaktywów, w tym tokenów, warto wskazać na pewne elementy istotne dla tego rozwiązania:

- powiązanie z bazami danych informujących o zidentyfikowanych podejrzanych transakcjach, portfelach, tokenach;
- scenariusze dotyczące przeciwdziałania oszustwom, praniu pieniędzy oraz finansowaniu terroryzmu;
- wizualizacja transakcji;
- analiza danych w sieci TOR;
- powiązanie z właściwą giełdą/kantorem kryptowalut.

Kolejnym aspektem przeciwdziałania zagrożeniom jest kwestia edukacji służb zajmujących się identyfikowaniem nieprawidłowości na rynku, ale również uczestników tego rynku – inwestorów indywidulanych. W zakresie działalności szkoleniowej i edukacyjnej, to istotne są tu inicjatywy Komisji Nadzoru Finansowego dla uczestników rynku, ale również służb zajmujących się przeciwdziałaniem zagrożeniom. Ponadto, nie bez znaczenie jest tu Lista

[285] Przykładem tego są, m. in. organizowane przez Międzynarodową Organizację Policji - Interpol kolejne edycje światowych konferencji na temat walut kryptograficznych.

ostrzeżeń publicznych Komisji Nadzoru Finansowego[286], w której potencjalny inwestor może znaleźć informacje o podmiotach, co do których KNF złożył zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa do jednostki organizacyjnej prokuratury.

Ponadto, rynek kryptoaktywów, poszczególne instrumenty tego rynku, w kontekście identyfikacji ryzyk, jak również projekty wypracowania metod przeciwdziałania zagrożeniom, powinny być wskazywane w strategicznych dokumentach dotyczących bezpieczeństwa państwa, w tym np. w Strategii bezpieczeństwa narodowego, Krajowej Ocenie Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu, jak również Strategii przeciwdziałania prania pieniędzy oraz finansowania terroryzmu.

1 6. Podsumowanie

Kryzys związany z pandemią Covid-19, oprócz wpływu na życie społeczne, polityczne, negatywnie oddziałuje również na gospodarkę, w tym rynek finansowy. Malejące znaczenie tradycyjnych metod oszczędzania, pozyskiwania i alokacji kapitału implikuje rozwój alternatywnych metod inwestycyjnych, w tym kryptoaktywów. Jednym z rozwijających się segmentów tego rynku są tokeny. Analiza funkcjonowania wybranych projektów tego rynku może wskazywać, iż oprócz wykorzystania do legalnego pozyskiwania kapitału, mogą być wykorzystywane do działań przestępczych, oszustw finansowych, ukrywania majątku i prania pieniędzy.

Identyfikacja i rozpoznanie podejrzanych transakcji z wykorzystaniem kryptoaktywów, z uwagi na uwarunkowania technologiczne, anonimowość, międzynarodowy charakter, oraz funkcjonowanie poza obszarem regulacyjnym, nie jest procesem prostym. Uzależniona jest od współpracy służb jednostki analityki finansowej zajmującej się przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu, nadzoru finansowego czy też ochrony zbiorowych interesów konsumentów, zarówno na płaszczyźnie krajowej, jak i międzynarodowej. Ponadto, często zaangażowanie służb i instytucji wspomagane jest pracą biegłych i specjalistów w zakresie informatyki śledczej. Przedmiotowa działania muszą być ponadto wspierane przez wyspecjalizowane jednostki organizacyjne prokuratury.

Istotna jest również edukacja uczestników rynku finansowego, w kontekście podejmowania właściwych decyzji inwestycyjnych.

---

[286] Zgodnie z art. 6b ust. 1 ustawy z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym Komisja podaje do publicznej wiadomości informację o złożeniu zawiadomienia o podejrzeniu popełnienia wybranych przestępstw dotyczących rynku finansowego.

Podsumowując, rozwijające się segmenty rynku kryptoaktywów stanowią w dalszym ciągu wyzwanie dla służb i instytucji zajmujących się ochroną finansowych interesów osób fizycznych i prawnych oraz Skarbu Państwa. W związku z tym powinny być przedmiotem działań analitycznych, kontrolnych, nadzorczo-regulacyjnych właściwych instytucji i służb, celem właściwego przeciwdziałania rozpoznawanym ryzykom.

7. Bibliografia

1. Bela S., Kopyściański T., Srokosz W., *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomicznej i prawne*, Wrocław 2016.
2. Financial Conduct Authority, *Guidance on Cryptoassets, Consultation Paper CP19/3*, January 2019.
3. Grzybkowski M., Bentyn Sz., Kryptowaluty, Wydawnictwo Crypto-logic Sp. z o.o., 2018.
4. Guidance For A Risk-Based Approach, Virtual Assets And Virtual Asset Service Providers, FATF, 21 czerwca 2019 r.
5. https://www.europol.europa.eu/newsroom/news/cryptocurrency-laundering-service-members-of-crimin al-organisation-arrested-in-spain
6. Komunikat Komisji Nadzoru Finansowego z dnia 22 listopada 2017 r. w sprawie sprzedaży tzw. monet lub tokenów (Initial Token Offerings – ITOs lub Initial Coin Offerings – ICOs).
7. Obwieszczenie Ministra Finansów z dnia 29 kwietnia 2020 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Ministra Finansów w sprawie zaniechania poboru podatku od czynności cywilnoprawnych od umowy sprzedaży lub zamiany waluty wirtualnej (DzU. 2020 poz. 793).
8. Opitek P., *Pranie pieniędzy i finasowanie terroryzmu z wykorzystaniem walut wirtualnych*, Instytut Kościuszki, Brief Programowy.
9. Projekt Rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków kryptograficznych oraz zmieniająca dyrektywę UE 2019/1937 z dnia 24 września 2020 r. COM (2020) 593.
10. Puls Biznesu*, Inwestorzy stawiają na jachty motorowe, atrakcyjna forma inwestowania to zaangażowanie finansowe w jachty, które może przynieść zyski w kwotach 8-12 % w skali roku.* https://www.pb.pl/inwestorzy-stawiaja-na-jachty-motorowe-1005716.
11. Raport European Banking Authity z 9 stycznia 2019 r., With advice for the European Commissionon on crypto-assets.
12. Raport European Securities and Markets Authority z 9 stycznia 2019 r., Advice Initial Coin Offerings and Crypto-Assets.

13. Raport Europolu SOCTA z 2017 r.
14. Stanowisko Urzędu Komisji Nadzoru Finansowego z dnia 16 lipca 2020 r. w sprawie wydawania i obrotu kryptoaktywami.
15. Ustawa z 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU z 2019 r., poz. 723).
16. Ustawa z dnia 15 września 2000 r. Kodeks spółek handlowych (DzU. z 2020 r., poz. 1526).
17. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (DzU z 2019 r., poz. 298 ze zm.).
18. Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (DzU. z 2020 r., poz. 95, 695).
19. Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (DzU 2020 poz. 1896).
20. Ustawa z dnia 6 czerwca 1997 r. Kodek karny (DzU z 2020 r. poz. 1444, 1517).
21. Ustawy z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (DzU. z 2020 r. poz. 89, 284, 288, 568).
22. Wolter A., Ignatowicz J., Stefaniuk K., *Prawo cywilne*, Wydawnictwo Lexis Nexis 2001.

ABSTRACT

CRIMINOLOGICAL AND LEGAL ASPECTS OF THE FUNCTIONING OF INVESTMENT TOKENS – IDENTIFICATION OF THE PHENOMENON AND PREVENTION OF THREATS

Summary: The chapter pesents the terminological and legal conditions of the crypto-assets and tokens market. The most common associated risks are characterized with crypto-assets trading, as well as an attempt to identify methods of counteracting the established threats.

Keywords: crypto-assets, tokens, threats, legal regulations, counteracting threats.

ROZDZIAŁ 14

PRZESTĘPSTWO „NA BLIKA”

Ryszard PIOTROWSKI [287]

STRESZCZENIE: Autor niniejszego rozdziału opisuje na czym polega przestępstwo „na BLIKa”. Zwraca uwagę na charakterystyvzne elementy takiego oszustwao zwracać uwagę i przedstawia mechanizmy wykorzystywane przez przestępców.

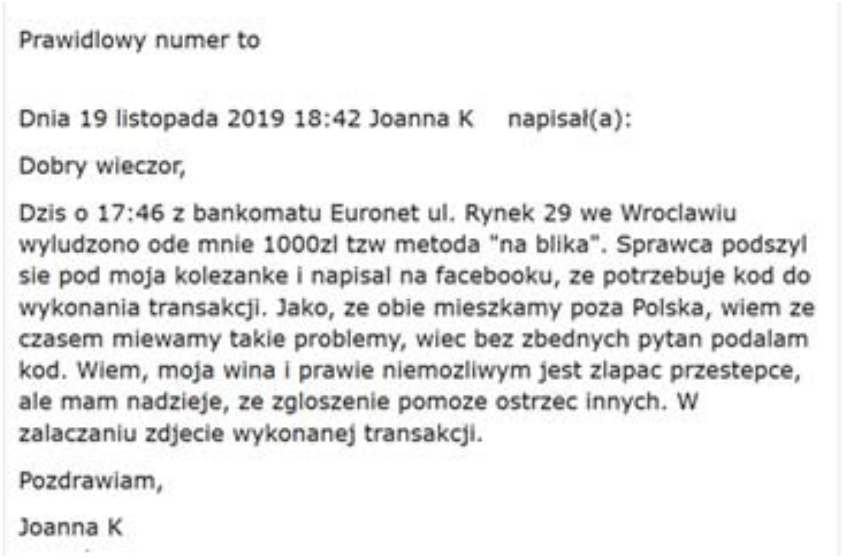
SŁOWA KLUCZOWE: BLIK, oszustwo, haking, tożsamość, spoofing.

„*Dzień Dobry.*
Chciałbym zgłosić przypuszczalne przestępstwo wyłudzenia.
Straciłem 900 złotych tj. pieniądze zostały wypłacone z mojego konta. tzn. ja je przelałem, ale nie tej osobie, której chciałem przekazać gotówkę”
– początkowe nieskładne, enigmatyczne dla przyjmującego, składane wyjaśnienie przez pokrzywdzonego.
„*Teraz wiem, że ktoś się podszył pod mojego kolegę Jarka i kontaktując się ze mną poprzez komunikator Messenger, poprosił mnie o przelanie tej kwoty. Tzn. oczywiście nie Jarek tylko ten ktoś trzeci. Dlaczego to zrobiłem? Zawsze tak z Jarkiem robimy, pożyczając sobie kasę, gdy*

[287] Naczelnik Wydziału dw. z Cyberprzestępczością KWP we Wrocławiu, biegły sądowy przy Sądzie Okręgowym we Wrocławiu z dziedziny Cyberprzestępczości, ryszardpio@wp.pl.

pieniędzy brakuje. Do tej pory wszystko było OK. Usługa BLIK jest bardzo wygodna. Można nią przenosić pieniądze na telefon znajomego i nawet wykorzystać do tego celu bankomat. Dopiero po telefonie Jarka zorientowałem się, że nie jemu podałem kod BLIK tylko innej osobie, która w jakiś sposób pozyskała dane Jarka. Może włamano się do jego komputera, a może do mojego. Nie wiem Szkoda, że wtedy nie pomyślałem, Po prostu byłem naiwny. Powinienem zadzwonić do kolegi i potwierdzić, że to on napisał do mnie tę wiadomość. Nie wiedziałem, że ktoś może podszyć się po niego. Nie wiem w jaki sposób, ale doprowadził do tego, przekonał mnie, że podałem kod do wypłaty. Gdyby przynajmniej byłby to przelew klasyczny, to może zdążyłbym zablokować środki, a tak przepadło. Kto to zrobił? Jak to się mogło właściwie stać?"

Takie pytania pojawiają się coraz częściej, m.in. przy zgłoszeniach o podejrzeniu popełnienia przestępstwa „na BLIKa" (rys. 1)


Prawidlowy numer to

Dnia 19 listopada 2019 18:42 Joanna K napisał(a):

Dobry wieczor,

Dzis o 17:46 z bankomatu Euronet ul. Rynek 29 we Wroclawiu wyludzono ode mnie 1000zl tzw metoda "na blika". Sprawca podszyl sie pod moja kolezanke i napisal na facebooku, ze potrzebuje kod do wykonania transakcji. Jako, ze obie mieszkamy poza Polska, wiem ze czasem miewamy takie problemy, wiec bez zbednych pytan podalam kod. Wiem, moja wina i prawie niemozliwym jest zlapac przestepce, ale mam nadzieje, ze zgloszenie pomoze ostrzec innych. W zalaczaniu zdjecie wykonanej transakcji.

Pozdrawiam,

Joanna K

Rys. 1. Informacja o o podejrzeniu popełnienia przestępstwa „na BLIKa". Źródło: materiały własne.

