POLSKIE
TOWARZYSTWO
KRYMINALISTYCZNE

Piotr Słowiński

INTERNET RZECZY

KRYMINALISTYCZNA ANALIZA ASPEKTÓW DOWODOWYCH ORAZ STUDIA PRZYPADKÓW

Internet of Things. Evidential forensic analysis and case studies

Warszawa 2020

Piotr Słowiński

INTERNET RZECZY

KRYMINALISTYCZNA ANALIZA ASPEKTÓW DOWODOWYCH ORAZ STUDIA PRZYPADKÓW

Internet of Things. Evidential forensic analysis and case studies

Warszawa 2020

Recenzja
Tadeusz Tomaszewski

Redakcja techniczna
Mieczysław Goc
Kacper Choromański

Korekta przypisów i bibliografii
Anna Kaniewska

Korekta tekstu
Redakcja

Skład komputerowy, projekt graficzny
Mieczysław Goc
Izabela Kułak
Kacper Choromański

ISBN: 978-83-926115-3-0

Wydawca
Polskie Towarzystwo Kryminalistyczne
ul. Zgoda 11 lok. 300
00-018 Warszawa
www.kryminalistyka.pl

Monografia jest publikowana na warunkach licencji
Creative Commons Attribution Non Commercial 4.0 International. (CC BY-NC 4.0)

Spis treści

Przedmowa 6

Rozdział 1. Wprowadzenie 8

Rozdział 2. Internet Rzeczy 12

2.1 Definicja Internetu Rzeczy 12

2.2 Tło historyczne oraz kierunki rozwoju Internetu Rzeczy 15

Rozdział 3. Cyberprzestępczość 22

3.1 Ogólna charakterystyka cyberprzestępczości 22

3.2 Przegląd definicji cyberprzestępczości 23

3.3 Typy i definicja szkodliwego oprogramowania 31

3.4 Wybrane zagrożenia związane z wykorzystaniem Internetu Rzeczy 35

Rozdział 4. Internet Rzeczy a polskie prawo karne 45

4.1 Wprowadzenie 45

4.2 Analiza wybranych przepisów kodeksu karnego 46

4.3 Statystyka wybranych cyberprzestępstw 50

4.4 Kierunki rozwoju 53

Rozdział 5. Internet Rzeczy a kryminalistyka 56

5.1 Podstawy prawne zabezpieczania dowodów cyfrowych 60

5.2 Przegląd wybranych modeli i procedur zabezpieczania dowodów cyfrowych 62

5.3 Ogólne zasady kryminalistycznego zabezpieczania dowodów 65

5.4 Wybrane aspekty zabezpieczania dowodów sieciowych 69

5.5 Modele zabezpieczania dowodów cyfrowych oraz sieciowych w przypadku funkcjonalności Internetu Rzeczy 72

Rozdział 6. Studia przypadków 76

6.1 Wprowadzenie 76

6.2 Urządzenia medyczne 77

6.3 Samochody i akcesoria do pojazdów 82

6.4 Dyn cyber attack 86
Rozdział 7. Zagrożenia i wyzwania 92
7.1 Inteligentne miasta i systemy SCADA 92
7.2 Terroryzm 96
7.3 Międzynarodowe prawo humanitarne – prawo konfliktów zbrojnych 103
7.4 Działalność inspirowana lub sponsorowana przez inne państwa 108
Rozdział 8. Wnioski i postulaty 113
8.1 Sfera prawna 113
8.2 Sfera kryminalistyczna 117
8.3 Uwagi końcowe 118
Bibliografia 121

Przedmowa

Internet jest naprawdę wspaniałym, ale jednocześnie groźnym miejscem. Otwiera nowe możliwości, dostępne na nawet bliżej niż na wyciągnięcie ręki, bo wymagające jedynie kliknięcia. Praktycznie cały świat dostępny z zacisza domowych pieleszy. W jednym momencie możemy porozmawiać ze znajomymi z drugiego końca świata, zaplanować nasze wakacje posiłkując się zdjęciami innych i zrobić niezbędne zakupy, niezależnie od ich rodzaju. Internet jest prawdziwym oknem na świat. Pociąga to jednak za sobą również ogrom ryzyk i zagrożeń. W Internecie każdy może być kimkolwiek, niezależnie od tego jak jest w rzeczywistości. Ze względu na dużą anonimowość oraz niewyobrażalne wcześniej możliwości komunikacji na odległość, zwiększyły się także możliwości przestępców. Rozwój każdej kolejne koncepcji lub rozwiązania niejako może przybliżyć sprawcę do jego ofiary.