Sama usługa moim zdaniem jest bardzo wygodna i prosta dla użytkownika. Jest bardzo popularna wśród młodych ludzi. Jest również doskonałym rozwiązaniem dla naszych pociech w przypadku, gdy na wakacjach zabraknie pieniędzy i wystąpi potrzeba szybkiego przelewu. Co wtedy? Prośba o kod BLIK, wynegocjowana kwota i najbliższy bankomat z usługą wypłat BLIK. Istnieje również przelew na telefon BLIK, ale o tym może następnym razem. Wszystko by było dobrze, gdyby wypłatę poprzedził kontakt telefoniczny, np. tak jak w przypadku rozrzutnego kolonisty. Natomiast w sytuacji tylko kontaktu wirtualnego, ryzyko jest wyższe i jak

widać po statystykach, zagrożenie całkiem realne. Wirtualizacja komunikacji jest szybka i wygodna, ale niesie za sobą ryzyko podszycia się pod inną osobę. Przez „pisanego” Messengera przecież nie sprawdzimy, kto jest po drugiej stronie i czy faktycznie jest to nasz znajomy.

Na czym polega przestępstwo „na BLIKa”? Na co zwracać uwagę? Jakie mechanizmy są wykorzystywane przez przestępców?

Użytkownicy szybko przyzwyczaili się do wygody wynikającej z wykorzystywania usług elektronicznych, takich jak: płatności elektroniczne, przelewy, zakupy, wymiana informacji, dzięki łatwości i szybkości dostępu do danych itp.

Cieszymy się z szybkości przeprowadzanych transakcji, z wygody i prostoty ich wykonywania, co w efekcie daje nam sporą oszczędność czasu. Niestety, często zapominamy o tym, że istnieje również ciemna strona sieci. Podszywanie się pod innych, tworzenie „fałszywej” – wirtualnej tożsamości, stało się już tak nagminne, że szanujący się usługodawcy wprowadzili i stale modyfikują procesy personalizacji, tj. zabezpieczenia użytkownika przed niebezpieczeństwami czyhającymi w sieci, również chroniące przed … nim samym. Najprostszym przykładem takich działań jest wprowadzenie przez banki, przy bankowości elektronicznej, dwustopniowego systemu weryfikacji dostępu. Początkowo do zalogowania się do naszych kont wystarczył login i hasło, jednak niefrasobliwość samych użytkowników i w konsekwencji przejmowanie ich tożsamości przez sprawców cyberprzestępstw, doprowadziły do konieczności uszczelnienie tego procesu przez banki. Warto tutaj wspomnieć, iż Policja Dolnośląska w latach 2001-2005 miała duży wkład w przekonanie instytucji bankowych o konieczności poprawy procesu personalizacji, tj. wprowadzenie dwustopniowego procesu weryfikacji tożsamości użytkownika.

Głównym „paliwem” w przestępczości skierowanej przeciwko usługom elektronicznym jest wykorzystanie przez sprawców mechanizmów bazujących na socjotechnice.

W przestępstwie spoofingu, metoda przestępcza polega na podszyciu się pod nadawcę wiadomości e-mail. Musimy pamiętać, że mimo niewzbudzającego podejrzeń adresu e-mail, z jakiego wysyłana jest wiadomość elektroniczna, istnieją narzędzia do stworzenia pozoru rzeczywistego nadawcy, co pozwala sprawcy – autorowi treści, podszyć się pod nadawcę wiadomości i przemycić złośliwy kod w załączniku. Zanim zaczniemy odpowiadać na treści zawarte w takiej wiadomości lub otworzymy załącznik powinniśmy skorzystać z alternatywnego kanału komunikacji, celem ustalenia, że autorem wiadomości jest faktycznie e-mailowy nadawca.

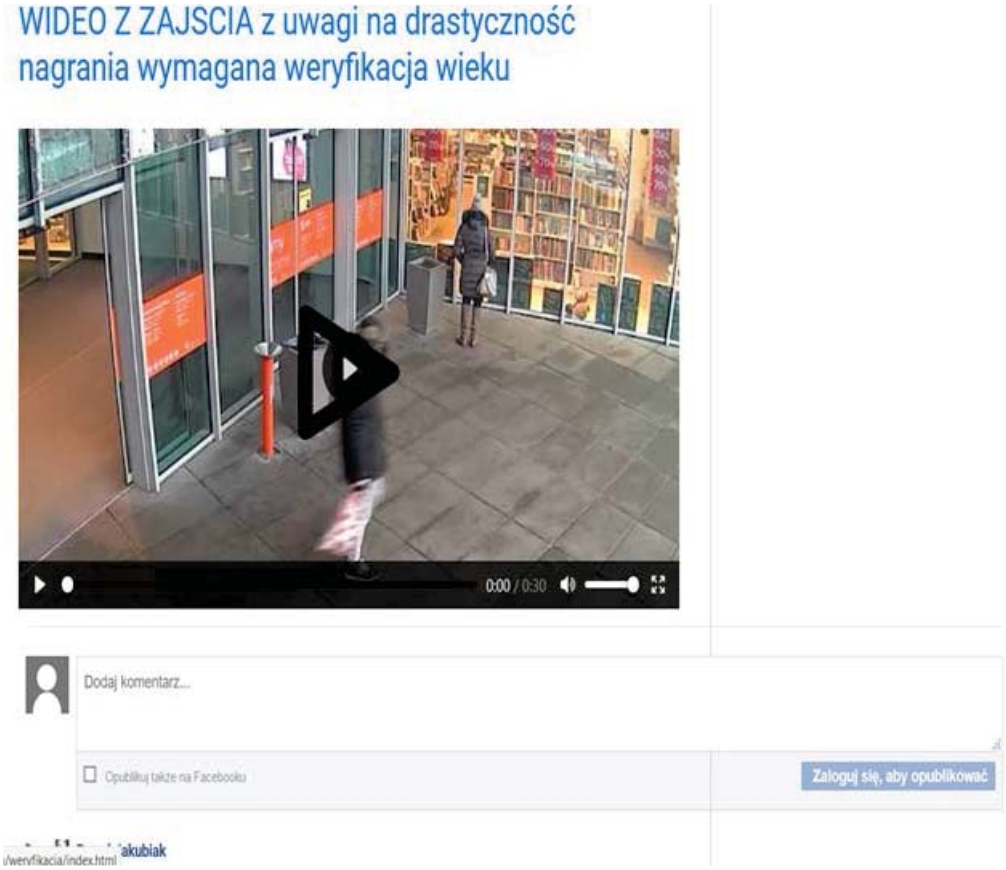
W przypadku komunikatorów internetowych, takich jak np. Messenger trochę inaczej wygląda mechanizm przestępczy. Podszycie się pod autora wiadomości nie jest już takie proste i wymaga wcześniejszego procesu pozyskania danych służących do zalogowania się na Facebooka. W tym przypadku sprawcy również wykorzystują, niestety często z zamierzonym przez

nich efektem, zabiegi bazujące na inżynierii społecznej. Ciekawość użytkownika sieci połączona z brakiem wiedzy na temat aktualnych zagrożeń, jest wstępem do całego łańcucha następujących po sobie okoliczności, które ostatecznie mogą doprowadzić do zachwiania właściwego poziomu bezpieczeństwa „twierdzy" użytkownika.

Przechodząc do sedna, bo przecież ten rozdział powinien być poświęcony przede wszystkim przestępstwu „na BLIKa" przysłowiowym początkiem końca jest przede wszystkim ciekawość użytkownika połączona z wyłączeniem wyobraźni i czasami zdrowego rozsądku. Zaczyna się od odnalezienia jakiejś sensacyjnej wiadomości, często na dziwnym, niesprawdzonym portalu. W wiadomości znajduje się, np. film dotyczący zarejestrowanego kamerą przemysłową porwania kilkuletniego dziecka z galerii handlowej (rys. 2).

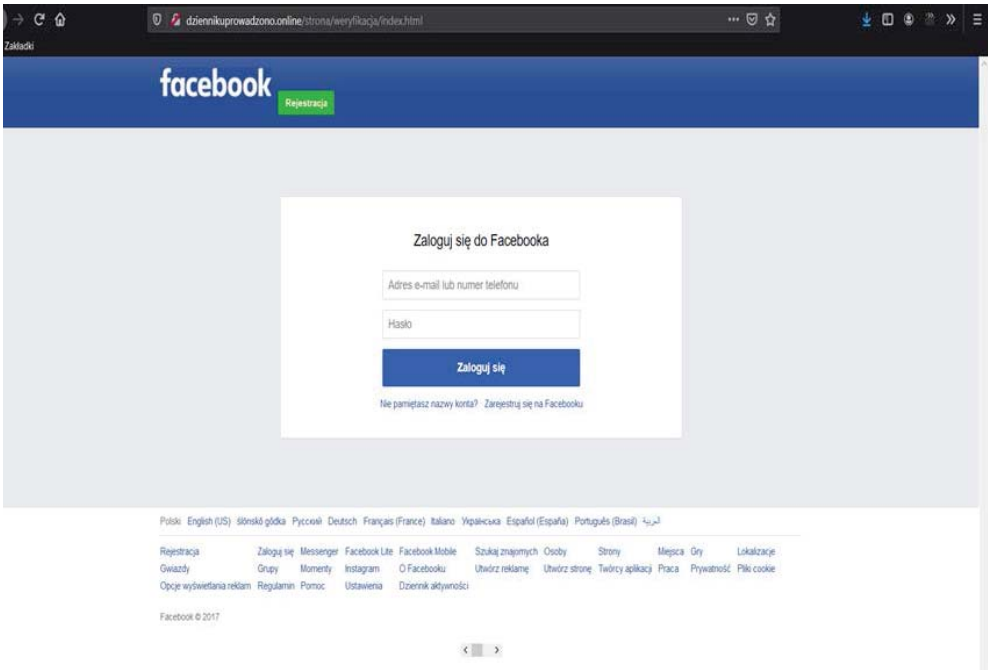
Rys. 2. Przykład sensacyjnej wiadomości wykorzystywanej do popełnienia przestępstwa „na BLIKa". Źródło: materiały własne.

Już w tym momencie powinna nam się zapalić przysłowiowa czerwona lampka, sygnalizująca dziwny adres strony, na której materiał się znajduje. Ciekawość Internauty pcha go jednak dalej, jest zachęcony także do kliknięcia w trójkącik uruchamiający materiał wideo (rys. 3), ale tutaj o dziwo, strona przekierowuje nas w następne miejsce, które ma za zadanie zweryfikowanie naszego wieku.



Rys. 3. Przykład sensacyjnej wiadomości wykorzystywanej do popełnienia przestępstwa „na BLIKa”. Źródło: materiały własne.

Wizualnie wydaje się, że przekierowanie prowadzi do strony logowania na Facebooku. Grafika ta sama, okienka proszące o login i hasło identyczne, nic podejrzanego (rys. 4).



Rys. 4. Fałszywa strona logowania do Facebooka". Źródło: materiały własne.

Wytrawny i ostrożny użytkownik zwróci jednak uwagę, że adres strony wyświetlanej na rys. 4, powiększony na rys. 5 różni się zupełnie od adresu oficjalnej strony (facebook.com). Nie wszyscy jednak tacy rozważni. Wielka szkoda.

Rys. 5. Adres fałszywej strony logowania do Facebooka". Źródło: materiały własne.

I tutaj zaczyna się właściwa aktywność przestępcy. Po pozyskaniu danych (specjalny program zbiera i gromadzi w chmurze dane zawierające loginy i hasła), sprawca loguje się na nasze konto facebook'owe i po analizie treści korespondencji, a ma dostęp do całości, potrafi ocenić nasze zwyczaje, ustalić dane personalne naszych dobrych znajomych i w konsekwencji, bez naszej wiedzy wysyłać do nich różne wiadomości. Również te dotyczące zapytań o nasze dane osobowe, zainteresowania oraz o możliwość pożyczki, tj. przelew BLIK.

Interesującym z punktu widzenia procesowego jest to, że przestępstwo „na BLIKa" wypełnia znamiona dwóch czynów zabronionych: przestępstwa hackingu, tj. wejścia przez

sprawcę bez uprawnień w posiadanie informacji dla niego nieprzeznaczonej poprzez przełamanie lub obejście elektronicznych zabezpieczeń (art. 267 par. 1 KK) oraz przestępstwa oszustwa – wyłudzenia środków finansowych (art. 286 par. 1 KK).

Efekty przestępczej działalności widoczne są przede wszystkim poprzez oddziaływanie na pokrzywdzonych przestępstwem oszustwa. Pokrzywdzony działalnością hackera dowiaduje się, że padł ofiarą dopiero po sygnale od jego znajomych lub od policjanta prowadzącego postępowanie.

Na końcu wypada umieścić podsumowanie. Może lepiej prośbę skierowaną do wszystkich użytkowników sieci. Prośbę o rozwagę połączoną z bardzo umiarkowaną ekscytacją wszystkim, czym karmimy się w Internecie, tj.: „gorącymi” wiadomościami, pogonią za sensacją, usilnym, ale i naiwnym poszukiwaniem znajomych, nierozważną ucieczką przed samotnością, wiarą we wszystko, co przychodzi do nas drogą elektroniczną i zaufaniem w źródło pochodzenia tych wiadomości.

Pamiętajmy również, że wraz ze wzrostem ilości użytkowników sieci Internet, wzrasta również zainteresowanie wszystkim, co jest związane z tym medium przez zorganizowane grupy przestępcze, zachęcone łatwością wprowadzenia w błąd nawet bardzo wytrawnych użytkowników zasobów internetowych. Nie unikajmy relacji face to face, ponieważ to może niekiedy ochronić nas przed czyhającymi niebezpieczeństwami.

ABSTRACT

THE "BLIK" CRIME

Summary: The author of this chapter describes what the "BLIK" crime is about. He draws attention to the characteristic elements of such fraud and presents the mechanisms used by criminals.

Keywords: BLIK, fraud, hacking, identity, spoofing.

ROZDZIAŁ 15

IDENTYFIKACJA OSOBNICZA NA PODSTAWIE CECH CHODU - ANALIZY MORFOMETRYCZNE W OPARCIU O ZAPISY CYFROWE Z MONITORINGU WIZYJNEGO

dr Dorota LORKIEWICZ-MUSZYŃSKA [288]

STRESZCZENIE: W rozdziale przedstawiono zagadnienia dotyczące analiz cech chodu, które mogą dostarczyć dodatkowych użytecznych informacji o osobach zarejestrowanych na nagraniach filmowych. W rozdziale omówiono cechy i cykle chodu, wpływ czynników mogących prowadzić do istotnych zmian w sposobie poruszania się człowieka, zarówno zamian czasowych, jak i stałych. Przedstawiono propozycje analiz morfometrycznych chodu dla potrzeb identyfikacji osobniczej na podstawie filmów i zdjęć cyfrowych. Identyfikacja osób zamaskowanych, a zarejestrowanych w nagraniach z monitoringu, oparta jest na wykorzystaniu cech jakościowych i ilościowych, a metody biometryczne dotyczące cech chodu mogą przyczynić się do identyfikacji widocznych na obrazach osób.

SŁOWA KLUCZOWE: antropologia sądowa, biometria, chód, ichnogram, identyfikacja, zdjęcie cyfrowe, kamery przemysłowe.

1. Wstęp

Wraz z dynamicznym rozwojem technologii kamer i systemów monitoringu wizyjnego nastąpiło ich rozpowszechnienie w miejscach publicznych oraz w obszarach prywatnych, a jakość

[288] Katedra i Zakład Medycyny Sądowej, Pracownia Antropologii i Odontologii Sądowej, Uniwersytet Medyczny w Poznaniu, dlorkiew@ump.edu.pl, +48 602 263 066, ORCID: 0000-0001-8868-8812.

rejestrowanego obrazu podniosła się, co umożliwia rejestrację obrazów z coraz większą dokładnością, lepszą czytelnością szczegółów. Lepsza jakość obrazu to jednocześnie znacznie większe możliwości identyfikacji zarejestrowanych osób, dlatego bardzo często wykorzystuje się zgromadzone w ten sposób informacje do celów śledczych. W praktyce, często jednak zapisy filmowe z monitoringu wizyjnego są słabej jakości, zwłaszcza z uwagi na sposób zamontowania kamery, kąt rejestracji, duży obszar rejestracji, słaby zoom oraz kompresję materiałów filmowych i w efekcie słabą ich rozdzielczość. Skutkuje to znacznymi ograniczeniami w identyfikacji zarejestrowanych na nagraniach osób [289, 290]. Identyfikacja osób zarejestrowanych w materiałach filmowych z monitoringu opiera się na podstawie zespołu cech fizycznych (dotyczących budowy ciała) i behawioralnych (zachowania) człowieka. Najpopularniejsze metody biometryczne wykorzystywane do celów identyfikacyjnych to między innymi badania DNA, daktyloskopia, geometria twarzy, geometria ręki, cechy tęczówki, ale także cechy behawioralne, jak badania głosu czy chodu[291, 292, 293, 294, 295]. W procesie identyfikacji osób zarejestrowanych w nagraniach z monitoringu wizyjnego analiza ciała człowieka, zwłaszcza ocena charakterystyki chodu, może dostarczyć użytecznych informacji pomocnych w dochodzeniu[296]. Chód jako naturalny sposób przemieszczania się człowieka jest jedną z najbardziej złożonych czynności ruchowych wykonywanych przez człowieka na co dzień i jest definiowany jako wzorzec ruchu podczas lokomocji. Jest cykliczną aktywnością ruchową, która polega na powtarzaniu się wzor-

[289] Seckiner D., Mallett X, Roux C., Meuwly D., Maynard P., Forensic image analysis – CCTV distortion and artefacts, Forensic Sci. Int., 285, 2018, ss 77–85.

[290] Lorkiewicz-Muszyńska D., Sidor T., Nie tylko biometria – możliwości identyfikacji osób z zapisów nagrań i monitoringów [w:] J.Kosiński (red.), Przestępczość teleinformatyczna 2015, Szczytno 2015.

[291] Al-Ani MS.,Rajab M.A., Biometrics Hand Geometry Using Discrete Cosine Transform (DCT), Science and Technology, 3(4) 2013.

[292] Gibelli D., Obertova Z., Ritz-Timme S. i wsp., The identification of living persons on images: A literature review, Legal Medicine, 19, 2016.

[293] Minura N., Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification, Machine Vision and Applications, 25, 2004.

[294] Seckiner D., Mallett X, Roux C., Meuwly D., Maynard P., 2018, op. cit.

[295] https://www.statista.com/statistics/938654/north-america-europe-business-use-biometric-authentication-method/, dostęp: 12.11.2019.

[296] Seckiner D., Mallett X, Maynard P., Meuwly D., Roux C., Forensic gait analysis — Morphometric assessment from surveillance footage, Forensic Sci. Int., 2019, 296, ss. 57–66.

ców koordynacyjnych kończyn dolnych oraz towarzyszących im ruchów kończyn górnych, tułowia oraz głowy[297, 298]. Wzorce chodu są badane od wielu już lat. Nie ma wątpliwości co do różnic w cechach chodu między ludźmi. Chód człowieka badany był najpierw w medycynie, był on i jest przedmiotem zainteresowania klinicystów i fizjoterapeutów w celu sprawniejszej diagnostyki i terapii[299, 300, 301]. Zmienność międzyosobnicza cech chodu znalazła także szerokie zastosowanie w identyfikacji kryminalistycznej. Prowadzone przez Stevenage i wsp.[302] dwie dekady temu badania potwierdziły możliwość rozróżnienia różnych wzorów chodu i możliwości identyfikacji osoby na podstawie cech chodu w oparciu o zapisy filmowe z monitoringu[303]. W Wielkiej Brytanii materiały filmowe w celu identyfikacji osób na podstawie chodu są wykorzystywane w sprawach karnych od ponad 15 lat[304, 305, 306], w Danii od ponad 10 lat[307]. Dopuszczenie analizy chodu jako dowodu zostało skrytykowane w Kanadzie, a główne obawy autorów dotyczyły znaczenia wyników ekspertyzy w procesie, rzetelności i naukowych podstaw badań chodu w kryminalistyce oraz niezdolności sądów do oceny ekspertyzy biegłych i wartości dowodowej wniosków[308, 309].

---

297 Contini R., Gage H., Drillis R., 34 - Human Gait Characteristics, Biomechanics and Related Bio-Engineering Topics, Proceedings of a Symposium Held in Glasgow, September 1964, Book 1965, ss. 413 -431.

298 http://www.biomech.pwr.wroc.pl/wp-content/uploads/2019/05/Analiza-chodu-instrukcja-do-%C4%87 wiczenia.pdf.

299 Blanke D. J. , Hageman P.A., Comparison of gait of young men and elderly men, Physical Therapy, vol. 69, no. 2, ss. 144–148, 1989.

300 Johansson G., Visualmotion perception, Scientific American, 232, 1975, ss. 76–88.

301 Whittle M.W., Clinical gait analysis: a review, Human Movement Science, 15, 1996, ss. 369–387.

302 Stevenage S.V., Nixon M.S., Vince K., Visual analysis of gait as a cue to identity, Appl. Cognit. Psychol., 31, 1999, ss. 513–526.

303 Stevenage S.V., Nixon M.S., Vince K., 1999, op. cit.

304 Birch I., Gwinnett C., Walker J., Aiding the interpretation of forensic gait analysis: development of a features of gait database. Sci Justice. 56, 2016, ss. 426–430.

305 Bouchrika I., Goffredo M., Carter J., Nixon M., On using gait in forensic biometrics. J Forensic Sci., 56, 2011; ss. 882–889.

306 Nirenberg M., Vernon W., Birch I., A review of the historical use and criticisms of gait analysis evidence. Sci Justice [Internet]. 2018:1–7. Available from: https://doi.org/10.1016/j.scijus.2018.03.000.

307 Larsen P.K., Simonsen E.B., Lynnerup N., Gait analysis in forensic medicine. J Forensic Sci., 53, 2008, ss.1149–1153.

308 Edmond G., Cunliffe E. Cinderella story? The social production of a forensic "science." J Crim Law Criminol., 106, 2017, ss. 219–275.

309 Cunliffe E., Edmond G. Gaitkeeping in Canada: Mis-Steps in assessing the reliability of expert testimony. Can B Rev. 9, 2013, ss. 327–368.

Dlatego przy dopuszczeniu dowodu z opinii wymaga się od eksperta, aby wykazał się odpowiednim poziomem wykształcenia, wyszkolenia i doświadczenia[310]. Dodatkowo teoria i podstawy naukowe zastosowane przez eksperta muszą być przetestowane, koniecznie określone poziomy błędów i przeprowadzona walidacja danych, opracowane ustandaryzowane protokoły. Powinny być także dostępne recenzowane publikacje na dany temat, a zastosowane techniki zaakceptowane przez społeczność naukową[311]. W opiniowaniu i identyfikacji człowieka na podstawie chodu istotna jest wiedza ekspertów z zakresu anatomii człowieka i wszelkich dysfunkcji układów mogących mieć wpływ na chód człowieka[312, 313]. Analizując bowiem chód człowieka należy rozpatrywać go holistycznie. Ocenę tę należy prowadzić uwzględniając czynniki, które mogą mieć istotny wpływ na zmianę chodu, czasową lub stałą w zależności od rodzaju zaistniałego czynnika zewnętrznego lub wewnętrznego.

Analizy dotyczące cech chodu są nieustannie rozwijane, zarówno w medycynie, biomechanice czy kryminalistyce[314], a wraz z rozwojem technologii pojawiają się nowe możliwości badawcze, ale także krytyczne spojrzenia na identyfikację na podstawie chodu w oparciu o zapisy filmowe.

2. Chód człowieka

Chód jest wynikiem ciągłego współdziałania wielu elementów ruchowych i układów, na które składają się między innymi stan i wytrzymałość układu kostnego, sprawność układu mięśniowego i układu nerwowego. Cechy chodu fizjologicznego zdrowego człowieka wykazują zespół cech wspólnych co do jego wzorca, a jednocześnie charakteryzuje się on dużą zmiennością międzyosobniczą.

Prawidłowy chód charakteryzuje się zespołem cech, jak[315]:

---

[310] Daubert v. Merrell Dow Pharmaceuticals, Inc., in 509, 1993, U.S. 579.

[311] Daubert v. Merrell Dow Pharmaceuticals, 1993, op. cit.

[312] Edmond G., Biber K., Kemp R.I., Porter D., Law's looking glass: expert identification evidence derived from photographic video images, Curr. Issues Crim. Justice 20, 2009, ss. 337– 377.

[313] Seckiner D., Mallett X, Roux C., Meuwly D., Maynard P., 2018, op. cit.

[314] Veres G.V.,Gordon L., Carter J.L., Nixon M.S., , What image information is important in silhouette-based gait recognition? J. Comput. Vision Pattern Recognit. 2004, ss. 776–782.

[315] Rochea J.L, Lowryb K.A, , Vanswearingenc J.M , Brachc J.S , Redferna M.S, Harmonic Ratios: A quantification of step to step symmetry, J Biomech., 46, 2013, ss. 828–831, doi:10.1016/j.jbiomech.2012.12.008.

1. dwunożny – do poruszania się człowiek wykorzystuje obie kończyny dolne jednocześnie;
2. naprzemienny – ruchy kończyn dolnych są zsynchronizowane;
3. skierowany przed siebie;
4. symetryczny – zarówno lewa jak i prawa strona ciała człowieka równo ze sobą współpracują;
5. harmonijny:
   – izometryczny (taka sama długość kroków przy danym tempie chodu);
   – izochroniczny (taki sam czas trwania kroków przy danym tempie chodu);
   – izotoniczny (takie samo napięcie mięśni w obu kończynach dolnych przy danym tempie chodu).