Nie inaczej ma się sytuacją z niejako głównym bohaterem niniejszej monografii. Choćby nie było to pierwotnym zamierzeniem twórców i producentów, Internet Rzeczy jest zarówno wspaniałym, i groźnym narzędziem. Ale właśnie – narzędziem? Czy jednak czymś zupełnie innym, pewnym systemem lub całokształtem rozwiązań technicznych? Z punktu widzenia kryminalistyki bliżej mu jednak do narzędzia lub metody działania, czyli *modus operandi*. Sprawca wykorzystując funkcjonalności lub podatności Internetu Rzeczy jest w stanie uzyskać efekt, który byłby trudny do uzyskania przy użyciu innej metody. W niniejszej monografii znajdziecie Państwo rozważania na styku cyberbezpieczeństwa, prawa karnego oraz kryminalistyki uzupełnione o przykłady „z życia wzięte". Urządzenia medyczne wyposażone w możliwość komunikacji bezprzewodowej, samochody zawierające coraz większą liczbę komponentów elektronicznych czy też urządzenia codziennego użytku, mogące posłużyć przestępcom za narzędzie do dokonania ataku na nasz komputer, dom lub szerzej ujmując: życie. Przywykliśmy do obcowania z wieloma różnorodnymi urządzeniami na co dzień, korzystamy z coraz większej liczby przedmiotów, o których często nie wiemy, że posiadają możliwość bezprzewodowej komunikacji z innymi lub zbierania danych o nas jako użytkownikach. Wszechobecność urządzeń i komputerów najprawdopodobniej nie zmieni się. Z dużą dozą prawdopodobieństwa można spodziewać się scenariusza odwrotnego.

Niniejsza monografia ma na celu przekazanie Czytelnikowi wiedzy dotyczącej prawnych oraz kryminalistycznych aspektów Internetu Rzeczy na podstawie polskich

uwarunkowań i specyfiki oraz z punktu widzenia polskiego porządku prawnego. Ponadto, umiejscawia zdarzenia wykorzystujące funkcjonalności lub podatności Internetu Rzeczy w systematyce cyberprzestępczości. Mimo tego, że w wielu miejscach przebrzmiewa negatywny lub zwyczajnie wzbudzający niepokój wydźwięk postępu technicznego to należy zaznaczyć jedno. Internet i nowe technologie są wspaniałymi narzędziami. Prawdziwymi oknami na świat, także dla osób dotychczas częściowo wykluczonych lub odizolowanych od wiedzy i świata. Jeżeli jakąkolwiek nauczkę należy wynieść z nieustającego postępu technicznego, to to że okno działa w obie strony – daje możliwość sięgnięcia za nie na zewnątrz, ale jednocześnie umożliwia tym z drugiej strony na zrobienie tego w stosunku do nas.

Piotr Słowiński

Rozdział 1. Wprowadzenie

Prawdziwa przyszłość komputera przenośnego oparta będzie o ich wykorzystanie w wąskich, specjalistycznych obszarach lub niszach. Ponieważ niezależnie od tego, jak niedrogie staną się te urządzenia i jak rozbudowane lub zaawansowane będzie ich oprogramowanie, wciąż nie wyobrażam sobie, aby przeciętny użytkownik zabierał je ze sobą na ryby.[1]

E. Sanberg-Diment

Cytat rozpoczynający jest ostatnim akapitem artykułu z gazety *The New York Times* z 8 grudnia 1985 r. Rozważania autora skupiają się wokół kwestii, czym w czasach mu współczesnych są komputery przenośne. Jego dywagacje są w dużej mierze krytyczne wobec wytwórców komputerów i marketingowców tychże przedsiębiorstw, czego podsumowaniem i apogeum jest właśnie przytoczony wyżej ostatni akapit artykułu. Nie chcą wdawać się w szczegóły rozważań autora, takie jak wyższość dyskietek nad przenośnym komputerem jako możliwości przenoszenia danych czy też kiepskiej jakości wyświetlaczy ciekłokrystalicznych[2] (w skrócie LCD, ang. *liquid crystal display*), ponieważ z uwagi na rok opublikowania artykułu są one całkowicie zdezaktualizowane. Wartym przytoczenia, z uwagi na temat pracy, jest argument zawarty w przytoczonym wyżej cytacie oraz pojawiający się we wcześniejszej części artykułu. Mianowicie chodzi o fakt, że *kto by chciał móc nosić ze sobą i używać komputer w pociągu lub na plaży na kilka godzin, kiedy zapewne wolałby spędzić ten czas na lekturze sportowych bądź ekonomicznych kolumn gazety* oraz to, że normalny użytkownik przecież nie będzie nosił ze sobą komputera na ryby[3]. Czas pokazał coś zgoła innego, obecnie większość ludzi ma przy sobie choć jeden *komputer przenośny*, czy to w postaci laptopa, czy też telefonu komórkowego, których specyfikacje dorównują niegdysiejszym superkomputerom, zajmującym całe pokoje. W dobie tak dynamicznego rozwoju nowych technik oraz technologii nie sposób już twierdzić, że komputery przenośne stanowić będą jedynie marginalne zjawisko. Szczególnie w obliczu rozkwitu technik komunikacji

---

1 E. Sandberg-Diment, *The executive computer*, „The New York Times", 8 grudnia 1985 r., https://www.nytimes.com/1985/12/08/business/the-executive-computer.html (dostęp: 20.05.2018).