Niewielka asymetria może być obserwowana w cechach chodu zdrowych osób, ale wyraźna asymetria jest na ogół obserwowana u osób z anomaliami rozwojowymi lub nabyta w wyniku różnych patologii (zmiany chorobowe lub urazowe), które pośrednio lub bezpośrednio wpływają na cechy chodu. W literaturze dostępnych jest wiele prac opisujących chód pacjentów z różnymi schorzeniami, jak na przykład choroba Parkinsona, mózgowe porażenie dziecięce, uszkodzenie centralnego układu nerwowego, choroby zwyrodnieniowe, zesztywniające zapalenia reumatoidalne stawów, amputacje kończyn, chorobowe i pourazowe deformacje szkieletowe, czy pacjentów po endoprotezoplastyce stawów[316, 317, 318, 319].
Występowanie asymetrii w zespole cech chodu i budowy ciała ma istotne znaczenie w procesie identyfikacji.

3. Cykl chodu

Chód jest zdefiniowany jako zsynchronizowana sekwencja ruchów ciała człowieka, obejmująca wszelkie zmiany położenia poszczególnych części ciała w zakresie od chwili zetknięcia stopy z podłożem do ponownego zetknięcia tej samej stopy. Podczas chodu jedna ze stóp stale

[316] Baik J.S., Lang A.E., Gait abnormalities in psychogenic movement disorders. Mov. Disord., 22, 2007, ss. 395–399.
[317] Nonnekes J., Ruzicka E., Serranowa T., Reich S.G., Bloem B.R. Hallet M., Funkcional gait dissorders. A sign-based approach, Neurology, 94, 2020.
[318] Baizabal-Carvallo J.F., Alonso-Juarez M., Jankovic J., Functional gait disorders, clinical phenomenology, and classification. Neurol. Sci. 41, 2019, ss. 911–915.
[319] Esqenazi A., Gait Analysis in Lower-Limb Amputation and Prosthetic Rehabilitation, Physical Medicine and Rehabilitation Clinics of North America, 25, 2014, ss. 153-167.

utrzymuje kontakt z podłożem, w przeciwieństwie do biegu gdzie występują fazy podczas których nie występuje stały kontakt stóp z podłożem. Często w definicji odnosi się do kontaktu pięty z podłożem, lecz doświadczenie kliniczne pokazuje jednak, że nie zawsze pierwszy kontakt to pięta (np. pacjenci po udarze, którzy stawiają stopę od palców)[320].

Cykl chodu można podzielić na dwie fazy: podporu, która stanowi około 60% cyklu, oraz przeniesienia – około 40%. Samą fazę podporu podzielono na podpór pojedynczy oraz podpór podwójny, w zależności od tego, czy w danym momencie przeciwna kończyna dolna pozostaje w kontakcie z podłożem, czy nie[321].

Na cykl chodu składają się [322, 323, 324]:

a. Faza podporu, którą można podzielić na 5 etapów:

1. **Początkowa Faza Podporu - Kontakt Początkowy - (Initial Contact)**

Jest to moment zetknięcia stopy z podłożem, trwa bardzo krótko stanowi jednak bazę do dalszego ruchu przetaczania kończyny dolnej nad stopą.

2. **Faza amortyzacji (Loading Responce)**

Faza, której zadaniem jest przyjęcie ciężaru ciała i utrzymanie ruchu w przód.

3. **Środkowa Faza Podparcia (Mid-Stance)**

Środkowa faza podporu. Cały ciężar spoczywa na jednej kończynie dolnej.

4. **Końcowa Faza Podparcia (Terminal Stance)**

Zadaniem tej fazy jest wyprowadzenie środka ciężkości z nad płaszczyzny podporu (czyli wychylenie się poza stopę).

5. **Przed Przeniesieniem (Pre-Swing)**

Faza przejściowa pomiędzy podporem, a przeniesieniem. Stopa jeszcze jest w kontakcie z podłożem, ale już nie ma na niej ciężaru.

b. Faza przenoszenia składa się z trzech etapów:

1. **Początkowe Przenoszenie (Initial Swing)**

---

[320] Baizabal-Carvallo J.F., Alonso-Juarez M., Jankovic J., 2019, op. cit.

[321] Perry J., Burnfield J., Gait Analysis : Normal and Pathological Function., Thorofare, United States, 2012.

[322] Perry J., Burnfield J., 2012, op. cit.

[323] Shahid S., Nandy A., Mondal S., Ahamad M., Chakraborty P., A study on human gait analysis. Natarajan Meghanathan, Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, 2012, ss. 358–364.

[324] Uustal H., Baerga E., Physical Medicine and Rehabilitation Board Review, Demos Medical Publishing, New York, 2004.

Początkowa faza przenoszenia. Reaktywne przeniesienie kończyny nad podłożem. Głównym zadaniem tej fazy jest podciągnięcie stopy w kierunku pozycji neutralnej.

2. Środkowe Faza Przenoszenia (Mid-Swing)

Środkowa faza przeniesienia. Kontynuacja poprzedniej fazy, stopa nadal dąży do pozycji neutralnej w stawie skokowym.

3. Końcowa Faza Przenoszenia (Terminal Swing)

Zaczyna się w momencie przekroczenia przez piszczel linii pionowej.

Budowę ciała i zachowanie zdrowego człowieka charakteryzują niewielkie asymetrie, jak asymetria twarzy czy asymetria parzystych narządów, czy szkieletu. Anomalie rozwojowe lub też nabyte zmiany skutkujące wyraźnymi asymetriami w budowie fizycznej, czy w zachowaniach behawioralnych (np. chód) są cechami indywidualnymi pozwalającymi często na identyfikację[325].

4. Czynniki mające wpływ na chód

Analizy cech chodu człowieka i wpływ czynników na chód należy rozpatrywać w podejściu holistycznym. Ocenę czynników mających wpływ na chód człowieka można podzielić na dwie kategorie:

1: cechy fizyczne, biologiczne danej jednostki

2: czynniki zewnętrzne.

1. Czynniki fizyczne wynikające z właściwości biologicznych jednostki, np.: [326, 327, 328, 329, 330, 331]:

---

[325] Seckiner D., Mallett X, Maynard P., Meuwly D., Roux C., 2019, op. cit.

[326] Ma K., Liu W., Miller P., An evidential improvement for gender profiling, Belief Functions — Theory and Applications, 164, 2012, ss. 29–36.

[327] Yam C., Nixon M.S., Carter J.N., Automated person recognition by walking and running via model-based approaches, Pattern Recognit, 37, 2004, ss. 1057–1072.

[328] Cunha U.V., Differential diagnosis of gait disorders in the elderly, Geriatrics, 43, 1998, ss 33–42.

[329] Whittle M.W., Clinical gait analysis: a review, Hum. Mov. Sci., 15, 1996, ss. 369– 387.

[330] Maddan S., Walker J.T., Mitchell Miller J., The BMI as a somatotypic measure of physique: a rejoinder to Jeremy E.C. Genovese, Soc. Sci. J., 46, 2009, ss. 394–401.

[331] E. McLaughlin, J. Muncie, The Sage Dictionary of Criminology, Sage Publications Ltd, London, 2013.

- genetycznie zdefiniowane cechy wpływające na chód;
  - płeć (ryc. 1);
- epigenetyczne, fenotypowe cechy wpływające na chód, zmiany z wiekiem i zmiany chorobowe i pourazowe;
  - wiek;
  - budowa somatyczna i BMI (Body Mas Index);
  - środek ciężkości;
  - cechy fizyczne stałe i przejściowe (ciąża, zmiana pozycji ciała pod wpływem przenoszonego bagażu, ciężkiego plecaka czy torby) mające wpływ na cechy chodu;
  - szybkość chodu;
  - zmęczenie;
  - zmiany chorobowe, szczególnie przewlekłe;
  - zmiany urazowe wpływające na chód;
  - endoprotezoplastyka, amputacje;
  - nawykowe odruchy;
  - stany emocjonalne umysłu.

2. Czynniki zewnętrzne (Ryc. 1 i 2), np.:
  - odzież – typ odzieży - luźna czy też przylegająca, a wręcz obcisła i krępująca ruchy – może mieć w pływ na sposób poruszania się, ale także ma wpływ na możliwości badawcze;
  - obuwie – płaskie, na obcasie, luźne czy tez ścisłe przylegające do stopy, klapki, sandały;
  - bagaż, plecach itp.; wpływ alkoholu na organizm i chód osoby pod wpływem alkoholu;
  - muzyka – słuchanie muzyki podczas chodu.

Ryc. 1. Kadry pobrane z filmu z widoczną tą samą osobą w ujęciu od przodu: bez kurtki (A) i w kurtce (B). Źródło: opracowanie własne.

Ryc. 2. Kadry pobrane z filmu z widoczną tą samą osobą w ujęciu z profilu w tej samej fazie chodu: bez kurtki (A), w kurtce (B), w kurtce i z torbą (C). Źródło: opracowanie własne.

5. Analiza chodu, materiał badawczy

W zależności od dostępnego materiału badawczego w identyfikacji na podstawie cech chodu człowieka można zastosować różne metody badawcze. Badanie cech chodu człowieka można realizować na podstawie:

1. śladów pozostawionych na podłożu, powstałych w wyniku przemieszczania się człowieka – jak, m.in. śladów bosych stóp, stóp w skarpecie lub rajstopach, stóp obutych;

2. zapisów z monitoringu wizyjnego i wszelkich zapisów filmowych, w których zarejestrowana została sylwetka człowieka podczas chodu w różnych ujęciach.

W każdym z tych obszarów badań celem jest uzyskanie jak najwięcej informacji o osobie i sposobie jej przemieszczania się. Niezależnie czy będą to badania śladów stóp bosych, stóp obutych, a pozostawionych przez człowieka podczas przemieszczania się, czy zarejestrowanego zapisu filmowego przemieszczającej się w chodzie osoby, analiza zabezpieczonych śladów, czy materiałów filmowych, to mogą dostarczyć wiele informacji dotyczących cech grupowych i indywidualnych osoby. Zakres i możliwości badawcze, a następnie identyfikacja osoby zależeć będą od wielu czynników, a analizy dotyczące chodu są bardzo złożone.

6. Ślady stóp bosych, odzianych lub obutych na podłożu

Analiza śladów pozostawionych na podłożu powstałych w wyniku przemieszczania się człowieka może dostarczyć wielu informacji i pozwolić na grupowe bądź indywidualne identyfikowanie człowieka oraz przedmiotu (np. obuwia, skarpety), który ślad pozostawił[332]. Wybór metod badawczych, kierunek badań identyfikacyjnych oraz rodzaj analizowanych cech będzie różny w zależności od podłoża, od tego czy ujawnione zostały ślady stóp bosych, odzianych czy obutych. Ślady mogą dostarczyć informacji czy osoba stała, czy się przemieszczała, mogą być źródłem informacji o dynamice przemieszczania się osoby – czy szła, czy biegła, pozwalają określić kierunek poruszania się oraz sposobu powstawania samego śladu[333, 334]. Badania mogą dotyczyć śladów stóp bosych lub obutych, czy też w skarpecie (rajstopach).

Ślady stóp bosych dotyczyć będą odwzorowania na podłożu poszczególnych części stopy: pięty, zewnętrznej krawędzi śródstopia, sklepienia stopy i palców. Duże znaczenie w identyfikacji mają wszelkie obserwowane anomalie wynikające z wad wrodzonych, rozwojowych czy nabytych. Na identyfikację indywidualną pozwalają linie papilarne, blizny, asymetrie, ubytki.

Ślad stopy odzianej (w skarpę lub rajstopy), umożliwia ustalenie wzoru tkania, określenia grup materiałów z jakiego jest ona wykonana, uszkodzenia i ubytki w materiale itp. Duże możliwości badawcze daje ślad stopy obutej bowiem dodatkowo można dokonać oceny wielu cech obuwia[335].

---

[332] Świętek M., Ekspertyza Traseologiczna, [w:] M. Kała, D. Wilk, J. Wójcikiewicz (red.), Ekspertyza Sądowa, Zagadnienia wybrane, Warszawa 2017, ss. 329 - 346.
[333] Borkowski K., Kryminalistyczna identyfikacja śladów stóp, Warszawa 2013.
[334] Rodowicz L., Kryminalistyczne badanie śladów obuwia, Warszawa 2000.
[335] Rodowicz L., 2000, op.cit.

Informacji o charakterze dynamicznym dostarcza nam tzw. ichnogram, czyli tzw. ścieżka chodu, która obejmuje zespół śladów co najmniej kilku kroków. Na podstawie obrazu chodu można określić wiele elementów dotyczących osoby, która pozostawiła ślad. Elementy te to głównie: kierunek chodu, linia chodu, linia stopy, kąt stopy, kąt kroku, długość i szerokość kroku, oraz długość i szerokość stopy lub podeszwy obuwia, jak również wszelkie asymetrie i odchylenia od normy w sposobie chodu[336].