2 Autor używa wręcz określenia *unreadable*, czyli: niepozwalające na odczytanie czegokolwiek, nieczytelne z uwagi na kiepską jakość wyświetlacza – przyp. autor.

3 E. Sandberg-Diment, op. cit.

bezprzewodowej, którego przejawem jest coraz dynamiczniej rozprzestrzeniająca się koncepcja Internetu Rzeczy należy stwierdzić, że twierdzenie te są tym bardziej nieprawdziwe. Wobec oczekiwań sporej grupy konsumentów i w wyniku dążenia producentów do ich zaspokojenia, a także wyjścia im naprzeciw, jesteśmy świadkami coraz intensywniej rosnącej liczby przedmiotów codziennego użytku podłączonych do Internetu, gromadzących i przetwarzających dane. Co więcej, tymi danymi urządzenia są w stanie się wymieniać i to często bez wiedzy użytkownika, choć przy jego zgodzie bądź chociaż przyzwoleniu.

Kryminalistykę na przestrzeni dziejów próbowano określać w różny sposób, jej definicje ulegały zmianom i przemianom charakterystycznym dla rozwoju zarówno świata, jak i nauki. Adekwatnym tego zobrazowaniem będzie przytoczenie dwóch różnych i odległych od siebie o kilkadziesiąt lat definicji. Pierwsza sformułowana przez prof. P. Horoszowskiego brzmi w następujący sposób: *Kryminalistyka bada sposoby i środki dokonywania przestępstw oraz opracowuje metody służące do wykrycia przestępstwa, tudzież do ustalenia i ujęcia sprawcy czynu przestępnego*[4]. Druga natomiast definicja sformułowana została przez prof. T. Hanauska: *Kryminalistyka to nauka o taktycznych zasadach i sposobach oraz o technicznych metodach i środkach rozpoznawania i wykrywania prawnie określonych, ujemnych zjawisk społecznych, a w szczególności przestępstw i ich sprawców oraz udowadniania istnienia lub braku związku pomiędzy osobami i zdarzeniami; a także zapobiegania przestępstwom i innym niekorzystnym, lecz prawnie relewantnym zjawiskom. Nauka ta zajmuje się również strategią przewidywania i przyszłego rozpoznawania oraz zwalczania tych zjawisk, zwłaszcza poprzez zapobieganie ich powstawaniu i rozwojowi*[5]. Mimo, iż definicje te powstały w różnych czasach to posiadają elementy wspólne. Jednak to, co istotniejsze – posiadają elementy różne, które znamionują właśnie czas, jaki upłynął między powstaniem jednej a drugiej. Współczesna kryminalistyka jest definiowana także jako *praktyczna nauka opracowująca zasady sprawnego działania, stosowania taktycznych i technicznych metod śledczych i badawczych wykorzystywanych w celu ujawniania i zabezpieczania faktów mających znaczenie wykrywcze i dowodowe oraz zapobiegania ujemnym zjawiskom społecznym*[6].

---

[4] P. Horoszowski, *Kryminalistyka*, Państwowe Wydawnictwo Naukowe, Warszawa 1958.

[5] T. Hanausek, *Kryminalistyka: zarys wykładu*, Oficyna a Wolters Kluwer business, Warszawa 2009.

[6] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Oficyna Wydawnicza Łośgraf, Warszawa 2011.

Kryminalistyka rozwija się wraz z rozwojem nauki, techniki i technologii, a we współczesnym świecie coraz silniejsze są związki z technologiami informacyjnymi i informatyką. Czy w dobie społeczeństwa informacyjnego, którym niewątpliwie się staliśmy, kryminalistyka, jako nauka mająca najbardziej doniosłe znaczenie w zakresie naukowych metod wykrywania przestępstw i sprawców, jest w odpowiedni sposób przygotowana na czekające ją wyzwania? Czy obecny jej stan jako nauki pozwala kategorycznie stwierdzić, że jest przygotowana na nową erę przestępczości? Czy posiada albo jest w stanie wykształcić instrumenty umożliwiające wypełnianie roli, wynikającej wprost z jej definicji? Na przykładzie nowego, dynamicznie rozwijającego się zjawiska można pokazać jak kryminalistyka jako nauka jest lub w jakim zakresie nie jest w stanie odpowiedzieć na przestępstwa XXI wieku.

Internet Rzeczy dopiero od niedawna postrzegany jest w kontekście zagrożeń związanych z przestępczością jako jeden z możliwych czynników i wektorów wykorzystywanych przez sprawców. Rozważania w tej materii należy podejmować zarówno pod kątem kryminalistycznym, jak również prawnym. Jest to konieczne z uwagi na fakt, iż kryminalistyka ma swoje podstawy w aktach prawnych oraz tworzy z doktryną i praktyką prawną nierozerwalny związek. Dotyczy to takich kwestii jak prawo dowodowe, procedury zabezpieczania potencjalnych dowodów na miejscu przestępstwa, standardów wykonywania ich analizy i sporządzania ekspertyz, a także następnie kwestii oceny zgromadzonego materiału w postępowaniu sądowym. Nie sposób przejść do rozważań pod kątem kryminalistycznym bez uwzględnienia i omówienia wymienionych wyżej kwestii.