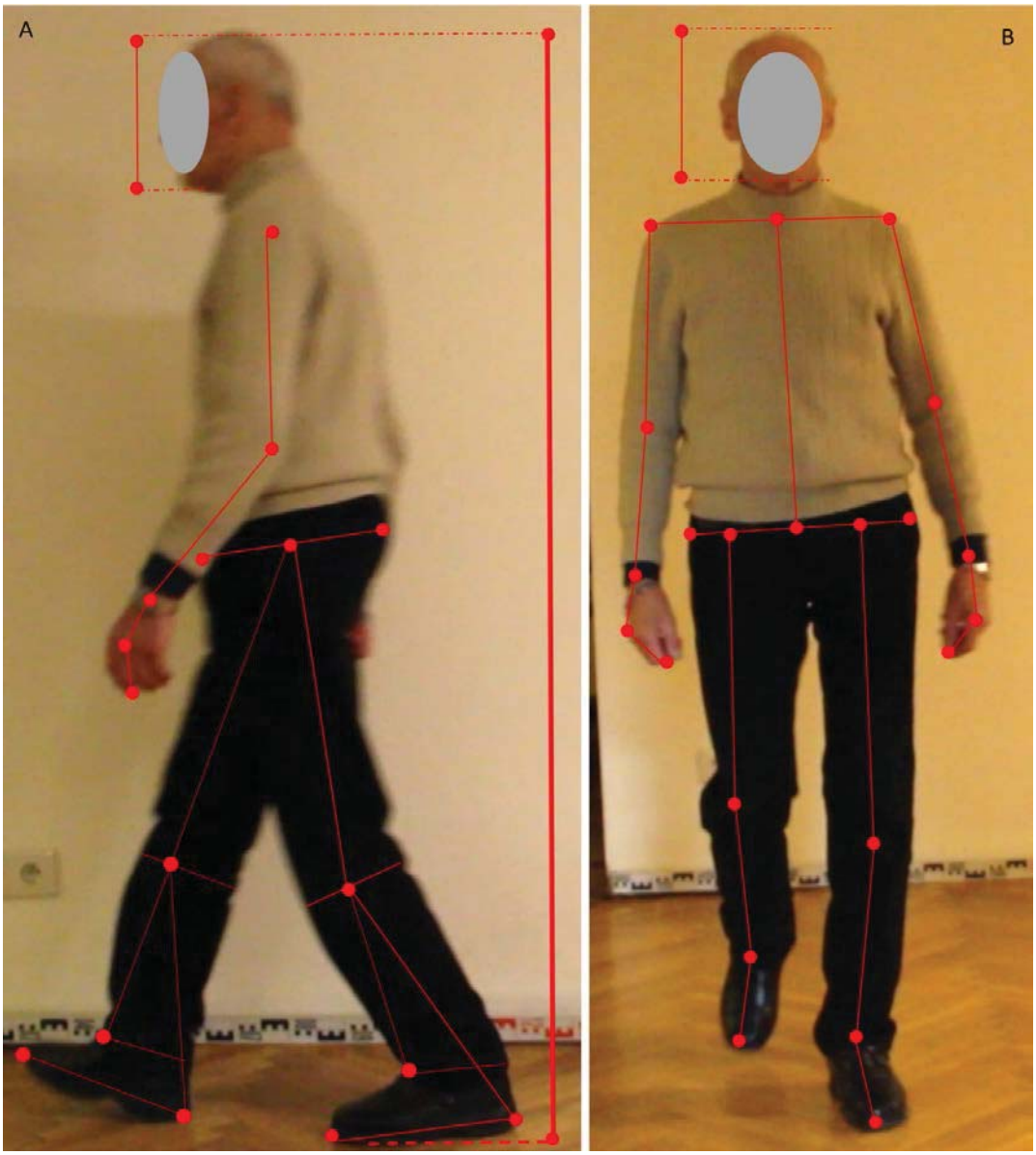
7. Zapisy filmowe osób podczas chodu. Analizy morfometryczne

W przypadku zapisów filmowych i zdjęć osób widocznych podczas chodu prowadzone są obserwacje dotyczące zachowań w czasie przemieszczania się oraz prowadzone są pomiary i obliczenia proporcji analizowane pod kątem cech chodu. Do oceny chodu stosuje się antropometryczne pomiary ciała, tj. cechy statyczne (A) i cechy dynamiczne (B)[337]. Cechy statyczne są zdefiniowane jako geometryczne pomiary ciała, np. długość całej kończyny dolnej osoby i długości poszczególnych jej odcinków, długość całej kończyny górnej osoby i długości poszczególnych jej odcinków itp. Cechy dynamiczne to pomiary związane z chodem, jak oś chodu, kąty stawiania stopy, kąt chodu, odchylenia od pionowej osi ciała, długości kroku i podwójnego kroku (całego cyklu chodu), szerokości kroków, odległości między lewym i prawym palcem (przodem buta) podczas chodu, pomiędzy piętami, odległość między kolanami. Propozycje pomiarów według Seckiner i in.[338] poszerzone o propozycje własne przedstawiono na rycinach 3 i 4. Cechy statyczne oznaczono przez linie i punkty węzłowe koloru czerwonego (ryc. 3), cechy dynamicznie przez linie i punkty węzłowe koloru niebieskiego (ryc. 4). Poprzez pobranie z materiału filmowego kadrów przedstawiających kilka pełnych cykli chodu, nałożenie obrazów metodą superprojekcji możliwe było wyznaczenie ścieżki chodu (ryc. 5). Badania dotyczące chodu muszą być sprzężone z oszacowaniem wysokości osoby badanej. Celem przeprowadzenia badań w kierunku szacowania wysokości ciała i analizy cech chodu konieczne jest przeprowadzenie eksperymentu procesowego z udziałem osoby podejrzanej/oskarżonej z wykorzystaniem tych samych kamer monitoringu. Celem walidacji metody wskazany jest udział pozorantów w eksperymencie. Ważne jest także określenie prędkości z jaką osoba się przemieszczała. Przyjmuje się, że prędkość około 6km/h odpowiada prędkości szybkiego marszu, lecz należy

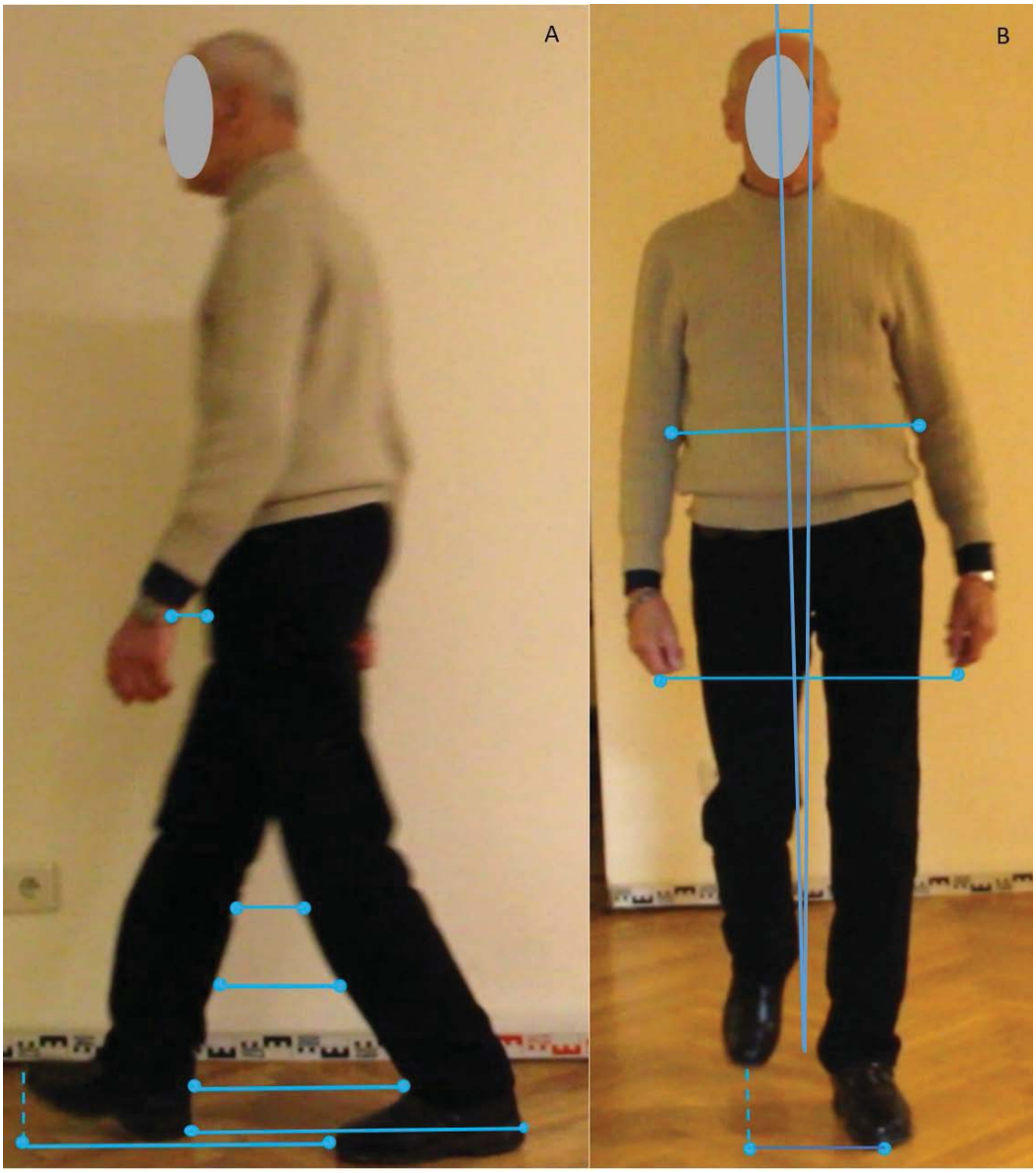
[336] Rodowicz L., 2000, op.cit.
[337] Seckiner D., Mallett X, Maynard P., Meuwly D., Roux C., 2019, op. cit.
[338] Seckiner D., Mallett X, Maynard P., Meuwly D., Roux C., 2019, op. cit.

zwrócić uwagę na wzrost analizowanej osoby. Wysokiemu wzrostowi osoby, zazwyczaj towarzyszą proporcjonalnie dłuższe kończyny dolne. Automatycznie przekłada się to na dłuższy odcinek drogi pokonywanej w jednym kroku przez osobę wysoką, w porównaniu do odległości pokonywanej przez osobę o niższym wzroście (charakteryzującą się mniejszą długością kończyn dolnych). Dynamika chodu także odgrywa istotną rolę w procesie przemieszczania się i chód szybki skutkuje dłuższymi krokami i szybszym przemieszczaniem się. Dlatego podczas eksperymentu należy wykonać pomiary stałych elementów w polu widzenia kamery, wykorzystać narzędzia pomiarowe w celu możliwości określenia długości kroków, ich szerokości, kątów, co pozowali na bardziej precyzyjne analizy i opracowanie ścieżki chodu (ichnogramu) osoby zarejestrowanej w materiale filmowy, należy określić prędkość, z jaką osoba się przemieszczała. Zróżnicowane ujęcia sylwetki podczas chodu pozwalają na precyzyjne obliczenia długości kroku, co wymaga przeprowadzenia pomiarów i wykorzystania narzędzi pomiarowych, np. łaty pomiarowej (ryc. 6).

Możliwości prowadzonych pomiarów cech fizycznych osoby i cech dynamicznych w dużym stopniu zależą od jakości nagrań, sposobu zamontowania kamery, ujęć kamery, zastosowanego zbliżenia, kąta rejestracji, elementów i cech odzieży (luźne, przylegające do ciała), czy osoba idzie z torbą (plecakiem). Znacznie większe możliwości analiz będą możliwe w przypadku materiałów filmowych zarejestrowanych z kilku kamer przedstawiających badaną osobę w różnych ujęciach, w tym od przodu, od tyłu i z profilu.

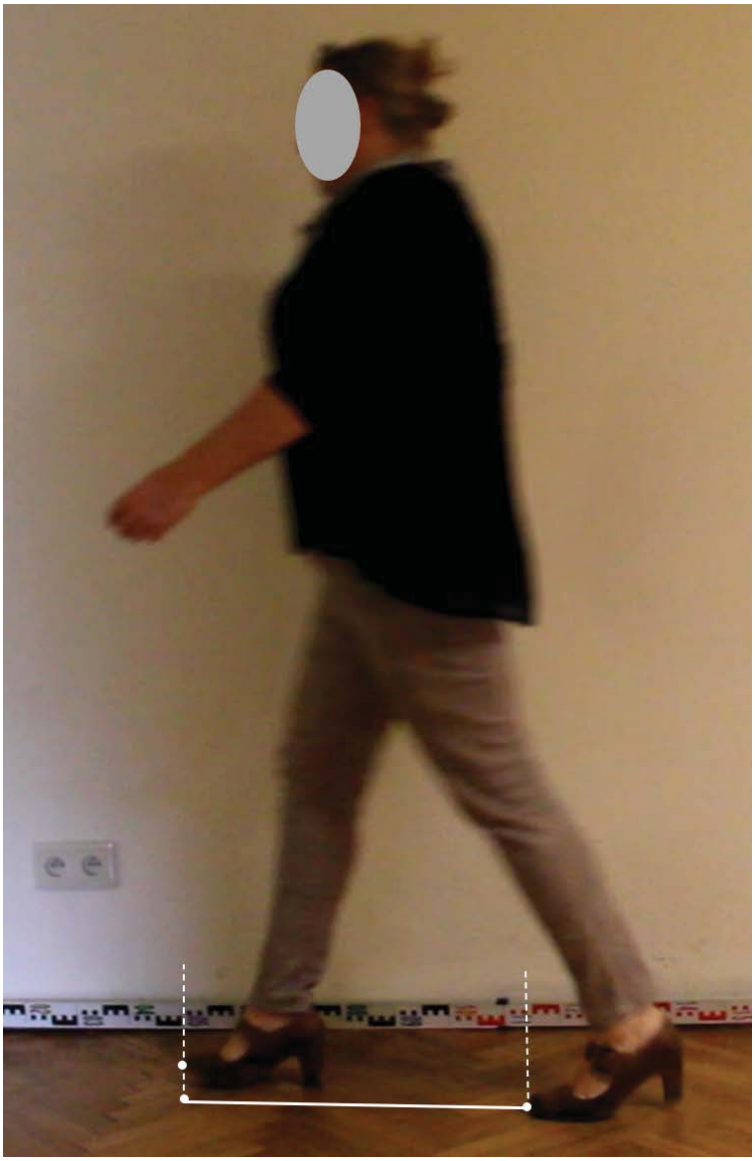


Ryc. 3. Ocena chodu. Wyznaczone pomiary cech statycznych: w ujęciu z profilu (A) i w ujęciu od przodu (B) (propozycja pomiarów wg Seckiner i inni (2019) poszerzona o badania własne). Źródło: opracowanie własne.



Ryc. 4. Ocena chodu. Wyznaczone pomiary cech dynamicznych: w ujęciu z profilu (A) i w ujęciu od przodu (B) (propozycja pomiarów wg Seckiner i inni (2019) poszerzona o badania własne). Źródło: opracowanie własne.

Ryc. 5. Wyznaczenie ścieżki chodu (ichnogram): kierunek chodu, kąty stawiania obytych stóp, szerokość chodu (A-C), superprojekcja kadrów pobranych na trasie przemieszczania się osoby (D). Źródło: opracowanie własne.



Ryc. 6. Wyznaczenie długość kroku w obrębie ścieżki chodu względem łaty pomiarowej. Źródło: opracowanie własne.

Ryc. 7. Ocena chodu. Wyznaczone pomiary cech dynamicznych osoby płci męskiej (A) i osoby płci żeńskiej (B) w ujęciu z profilu, zarejestrowanych z wykorzystaniem tej samej kamery i w tej samej lokalizacji. Obserwuje się zróżnicowanie między płciami i międzyosobnicze w zakresie cech sylwetki oraz cech dynamicznych chodu w tej samej fazie chodu. Źródło: opracowanie własne.

8. Podsumowanie

Rozpowszechnienie wykorzystania systemów monitoringu wizyjnego czy kamer przemysłowych w miejscach publicznych niejednokrotnie przyczynia się do możliwości wykorzystania zapisów i zgromadzonych w ten sposób informacji do celów dochodzeniowych, w tym identyfikacji osób. W aglomeracjach miejskich kamery monitoringu towarzyszą człowiekowi na ulicach, w środkach komunikacji miejskiej, w bankach, centrach handlowych, obiektach sportowych i w wielu innych miejscach. Pozwalają one na ciągłe monitorowanie obszaru, pozwalają na zapis materiału filmowego z możliwością późniejszego ich wykorzystania. Jednocześnie coraz częściej do identyfikacji człowieka wdraża się zaawansowane technologie i systemy, coraz częściej też w systemach identyfikacji i weryfikacji kluczem jest sam człowiek wraz z jego unikalnym zestawem cech mierzalnych, wykorzystywanych w identyfikacji biometrycznej. Do szeroko znanych i dość powszechnie stosowanych, w tym także w użytku prywatnym, danych biometrycznych, jak linie papilarne, geometria twarzy, czy siatkówka oka, dochodzą kolejne sposoby identyfikacji, także cechy behawioralne[339]. Biometria chodu to identyfikowanie człowieka na podstawie sposobu poruszania się. Analizie poddawane są wymiary i proporcje ciała człowieka oraz elementy biomechaniki chodu, takie jak długość i szerokość kroku, kąt układania stopy, nacisk przy stawianiu kroku czy ciężar ciała[340]. Prowadzone obserwacje dotyczące cech chodu, pomiary i analiza proporcji ciała, do tego analiza obrazu ścieżki chodu, czyli ichnogram i wynikające z niego indywidualne cechy, takie jak kierunek i linia chodu, długość i szerokość kroku, zmiany tempa oraz wszelkie asymetrie czy anomalie ruchowe, mogą istotnie przyczynić się do identyfikacji osoby zarejestrowanej w zapisach z kamer monitoringu.

Należy pamiętać również o ograniczeniach jakie mogą pojawić się podczas analiz materiałów filmowych z monitoringu, chociażby z uwagi na różne techniki rejestracji obrazów, zniekształcenia obrazów, jak również wpływ czynników powodujących zmiany podczas poruszania się (w cechach chodu)[341]. W przypadku utrudnień w identyfikacji wynikających z jakości materiałów filmowych, celowego osłaniania twarzy, badania identyfikacyjne należy

---

[339] https://ceo.com.pl/identyfikacja-na-podstawie-biometrii-umozliwi-podrozowanie-bez-dokumentow-potrzebne-sa-jednak-odpowiednie-regulacje-prawne-i-ich-ujednolicenie-92007

[340] https://ceo.com.pl/identyfikacja-na-podstawie-biometrii-umozliwi-podrozowanie-bez-dokumentow-potrzebne-sa-jednak-odpowiednie-regulacje-prawne-i-ich-ujednolicenie-92007

[341] Kavanagh J.J., Barrett R.S., Morrison S. Age-related differences in head and trunk coordination during walking. Human movement science. 2005a; 24:574–587. [PubMed: 16125264].

prowadzić kompleksowo z uwzględnieniem wszystkich możliwych do oceny cech grupowych i indywidualnych. Kompleksowe badania w kierunku zarówno szacowania wysokości osoby (z uwzględnieniem wysokości obuwia, obecnego nakrycia głowy), oceny cech sylwetki (budowy somatycznej, kształtu sylwetki, tułowia, kończyn dolnych i górnych), pomiarów i analizy proporcji ciała, jak również identyfikacji na podstawie ręki i chodu, w znacznym stopniu może poszerzyć i ułatwić identyfikację osoby[342, 343].

9. Literatura

1. Al-Ani M.S., Rajab M.A., Biometrics Hand Geometry Using Discrete Cosine Transform (DCT), Science and Technology, 3(4) 2013.
2. Baik J.S., Lang A.E., Gait abnormalities in psychogenic movement disorders. Mov. Disord., 22, 2007.
3. Baizabal-Carvallo J.F., Alonso-Juarez M., Jankovic J., Functional gait disorders, clinical phenomenology, and classification. Neurol. Sci. 41, 2019.
4. Birch I., Gwinnett C., Walker J., Aiding the interpretation of forensic gait analysis: development of a features of gait database. Sci Justice, 56, 2016.
5. Blanke D. J. , Hageman P.A., Comparison of gait of young men and elderly men, Physical Therapy, 69, 1989.
6. Borkowski K., Kryminalistyczna identyfikacja śladów stóp, Warszawa 2013.
7. Bouchrika I., Goffredo M., Carter J., Nixon M., On using gait in forensic biometrics. J Forensic Sci. 56, 2011.
8. Contini R., Gage H., Drillis R., 34 - Human Gait Characteristics, Biomechanics and Related Bio-Engineering Topics, Proceedings of a Symposium Held in Glasgow, September 1964, Book 1965.
9. Cole S.A., Suspect Identities — A History in Fingerprinting and Criminal Identification, Harvard University Press, Cambridge, 2001.
10. Cunliffe E., Edmond G. Gaitkeeping in Canada: Mis-Steps in assessing the reliability of expert testimony. Can B Rev. 2013, 2.
11. Daubert v. Merrell Dow Pharmaceuticals, Inc., 509, 1993, U.S. 579.

---

[342] Lorkiewicz-Muszyńska D., Sidor T., 2015, op. cit.

[343] Lorkiewicz-Muszyńska D., Rychlik M., Głąbińska M., Wykorzystanie biometrycznej metody identyfikacji ręki na podstawie zdjęć cyfrowych [w:] J.Kosiński (red.), Przestępczość teleinformatyczna 2019, Gdynia 2020, ss. 303-345.

12. Edmond G., Biber K., Kemp R.I., Porter D., Law's looking glass: expert identification evidence derived from photographic video images, Curr. Issues Crim. Justice, 20, 2009.
13. Edmond G., Cunliffe E. Cinderella story? The social production of a forensic "science." J Crim Law Criminol, 106, 2017.
14. Esqenazi A., Gait Analysis in Lower-Limb Amputation and Prosthetic Rehabilitation, Physical Medicine and Rehabilitation Clinics of North America, 25, 2014.
15. Gibelli D., Obertova Z., Ritz-Timme S. i wsp., The identification of living persons on images: A literature review, Legal Medicine, 19, 2016.
16. Kavanagh J.J., Barrett R.S., Morrison S. Age-related differences in head and trunk coordination during walking. Human movement science. 2005a; 24:574–587. [PubMed: 16125264].
17. Johansson G., Visualmotion perception, Scientific American, 232, 1975.
18. Larsen P.K., Simonsen E.B., Lynnerup N., Gait analysis in forensic medicine. J Forensic Sci., 53, 2008.
19. Lorkiewicz-Muszyńska D., Sidor T., Nie tylko biometria – możliwości identyfikacji osób z zapisów nagrań i monitoringów [w:] J.Kosiński (red.), Przestępczość teleinformatyczna 2015, Szczytno 2015.
20. Lorkiewicz-Muszyńska D., Rychlik M., Głąbińska M., Wykorzystanie biometrycznej metody identyfikacji ręki na podstawie zdjęć cyfrowych [w] J.Kosiński (red.), Przestępczość teleinformatyczna 2019, Gdynia 2020.
21. Ma K., Liu W., Miller P., An evidential improvement for gender profiling, Belief Functions — Theory and Applications, 164, 2012.
22. Minura N., Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification, Machine Vision and Applications, 25, 2004.
23. Ng H., Tong H., Tan W., Tzen-Vun Yap T., Chong P., Abdullah J., Human identification based on extracted gait features, Int. J. New Comput. Archit. Appl. 2, 2011.
24. Nirenberg M., Vernon W., Birch I., A review of the historical use and criticisms of gait analysis evidence. Sci Justice [Internet]. 2018:1–7, https://doi.org/10.1016/j.scijus.2018.03.000.
25. Nonnekes J., Ruzicka E., Serranowa T., Reich S.G., Bloem B.R. Hallet M., Funkcional gait dissorders. A sign-based approach, Neurology, 94, 2020.
26. Perry J., Burnfield J., Gait Analysis : Normal and Pathological Function., Thorofare, United States, 2012.
27. Rodowicz L., Kryminalistyczne badanie śladów obuwia, Warszawa 2000.

28. Rushton P., Race, Evolution and Behaviour: A Life History Perspective, Charles Darwin Research Institute, Port Huron, MI, 2000.
29. Seckiner D., Mallett X, Roux C., Meuwly D., Maynard P., Forensic image analysis – CCTV distortion and artefacts, Forensic Sci. Int. 285, 2018.
30. Seckiner D., Mallett X, Maynard P., Meuwly D., Roux C., Forensic gait analysis — Morphometric assessment from surveillance footage, Forensic Sci. Int. 296, 2019.
31. Shahid S., Nandy A., Mondal S., Ahamad M., Chakraborty P., A study on human gait analysis. Natarajan Meghanathan, Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology, 2012.
32. Stevenage S.V., Nixon M.S., Vince K., Visual analysis of gait as a cue to identity, Applied Cognitive Psychology, . 13, 1999.
33. Uustal H., Baerga E., Physical Medicine and Rehabilitation Board Review, Demos Medical Publishing, New York, 2004.
34. Whittle M.W., Clinical gait analysis: a review, Human Movement Science, 15, 1996.
35. Veres G.V.,Gordon L., Carter J.L., Nixon M.S., What image information is important in silhouette-based gait recognition? J. Comput. Vision Pattern Recognit., 2004.
36. https://www.statista.com/statistics/938654/north-america-europe-business-use-biometric-authentication-method/.
37. https://ceo.com.pl/identyfikacja-na-podstawie-biometrii-umozliwi-podrozowanie-bez-dokumentow-potrzebne-sa-jednak-odpowiednie-regulacje-prawne-i-ich-ujednolicenie-92007.

ABSTRACT

GAIT ANALYSIS FOR HUMAN IDENTIFICATION - MORPHOMETRIC ANALYSES BASED ON DIGITAL RECORDS FROM CCTV

Summary: The chapter presents issues related to the analyses of gait features, which may provide additional useful information about recorded people from CCTV. Analysis of the body, especially the assessment of gait characteristics, can provide useful infor-mation to aid the investigation. The chapter discusses the body features and gait cy-cle, the influence of factors that can lead to significant changes in gate features. Pro-posals of gait morphometric analyses for the purposes of individual identification are presented.