Niewątpliwie także wykorzystanie nowoczesnych technik i technologii w działaniach o charakterze terrorystycznym zasługują na zainteresowanie nauki, również z uwzględnieniem możliwości koncepcji IR. Dogłębne omówienie wszelkich kwestii związanych z aspektami kryminalistycznymi, prawnymi oraz technicznymi związanymi z IR nie jest możliwe w ramach jednego opracowania. Sygnalizuje ten fakt już tytuł, sugerujący że będzie to jedynie początek rozważań odnośnie tej koncepcji, a właściwie kryminalistycznego spojrzenia na nią. Rozważania dotyczące cyberprzestępczości, a takimi są kryminalistyczne dociekania nad IR, wymagają odniesienia się w szerokim sensie do informatyki, definiowanej jako *nauka o tworzeniu i wykorzystywaniu systemów komputerowych* albo *szeroko rozumiana działalność informacyjna*[7].

[7] https://sjp.pwn.pl/sjp/informatyka;2561527.html (dostęp 3.02.2020).

Kolejnym z punktów zainteresowania, nieoczywistym wydawać by się mogło na pierwszy rzut oka, będzie sama informacja. W szczególności jej rozumienie pod kątem kryminalistycznym i prawnym, a więc o znaczeniu dowodowym dla procesu karnego i badawczym dla kryminalistyki. W ramach rozważań podjętych w kolejnych rozdziałach należy przyjąć kilka założeń badawczych, pozwalających zasygnalizować kierunek podjętych wstępnych badań nad tematyką Internetu Rzeczy w kontekście kryminalistycznym, ze szczególnym uwzględnieniem możliwości wykorzystania podatności lub funkcjonalności tej koncepcji do popełniania przestępstw. Zakładają one między innymi to, że:

1. Internet Rzeczy nie jest szerzej znany oraz opisany w kontekście kryminalistycznym i prawnokarnym.
2. Brak jest uregulowań w wymiarze doktrynalnym i proceduralnym dotyczących *stricte* Internetu Rzeczy w kontekście ścigania i zapobiegania przestępczości wykorzystującej jego podatności lub funkcjonalności.
3. Brak wiedzy oraz świadomości organów ścigania i wymiaru sprawiedliwości, co do możliwości wykorzystania Internetu Rzeczy do popełniania i zapobiegania przestępczości wpływa na poziom bezpieczeństwa oraz zdolności wspomnianych organów do wypełniania ustawowych zadań.
4. Liczba urządzeń mogących być potencjalnie wykorzystana do popełnienia przestępstw będąca jednocześnie częścią Internetu Rzeczy zwiększa liczbę możliwych do zabezpieczenia dowodów w toku postępowania. Większa liczba dowodów w konsekwencji może prowadzić do zmniejszenia efektywności prowadzonego przez służby śledztwa lub dochodzenia, co może mieć wpływ na skuteczność wykrycia sprawcy.
5. Rozwój Internetu Rzeczy niesie ze sobą poważne zagrożenia dla bezpieczeństwa, szczególnie w kontekście cyberprzestępczości, gdzie atrybucja zdarzeń jest znacząco utrudniona z uwagi na funkcjonalności tej koncepcji oraz wykorzystywane przez sprawców podatności.

Rozdział 2. Internet Rzeczy

2.1 Definicja Internetu Rzeczy

Internet Rzeczy (ang. *Internet of Things*) jest definiowany w dostępnych polskojęzycznych publikacjach jako koncepcja połączenia dwóch światów: wirtualnego i rzeczywistego. Oparta jest ona na trzech filarach odnoszących się do cech inteligentnych obiektów:

- **umożliwienia identyfikacji siebie nawzajem** (wszystko jest w stanie się przedstawić),
- **zapewnienia komunikacji** (wszystko może się komunikować) oraz
- **współdziałania** (wszystko może wzajemnie na siebie oddziaływać)[8],

można się również spotkać z pojęciem, że jest to swego rodzaju ekosystem, w którym wyposażone w sensory przedmioty komunikują się z komputerami[9]. Niezwykle istotna dla tej definicji jest koncepcja działania IR bazująca na trzech pojęciach:

- **zawsze** (ang. *anytime*),
- **wszędzie** (ang. *anyplace*) oraz
- **ze wszystkim** (ang. *anything*)[10].

Ma to na celu zobrazowanie zdolności komunikacyjnych między przedmiotami mogącymi być częścią koncepcji Internetu Rzeczy. Łączność bezprzewodowa, wykorzystująca różnego typu standardy i technologie, ma zapewnić możliwość przetwarzania danych niezależnie od lokalizacji poszczególnych przedmiotów, o ile będą wykorzystywać ten sam rodzaj lub technologię komunikacji. Wszechobecność przedmiotów połączonych ze sobą jest zjawiskiem coraz bardziej powszechnym, ale także niosącym w związku z tym zagrożenia dla prywatności i bezpieczeństwa użytkowników.

O koncepcji Internetu Rzeczy wspomina również J. Kosiński wskazując na zagrożenia wynikające z coraz powszechniejszego występowania urządzeń określanych mianem „smart". Urządzenia codziennego użytku zostają wyposażone w oprogramowanie umożliwiające wysyłanie do nich wiadomości oraz uruchamianie aplikacji, czyli funkcji

---

8 A. Brachman, *Internet przedmiotów – Raport*, Obserwatorium ICT, Technopark Gliwice 2013.

9 *Raport Internet Rzeczy w Polsce*, IAB Polska, 2015.

10 A. Brachman, op. cit.

zarezerwowanych do tej pory dla zupełnie innego typu urządzeń np. komputerów. W rezultacie wskazuje na następujące zagrożenia: braki aktualizacji lub błędy w oprogramowaniu mogą zagrażać bezpośrednio użytkownikowi (życiu i zdrowiu na przykładzie inteligentnego samochodu) albo może narazić byłego użytkownika inteligentnego urządzenia na utratę poufnych danych lub pozwoli na jego sprofilowanie (przy sprzedaży inteligentnego urządzenia)[11]. W. Iszkowski z kolei definiuje zjawisko Internetu przedmiotów (autor używa tego wyrażenia zamiast wyrażenia Internet Rzeczy) w następujący sposób: „pojedyncze systemy wbudowane podłączone przez Internet do wspólnego systemu nimi zarządzającego" lub „dwa systemy współdziałające poprzez aplikacje w chmurach, wraz z trzecim systemem są scalone poprzez zbiór danych, którego analiza pozwala na dodatkowe sterowanie wybranymi systemami". Ponadto wskazuje na następujące cechy, które mają być charakterystyczne dla zjawiska Internetu przedmiotów:

1. Zastosowanie Internetu przedmiotów musi mieć sens i przynosić korzyści osobom i społeczeństwu, które może znajdować się w zasięgu ich działania.
2. Przez przedmioty podłączone do Internetu przekazywane są informacje o czasie i sposobie ich aktywności, ale też mogą to być inne informacje niezwiązane bezpośrednio z zakresem ich działania.
3. Dane (w tym prywatne) zbierane i przekazywane przez Internet przedmiotów mogą być „łatwo" przejęte i wykorzystane.
4. „Darmowe" udostępnianie Internetu przedmiotów może być opłacane danymi z niego pozyskiwanymi.
5. Nie istnieje (jeszcze) oprogramowanie w pełni zabezpieczające przed nieuprawnionym dostępem do przedmiotów podłączanych do Internetu.
6. Nieuprawniony dostęp do przedmiotów podłączonych do Internetu może spowodować przejęcie kontroli nad przedmiotami przez niego sterowanymi, co może mieć negatywny wpływ zdrowotny, ekonomiczny lub psychiczny na osoby przebywające tamże.
7. Przepisy prawne nigdy nie zabezpieczą w pełni osób i społeczeństwa przed nieuprawnionym, szkodliwym wykorzystaniem Internetu przedmiotów przeciwko nim.

[11] J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015.

8. Zabezpieczenie Interesów osób i społeczeństw korzystających z Internetu przedmiotów powinno być wmontowane technicznie w same przedmioty już na etapie ich projektowania.
9. Pełna wiedza o funkcjonalności każdego przedmiotu podłączonego do Internetu powinna być powszechnie dostępna w postaci zrozumiałej dla przeciętnie inteligentnej technicznie osoby.
10. Nie są obecnie znane skutki społeczne i ekonomiczne gwałtownego powszechnego rozwoju zastosowań Internetu przedmiotów.[12]

Celem rozwoju Internetu Rzeczy jest rozbudowanie, a właściwie zdominowanie komunikacji między urządzeniami elektronicznymi przez komunikację typu Maszyna–Maszyna (M2M). Obecnie Internet Rzeczy jest przedmiotem badań głównie z punktu widzenia gospodarki i ekonomii, jako funkcjonalność mająca wzbogacić ofertę producentów sprzętów, co w konsekwencji ma przełożyć się na lepsze wyniki sprzedaży. Niewłaściwemu rozumieniu tej koncepcji oraz zagrożeń z niej wynikających sprzyja również brak jednolitego nazewnictwa w polskojęzycznych publikacjach, jak to zostało zresztą wskazane powyżej. Obecnie w literaturze polskojęzycznej używane są głównie trzy określenia: Internet rzeczy, Internet przedmiotów lub angielska nazwa *Internet of Things*. Wskazana dywersyfikacja określeń tego samego zjawiska nie sprzyja klarowności, naukowemu dyskursowi, a także popularyzowaniu wiedzy dotyczącej bezpieczeństwa Internetu Rzeczy. Na tej kanwie najlepszym postulatem wydaje się być przyjęcie jednej nazwy. Zarówno najbardziej logiczne, jak i najprostsze wydawałoby się stosowanie bezpośrednie tłumaczenie nazwy angielskiej, czyli Internet Rzeczy, zachowując przy tym charakter określenia jako nazwy własnej (zapis obu wyrazów z wielkiej litery). Ponadto niezbędne jest uważne skonstruowanie definicji tej koncepcji, uwzględniającej jednocześnie potrzeby i specyfikę kryminalistyki. Mogłaby brzmieć następująco:

Internet Rzeczy to koncepcja, w której większość lub wszystkie rzeczy codziennego użytku lub po prostu rzeczy, których używamy, są połączone z Internetem i mogą zostać indywidualnie zidentyfikowane przez inne urządzenia bez aktywności człowieka.

[12] W. Iszkowski, *Internet of Things. Systemy wbudowane*, w: G. Szpor (red.), *Internet Rzeczy. Bezpieczeństwo w Smart city*, C.H. Beck, Warszawa 2015.

Występuje ona w postaci jednej wielkiej sieci powiązanych wzajemnie obiektów, komunikujących się ze sobą, wymieniających i zbierających dane[13]

Dopiero taka definicja, zdaniem autora, pozwala na odpowiednie zrozumienie podstawowych zagrożeń oraz potencjalnej problematyki kryminalistycznej wynikającej z rozwoju Internetu Rzeczy.

2.2 Tło historyczne oraz kierunki rozwoju Internetu Rzeczy

W celu lepszego zrozumienia Internetu Rzeczy należy przytoczyć historię jego rozwoju. Przyjmuje się obecnie, że twórcą tego pojęcia jest Kevin Ashton, który sformułował je już w 1999 r. Przewidywał, że okaże się ono jeszcze większą rewolucją niż sam Internet. Zwiększone zainteresowanie tą koncepcją zaczęło się dopiero wiele lat później, na co zwraca uwagę sam Ashton[14]. Skupiono się głównie na możliwym zastosowaniu jej w rozwoju technicznym w celu ułatwienia codziennego życia. Skoncentrowano się więc raczej na biznesowym wykorzystaniu tej nowatorskiej i interesującej koncepcji. W 2010 r. do urządzeń łączących się bezprzewodowo można było zaliczyć już wiele różnego rodzaju przedmiotów m.in. lodówki, mikrofalówki, zegary, kuchenki, ekspresy do kawy, naturalnie komputery wraz z wieloma towarzyszącymi im urządzeniami peryferyjnymi oraz telefony komórkowe. Natomiast w 2015 r. do urządzeń mogących być wykorzystanymi w ramach tej koncepcji można było zaliczyć już nie tylko powyższe, ale także sprzęt medyczny, wszelkiego rodzaju czujniki i systemy monitorowania, np. stanu zdrowia czy lokalizacji zwierząt, a także przedmioty używane do uprawiania sportu, akcesoria rowerowe, samochodowe lub ogrodowe. Oznacza to właściwie większość urządzeń, wyposażonych w możliwość wykorzystania jakiegokolwiek typu komunikacji bezprzewodowej, pozwalającego łączyć się z innymi przedmiotami lub urządzeniami.

Skala i dynamika rozwoju Internetu Rzeczy implikuje potrzebę dopatrywania się ryzyk i zagrożeń dla bezpieczeństwa. Według informacji zamieszczonej w prezentacji

---

[13] P. Słowiński, *Nowe metody popełniania przestępstw na przykładzie rozwoju Internetu Rzeczy,* „Problemy Współczesnej Kryminalistyki" 2016, t. XX.

[14] K. Ashton, *That 'Internet of Things' thing,* „RFID Journal", 22 września 2009 r., http://www.rfidjournal.com/articles/view?4986 (dostęp 31.10.2020).

stworzonej wspólnie przez naukowców z University College London i brytyjskiego Home Office, do 2020 r. liczba urządzeń połączonych ze sobą może wynieść 25 miliardów, prawdopodobnie będzie ona większa.[15] Inne szacunkowe liczby wskazuje natomiast Międzynarodowy Związek Telekomunikacyjny (ang. *International Telecommunication Union*, w skrócie ITU), czyli jedna z organizacji wyspecjalizowanych ONZ odpowiedzialna za standaryzowanie, regulowanie oraz badanie rynku telekomunikacyjnego, teleinformatycznego i informacyjnego (w skrócie ICT, ang. *Information and communications technology*). W swoim raporcie *Measuring the Information Society Report 2015* zebrała różne predykcje odnośnie liczby urządzeń, które można wykorzystać jako część Internetu Rzeczy. Przewidywania te wahały się między 26 a 110 miliardami urządzeń[16]. Niezależnie od tego, która liczba znajdzie swoje odzwierciedlenie w rzeczywistości, należy się spodziewać tendencji rosnącej, jeżeli chodzi o liczbę urządzeń wykorzystywanych w ramach tej koncepcji. Wpływ na to będzie miał zapewne rozwój nowych technik komunikacji bezprzewodowej, sztucznej inteligencji, wykorzystania *big data* oraz potrzeb użytkowników. Jednocześnie należy oczekiwać także zwiększenia różnorodności urządzeń, obiektów i przedmiotów połączonych ze sobą, tak jak to miało miejsce do tej pory.