Keywords: forensic anthropology, biometry, gait analysis, morphometric assessment, identification, CCTV.

ROZDZIAŁ 16

ANALIZA WYBRANYCH CYBERZAGROŻEŃ W ŚWIETLE TEMATÓW PORUSZANYCH PODCZAS MIĘDZYNARODOWEJ KONFERENCJI CYBERBEZPICZEŃSTWA OBSZARU MORSKIEGO

dr Adam STOJAŁOWSKI [344]

STRESZCZENIE: Celem rozdziału jest przedstawienie wybranych cyberzagrożeń, które mogą wywierać wpływ na bezpieczeństwo systemów teleinformatycznych, powodowanych przez ataki pochodzące z cyberprzestrzeni, jak również analiza wybranych zagrożeń w kontekście zagadnień poruszanych podczas międzynarodowej konferencji cyberbezpieczeństwa obszaru morskiego (the 4th Conference on "Cyber Security in Maritime Domain", 30.09-01.20.2020, Greece).

SŁOWA KLUCZOWE: świadomość sytuacji, cyberbezpieczeństwo obszaru morskiego, bezpieczeństwo systemu teleinformatycznego, cyberzagrożenia, ransomware.

1. Wstęp

Bezpieczeństwo obszaru cyberprzestrzeni wykracza poza ramy zabezpieczenia pojedynczego systemu teleinformatycznego, czy też wielu systemów tworzących mniej lub bardziej złożoną architekturą sieci komputerowej. Cyberbezpieczeństwo coraz częściej pozostaje w centrum zainteresowania już nie tylko wąskiej grupy specjalistów ale ponadto dostawców sprzętu czy usług informatycznych, jak również przedstawicieli instytutów i uczelni wyższych, głównie o profilach technicznych. Dowodzi temu organizowanie szeregu spotkań, konferencji czy treningów międzynarodowych. Jedną z konferencji, którą przywołano w tym opracowaniu była

[344] Regionalne Centrum Informatyki w Gdyni, e-mail: a.stojalowski@gmail.com; ORCID ID 0000-0001-9503-8762.

konferencja „4th NMIOTC Conference on Cyber Security in the Maritime Domain", cyklicznie organizowana przez NATO Maritime Interdiction Operational Training Centre NMIOTC Souda Bay Greece w 2020 roku.

Głównym celem przytoczonej konferencji było zachęcenie do udziału oraz promowanie współpracy naukowej, przemysłowej, morskiej i akademickiej, współpracy z wykonawcami, sztabami marynarki wojennej, członkami istniejących stowarzyszeń, środowiskami akademickimi, przedsiębiorstwami żeglugi, organami normalizacji, w tym departamenty rządowe, organizacje i agencje międzynarodowe, publiczny i prywatny sektor realizujący zadania na rzecz cyberbezpieczeństwa w dziedzinie morskiej oraz operacjach cyberobrony [1].

Dalsza część rozdziału poświęcona zostanie analizie wybranych cyberzagrożeń, w tym również w odniesieniu do tematów poruszonych podczas przywołanej konferencji.

2. Cyberzagrożenia systemów żeglugi morskiej

Systemy teleinformatyczne przeznaczone do wspomagania nawigacji oraz transportu statków żeglugi morskiej są w równym stopniu narażone na cyberataki jak każdy inny system. Jednym z kluczowych systemów zapewniających bezpieczeństwo żeglugi jest System Automatycznej Identyfikacji (AIS), którego przeznaczenie i zadania opisano w Rozdziale 5 dokumentu Bezpieczeństwo żeglugi Konwencji SOLAS [2]. Nie brakuje opinii, w których opis aktualnego stanu bezpieczeństwa systemów żeglugi morskiej pozostaje na poziomie niewystarczającym.

Powyższą problematykę poruszono również w trakcie jednego z paneli wcześniej wspomnianej konferencji, podczas której przedstawiciel Yango Satellite Communications odniósł się do cyberataków przeprowadzonych na infrastrukturę teleinformatyczną statków żeglugi morskiej. Podkreśla się niewystarczającą świadomość w zakresie odpowiedzialności za cyberbezpieczeństwo żeglugi, w szczególności brak lub niewystarczającą implementację mechanizmów bezpieczeństwa w systemach operacyjnych. Zwraca się uwagę na potencjalne zagrożenia wynikające z przełamania zabezpieczeń oraz przejęcie kontroli nad zarządzaniem systemami odpowiedzialnymi za nawigację i ruch statków żeglugi morskiej.

Uzupełniając obszar cyberzagrożeń domeny morskiej warto również odnieść się do bezpieczeństwa systemów nadzorujących przebieg procesu technologicznego (ang. Supervisory Control And Data Acquisition), popularnie nazywanych układami SCADA [3]. Bezpieczeństwo omawianych układów SCADA zostało również poruszone w ramach przywołanej konferencji. Przedstawiciel Aegean University odniósł się do aspektów związanych z systemami kontroli dostępu (ang. Distributed Control System, DCS) na przykładach analizy układów SCADA. Akcentuje się szerokie wykorzystanie układów SCADA z uwzględnieniem nowocze-

snych implementacji w tym w domenie morskiej. Zostało zaprezentowane zestawienie najpopularniejszych podatności oraz konsekwencje wynikające z przeprowadzenia cyberataku ukierunkowanego na przejęcie kontroli zarządzania układami SCADA.

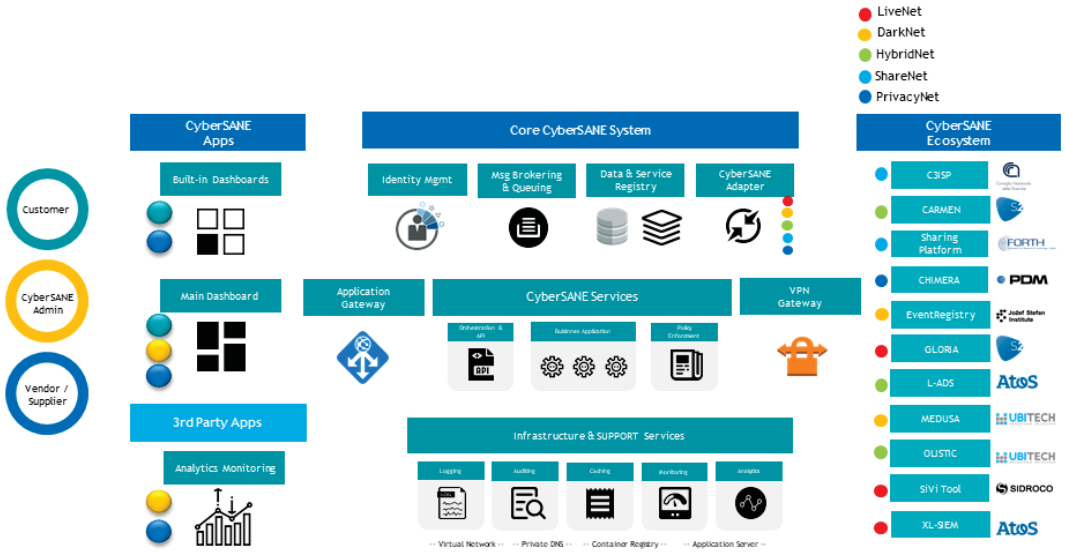
3. Świadomość sytuacji

Dysponowanie wiedzą o aktualnych cyberzagrożeniach wpływających na poziom bezpieczeństwa posiadanego systemu teleinformatycznego jest jednym ze składników przyczyniających się do zmniejszenia ilości potencjalnych incydentów bezpieczeństwa. Świadomość sytuacji jest jednak czymś więcej niż tylko wiedzą o aktualnych cyberatakach. Przywołując publikację Ryszarda Szpyra „Cyberbezpieczeństwo i cyberaktywność militarna", świadomość sytuacji można określić jako postrzeganie i rozumienie bieżącej sytuacji oraz jej przyszłych stanów [4]. Termin świadomości sytuacji został również określony w dokumencie doktrynalnym „Operacje w cyberprzestrzeni DD-3.20", wydanym na podstawie doktryny NATO Allied Joint Doctrine for Cyberspace Operations - AJP-3.20. W przywołanej doktrynie czytamy, że świadomości sytuacji to postrzeganie elementów i zdarzeń środowiskowych w odniesieniu do czasu lub przestrzeni, rozumienie ich znaczenia oraz prognozowanie ich przyszłego stanu [5]. W bieżącym roku (2020) termin świadomości sytuacji został również podniesiony na szczeblu dokumentów strategicznych państwa polskiego – Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020. W przywołanym dokumencie w obszarze celów strategicznych Sił Zbrojnych RP określono potrzebę stworzenia narodowego zintegrowanego systemu świadomości sytuacyjnej, opartego na różnych rodzajach środków rozpoznania, łączności, dowodzenia, w tym krajowych systemach satelitarnej obserwacji Ziemi i systemach bezzałogowych statków powietrznych działających w strukturach sieciocentrycznych, przy zachowaniu pełnego bezpieczeństwa kryptograficznego [6].

Problematykę świadomości sytuacji podniesiono również w ramach konferencji „4th NMIOTC Conference on Cyber Security in the Maritime Domain". Przedstawiciel ACOS MARCOM/N6/Cyberspace zaprezentował wdrożony system świadomości sytuacji w obszarze cyberprzestrzeni (cyber situation awareness). System dostarcza informacje o aktualnych cyberzagrożeniach z podziałem na czterostopniową skalę bezpieczeństwa (low, medium, high, severe). Informacja o zagrożeniach udostępniana jest obiektom pozostającym w obszarze odpowiedzialności Allied Maritime Command (MARCOM) w formie elektronicznych map.

Również w trakcie przedmiotowej konferencji prelegentka z Ubitech Limited omówiła projekt CyberSANE realizowany w ramach funduszy Komisji Europejskiej. Zostały przedstawione główne założenia projektu obejmujące aspekty związane z reagowaniem na incydenty dotyczące morskiej infrastruktury krytycznej. CyberSANE stanowi projekt obejmujący aspekty

odnoszące się do identyfikacji, przeciwdziałania oraz ochrony przed atakami na infrastrukturę krytyczną, oparty na analizie zdarzeń pochodzących z szeregu obszarów: LiveNet, DarkNet, HybridNet, ShareNet, oraz PrivacyNet. Założenia projektu CyberSANE ukierunkowane są na identyfikację ataków poprzez monitorowanie, alarmowanie oraz podejmowanie właściwej reakcji na wykryte zdarzenia.



Rys. 1. Architektura Systemu CyberSANE. Źródło: [7]

4. Cyberzagrożenia w trakcie pandemii COVID-19

Analizując raporty cyberzagrożeń publikowane przez zespoły CSIRT oraz ENISA [8] [9] [10] można zaryzykować stwierdzenie, że średni wzrost incydentów komputerowych z roku na rok przyrasta liniowo. Jest on oczywiście zależny od kategorii incydentów oraz instytucji raportującej zgłaszane zdarzenia. Niewątpliwie na przyrost incydentów bezpieczeństwa ma wpływ rozwój technologii informatycznej oraz skala jej wykorzystania zarówno do celów komercyjnych, publicznych jak i prywatnych.

Wato w tym miejscu odnieść się do obecnej sytuacji oraz poruszyć tematykę związaną z cyberprzestępczością powiązaną z aktualnie trwającą pandemią COVID-19. Można założyć, że podczas tak dużego, masowego zagrożenia życia i zdrowia ludzkiego, główny wysiłek powinien zostać położony na wspomaganie instytucji medycznych. Przyjęcie takiego założenia jest

słuszne pod warunkiem, kiedy rozpatruje się poprawnie przyjęte postawy społeczne. Tymczasem przestępczość komputerowa kieruje się zgoła odmiennym poczuciem wartości.

Problem wykorzystywania aktualnej sytuacji epidemiologicznej został również zauważony w trakcie przywołanej konferencji, podczas której przedstawiciel CyBureau S.R.L odniósł się do znaczącego wzrostu liczby nowo zakładanych domen wykorzystywanych w ramach przestępczości komputerowej. Zauważono stosowanie narzędzi socjotechniki mających na celu wzbudzanie powszechnego strachu podczas prowadzenia kampanii mailowych. Podkreśla się również aspekty odnoszące się do sektora medycznego będącego jednym z głównych obszarów narażonych na cyberataki.

Odnosząc się do raportu ENISA zawierającego przekrój rozpatrywanych cyberzagrożeń, można zauważyć że przewidywania dotyczące ilości wystąpień w obecnej sytuacji kształtują się zgoła odmiennie.