Jednym z przejawów kierunków rozwoju może być obecnie zyskująca na popularności koncepcja produkcji pojazdów autonomicznych. Mogłyby one przewozić pasażerów bez ingerencji kierowcy lub nawet bez jego obecności w pojeździe. Jak można to sobie wyobrazić, nie ogranicza to liczby komponentów i elementów elektronicznych wykorzystywanych do produkcji, a więc jednocześnie mogących być częścią zjawiska Internetu Rzeczy[17]. Jest wręcz przeciwnie, ponieważ koncepcja autonomiczności pojazdów wymaga implementacji jeszcze większej liczby tzw. elektronicznych modułów sterujących (w skrócie ECU, ang. *electronic control unit*) niż w przypadku samochodów bez tej funkcjonalności. Ich liczba, dodatkowo wyposażonych w opcję komunikacji

---

[15] *Internet of Things. Potential Risk of Crime and How to Prevent It,* UK Home Office and University College London report, London 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/410117/Internet_of_things_-_FINAL.pdf (dostęp 31.10.2020).

[16] *Measuring the Information Society Report 2015*, International Telecommunication Union, 2015, s. 154–155.

[17] X. Krasniqi, E. Hajrizi, *Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles*, „IFAC-PapersOnLine", 2016, t. 49(29), s. 269–274, https://doi.org/10.1016/j.ifacol.2016.11.078 (dostęp 31.10.2020).

bezprzewodowej, rośnie proporcjonalnie w stosunku do liczby autonomicznie obsługiwanych funkcjonalności pojazdu. W naturalny sposób zwiększa to podatność systemów i pojazdów na ataki oraz zwiększa ryzyko dla użytkowników.

Ostatnie badania przeprowadzone wśród brytyjskich sprzedawców sprzętu elektronicznego wykazały, że instrukcje i strony internetowe producentów urządzeń wykorzystujących funkcjonalności Internetu Rzeczy nie zawierają odpowiednich informacji na temat zabezpieczeń. Użytkownikom nie przekazuje się informacji odnośnie zastosowanych zabezpieczeń w sferze sprzętowej oraz oprogramowania, a także informacji czy i jakie stosowane są protokoły do szyfrowania komunikacji z serwerami producenta. Co więcej, rzadko zawierają porady dotyczące tzw. cyberhigieny, która ma na celu zadbanie o prywatność poprzez podejmowanie działań przez użytkownika. Może to obejmować takie działania jak tworzenie silnych, wieloznakowych haseł, stosowanie różnych haseł do różnych serwisów lub choćby stosowanie zabezpieczeń w formie oprogramowania antywirusowego. Ponadto, według badaczy urządzenia przeznaczone dla konsumentów, wykorzystujące funkcjonalności Internetu Rzeczy, nie są zabezpieczone pod kątem *secure by design*. Jest to wymóg, aby już na etapie projektowania oprogramowania urządzeń zapewnić adekwatny poziom bezpieczeństwa użytkownikowi, np. poprzez stosowanie wzorów lub schematów jak najbardziej bezpiecznych kosztem innych funkcjonalności[18]. Jest to znaczące utrudnienie w zapewnieniu ochrony przed zagrożeniami, jeśli producenci i twórcy rozwiązań nie zapewniają adekwatnego standardu, który minimalizowałby możliwość stania się ofiarą przez konsumenta. Niepokojącym jest fakt, iż nie są komunikowane rozwiązania stosowane w urządzeniach, co uniemożliwia weryfikację środków mających zapewnić bezpieczeństwo przetwarzanym danym oraz informacjom, a także innym urządzeniom powiązanym lub połączonym, choćby z tą samą siecią.

Internet Rzeczy to nie tylko urządzenia codziennego użytku. To także tak zwane ICS (ang. *Industrial Control Systems*), czyli systemy kontrolujące i powiązane z nimi urządzenia wykorzystywane do przemysłowego procesu kontroli[19] oraz ich największa część, czyli systemy SCADA (ang. *Supervisory Control And Data Acquisition*). Mogą się

---

[18] J.M. Blythe, N. Sombatruang, S.D. Johnson, *What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?*, „Journal of Cybersecurity" 2019, t. 5(1), https://doi.org/10.1093/cybsec/tyz005 (dostęp 3.02.2020).