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	⊃	1. Malware	⊃	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	⊃	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	⊃	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	⊃	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	⊃	10. Physical manipulation/ damage/ theft/loss	⊃	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Rys. 2. Przegląd i porównanie zagrożeń występujących w 2018 roku w stosunku do 2017 roku. Źródło: [10]

Powyższe zestawienie (rys. 2), zwłaszcza w części dotyczącej zagrożeń typu ransmomware, wskazuje na tendencję zmniejszania ilości przedmiotowych cyberataków. Tymczasem w ostatnim czasie odnotowuje się znaczący ich przyrost. Można przypuszczać, że niedoszacowanie tych zagrożeń wskazuje na trudności w doborze prawidłowych mierników, jak również mechanizmów warunkujących określenie trendów i przewidywań.

Analiza obecnie odnotowywanych cyberzagrożeń prowadzona pod kątem trwającej pandemii COVID-19, wskazuje na wysokie nasilenie cyberataków mających na celu wymuszenie okupu. Dowodzą temu analizy oraz raporty publikowane przez organizacje i instytucje zajmujących się obserwacją i oceną cyberbezpieczeństwa [11].

Tabela 1. Zestawienie ataków typu ransmoware w dniach 4-5 listopada 2020. Źródło: [12]

--Vermont National Guard Called in to Help with Hospital Recover from Ransomware (November 5, 2020) Vermont's governor has called in the state's Army National Guard's Combined Cyber Response Team to help the University of Vermont Health Network respond to a ransomware attack that affected six area hospitals.
--Brazilian Courts Suffer Ransomware Attack (November 5, 2020) The computer network of Brazil's Superior Court of Justice was the victim of a ransomware attack earlier this week. The country's Secretariat for Information and Communication Technology (STI) is working to recover affected systems. A Brazilian journalist said that other Brazilian government agencies are offline.
--Mattel Discloses Ransomware Attack (November 4, 2020) Toy manufacturer Mattel has disclosed that its network was hit with a ransomware attack in late July. The company revealed the information in a form 10-Q filing with the US Securities and Exchange Commission (SEC).
--Campari Group Network Hit With Ransomware (November 5, 2020) Italian beverage company Campari Group disclosed that ransomware infiltrated its network on Sunday, November 1. The company said that it isolated affected systems and temporarily suspended IT services, and that it plans to wipe and restore affected systems.
--Private Prison Operator Discloses Ransomware Attack (November 5, 2020) A company that operates private prisons says it was the victim of a ransomware attack. GEO Group says that attackers may have stolen data during the incident, which occurred in August 19, 2020. The company's 120 facilities include several US immigration and Customs Enforcement (ICE) detention centers. The information was disclosed in a form 8-K filing with the US Securities and Exchange Commission (SEC).

5. Wnioski

Pomimo wielokrotnie poruszanej tematyki cyberbezpieczeństwa systemów teleinformatycznych wspomagających transport w tym żeglugę morską, nadal podnoszone są apele o zwiększenie bezpieczeństwa omawianych systemów. Szczególnie narażone na cyberataki są niezabezpieczone systemy nawigacyjne, których celowa manipulacja może narazić na poważne konsekwencje w tym prowadzące do niebezpiecznych sytuacji.

Przyczynę niewystarczającego zabezpieczenia systemów wspomagania nawigacji oraz transportu statków żeglugi morskiej postrzega się w dużej skali różnorodności tych systemów często pozostających we wzajemnej niekompatybilności. Ponadto dostrzega się również brak wymaganych umiejętności i wiedzy personelu odpowiedzialnego za bezpieczeństwo tych systemów.

Niewątpliwie do zwiększenia cyberbezpieczeństwa może się przyczynić wprowadzenie systemów świadomości sytuacji. Dostęp do informacji o aktualnych cyberzagrożeniach oraz możliwych przyszłych stanach zagrożeń może stanowić przyczynek do uniknięcia potencjalnie niebezpiecznych sytuacji, jak również wypracować stosowne procedury postępowania.

Poruszone w niniejszym artykule zagrożenia związane z nasileniem ataków typu ransomware podczas trwającej pandemii COVID-19 dowodzą bezwzględności osób wykorzystujących aktualną sytuację do celów przestępczych. Można przypuszczać, że Ilość obserwowanych cyberzagrożeń wykorzystujących podłoże epidemiologiczne skłoni międzynarodowe instytucje do jeszcze większych wysiłków w zwalczaniu przestępczości komputerowej.

6. Bibliografia

1. http://nmiotc.nato.int/transformation/conferences/cyber-security-conference.
2. Międzynarodowa konwencja o bezpieczeństwie życia na morzu, 1974, sporządzoną w Londynie dnia 1 listopada 1974 r., SOLAS, Tekst jednolity 2015, Międzynarodowa Organizacja Morska – IMO.
3. NIST National Institute of Standard and Technology - Special Publication 800-82, Revision 2. Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and Other Control System Configurations such as Programmable Logic Controllers (PLC), May 2015.
4. Banasiński C. (red.), Cyberbezpieczeństwo Zarys wykładu, Wolters Kluwer Polska Sp. z o.o., Warszawa 2018.
5. Operacje w cyberprzestrzeni – DD-3.20, Decyzja Nr 63/SG Ministra Obrony Narodowej z dnia 16.09.2020 r.

6. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.
7. Architecture for an innovative, knowledge-based, and collaborative, security and dynamic response system, https://www.cybersane-project.eu/architecture.
8. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2019 roku, https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/969,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2019-roku.html.
9. Krajobraz bezpieczeństwa polskiego internetu. Raport roczny 2019 z działalności CERT Polska, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.
10. ENISA Threat Landscape Report 2018, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.
11. SANS, Newsletters: NewsBites, https://www.sans.org/newsletters/newsbites.
12. SANS, Newsletters: NewsBites, Volume XXII - Issue #88, https://www.sans.org/newsletters/newsbites/xxii/88.

13. ABSTRACT

ANALYSIS OF SELECTED CYBERSECURITY THREATS IN THE CONTEXT OF THE SUBJECTS OF THE INTERNATIONAL CYBERSECURITY CONFERENCE IN THE MARITIME DOMAIN

Summary: The purpose of this chapter is to present selected cyber threats that may affect the security of ICT systems caused by attacks originating in cyberspace, as well as to analyze selected threats in the context of the subjects raised during the international maritime cybersecurity conference.

Keywords: situation awareness, cybersecurity in the maritime domain, security of the ICT system, cyber threats, ransomware.

communication@formobile-project.eu
Linkedin – Formobile-project
Twitter – @Formobile2019
www.formobile-project.eu

FORMOBILE

What is the FORMOBILE Project?

FORMOBILE is a 3-year research and innovation project addressing the pillar of "Societal Challenges" in the Horizon 2020 framework that funds research, technological development and innovation.

The FORMOBILE consortium includes nineteen institutions, from thirteen European states, and two associated countries. The University of Mittweida is the coordinator of the consortium.

FORMOBILE aims to develop an end-to end forensic investigation chain for mobile devices.

Why FORMOBILE is Relevant

In 2009, the average number of mobile phone subscriptions per 100 inhabitants already stood at 125 in the EU-27. In 2017, altogether 65% of people within the EU used a mobile device to connect to the Internet. In 2020, the figures are even higher. The range of phones are greater and the technologies are more advanced.

[345] This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

There are many challenges related to this area – Law Enforcement Agencies do not have adequate tools to access all smartphones, due to the rise of encryption and more secure interfaces used in today's smart phones.

Moreover, the amount of stored data is rising exponentially. There is a strong need for tools to help in acquisition, decoding and analysis of mobile data. In addition, there is no EU-wide standard covering the forensic analysis of mobile phones. This impedes the exchange of data between the EU member states, and hinders the use of evidence in certain jurisdictions. As a third point, we need better training for LEAs in the field of mobile forensics. Criminals often have specialist knowledge, and to counter-balance this – Law Enforcement require greater numbers of practitioners and experts.

Who will Benefit?

Security Practitioners

FORMOBILE will make your work easier.

Giving access to leading, innovative tools to fight crime and terror. The common standard and supportive training will make you more efficient in your duty. Cooperating with other specialists across the EU will increase security productivity.

Research Groups

Continuing the goal of a united EU.

FORMOBILE is gathering information and knowledge from experts across Europe. The results of the project will pave the way for future advancements - assisting holistic improvement of EU polices.

EU Citizens

Take assurance, work is being done to keep you safe.

Citizens can have confidence work is being done to keep them safe and protect their fundamental rights. FORMOBILE will help fight crime in the short, with overarching goals to deter criminals and terrorists from using mobile technology.

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

What FORMOBILE will Achieve?

Novel tools

Include the acquisition of **previously unavailable mobile data**, unlocking mobile devices, as well as the decoding and analysis of mobile data.

- **Acquisition of mobile data:** the acquisition of RAM memory, the acquisition of cloud storages and the acquisition of counterfeit devices.

- **Decoding mobile data:** decoding tools for mobile data and to overcome security measures like anti-forensic systems.

- **Analysis of mobile data:** new analysis tools for the processing of mobile data to overcome problems that arise with mass data, specifically by doing a semantic analysis and visualization of conversations as well as performing malware analysis on files extracted from Android devices**.**

Standard

The primary purpose is to provide recommendations for a complete forensic investigation chain targeting mobile devices. This covers good practices for the mobile phone forensic process, tools for the successful acquisition, recovery, analysis and visualisation of data; as well as the necessary training required to effectively use the new tools and effectively follow the good practices.

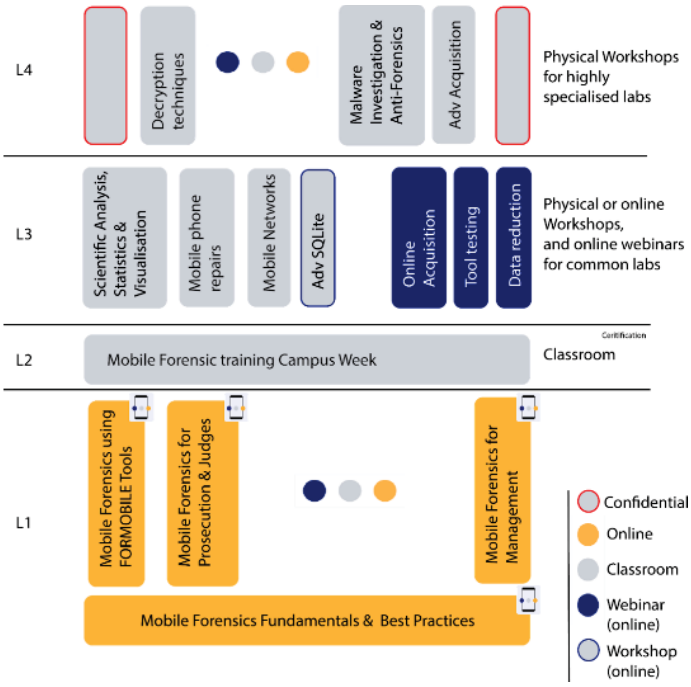
The four areas of critical importance will be addressed in the CWA: **Personnel, Tools, Processes, Legal and Ethical requirements.**

#MobileForensics

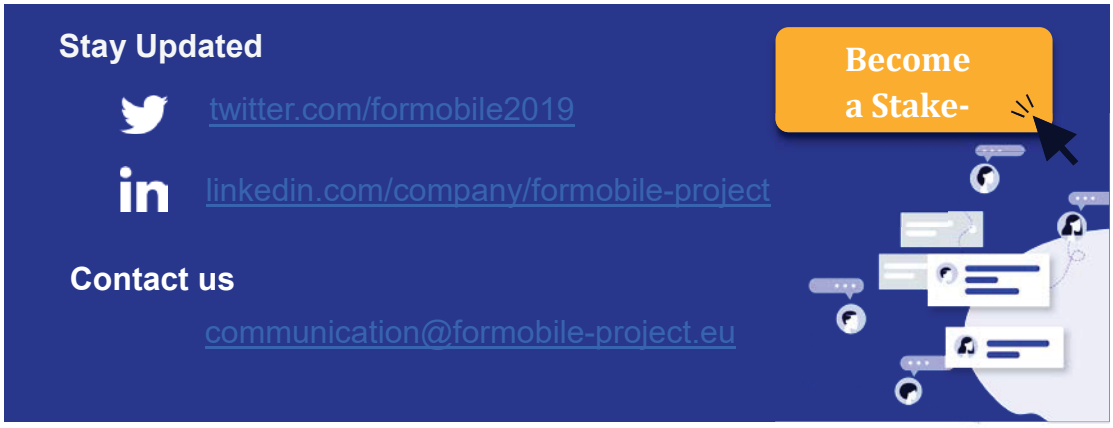
CWA Roadmap

This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800

Training



With the developments of the new standard and the new tools, training for police and criminal prosecution will be established, providing the end users with the latest knowledge in a novel and an innovative curriculum to ensure a quality standard of investigations. A key aim of FORMOBILE is to create an original curriculum developed for law enforcement and legal specialists. The curriculum will address a range of stakeholders, from first responders through to mobile forensic experts. The training will be didactically structured and include unique concepts and approaches taking into consideration differing knowledge bases, and will cover the investigation process, from crime scene to court.



This project has received funding from the European Union's Horizon 2020 – Research and Innovation Framework Programme. H2020-SU-SEC-2018, under grant agreement no.832800