[19] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (dostęp 3.02.2020).

różnić między sobą w rozmiarze i ilości (od pojedynczych kontrolerów do wielkich połączonych ze sobą systemów i sieci odpowiadających za kontrolę procesów przemysłowych), zależnie od gałęzi przemysłu oraz konkretnego zastosowania i kontrolowanego procesu. Przykładowo systemy tego typu można wykorzystać, w celu kontrolowania ciśnienie na zaworach w miejskim przedsiębiorstwie wodociągowym, monitorowania przepływ prądu w miejskiej elektrowni, w rafineriach, przedsiębiorstwach produkujących chemikalia, a także w instytucjach lub przedsiębiorstwach zajmujących się przewozem dóbr i ludzi.

Mnogość przedmiotów, urządzeń i komponentów mogących wchodzić w skład Internetu Rzeczy wymaga odpowiedniej uwagi ze strony tak producentów, jak i użytkowników, prawników, przedstawicieli organów ścigania i wymiaru sprawiedliwości, a także i naukowców. Krótka, jednak coraz bardziej dynamiczna historia rozwoju, niczym kula śnieżna staczająca się coraz szybciej ze zbocza góry z każdym kolejnym metrem, sprawia, że należy zwrócić uwagę na możliwe niebezpieczeństwa związane z rozwojem Internetu Rzeczy. Zaniedbanie tego obowiązku, jaki powstaje po stronie wymienionych powyżej podmiotów, może mieć katastrofalne skutki dla każdego z nas w wymiarze indywidualnym, jak i generalnym dla społeczeństwa. Należy zacząć od umiejscowienia omawianego zjawiska w metodologii cyberprzestępczości, co zostanie opisane w następnej części.

Obiekty, które można wykorzystać w ramach koncepcji Internetu Rzeczy są niezwykle różnorodne. Na tyle, że nie sposób je zaklasyfikować w jedną ściśle określoną grupę. Można je jedynie ogólnie określić jako „przedmioty codziennego użytku" bądź jeszcze bardziej ogólnie, biorąc pod uwagę ich funkcję, jako „przedmioty, których używamy". Obecny kierunek rozwoju techniki powoduje, iż w funkcję bezprzewodowego łączenia się z Internetem bywają wyposażone przedmioty takie jak lodówki, czajniki, zabawki, bramy garażowe, samochody oraz wiele innych. Ograniczeniem często bywa już tylko ludzka wyobraźnia i możliwości techniczne. Istotnym jest, że obiekty te mogą być ze sobą połączone lub powiązane np. poprzez jedno konto, uzyskują dostęp do innych urządzeń powiązanych z tym kontem lub po prostu będących połączonych z tym samym modemem Wi-Fi. Do tej pory Internet Rzeczy najczęściej był utożsamiany z nieuniknionym i nieuchronnym rozwojem technicznym prowadzącym do przekształcenia przeciętnego domu, w tzw. Smartdom. Miało to w teorii być znaczącym ułatwieniem w życiu, umożliwiającym kontrolę nad mieszkaniem lub domem niezależnie od naszej

lokalizacji - od ogrzewania po zabezpieczenia antywłamaniowe. Jednak niewiele osób dostrzegało w tym potencjalne zagrożenie dla bezpieczeństwa. Co istotniejsze, nie dostrzegali tego również producenci takich rozwiązań. Wytwarzane przez nich produkty nie posiadały lub dalej nie posiadają zabezpieczeń mogących ochronić użytkowników przed niepożądanymi działaniami osób trzecich. Szczególnie groźnym, jak się wskazuje, byłoby naruszenie bezpieczeństwa informacji – ich poufności, dostępności i integralności. Jest to fundamentalny problem do rozwiązania dla producentów urządzeń[20]. Wątpliwości, co do bezpieczeństwa, także w wymiarze braku wiedzy i stosowanych sposobów oraz środków zabezpieczających, może wpływać albo na niepełne zaufanie użytkowników albo nieadekwatną świadomość społeczną. W wyniku tego stwarza to większe zagrożenie dla prywatności i potencjalnie niesie ze sobą ryzyko narażenia na stanie się ofiarą przestępstwa. Rozwiązania mające być częściami składowymi takich systemów nie były w odpowiedni sposób testowane, m.in. pod kątem zagrożeń związanych z szeroko atakami hakerskimi i działaniem szkodliwego oprogramowania (ang. *malware*). Brak testów wynikać może choćby z braku przyjętych ogólnie standardów przeprowadzania testów na urządzeniach lub przedmiotach koncepcji Internetu Rzeczy [21].

W ostatnim czasie zaobserwować można wzrost zdarzeń – między drugim kwartałem 2020 r. a czwartym 2019 r. nastąpił wzrost ataków wykorzystujących funkcjonalności lub podatności Internetu Rzeczy o 14% (mimo spadku między pierwszym, a drugim kwartałem 2020 r.). Według firmy Symantec w pierwszym kwartale 2020 r. dochodziło średnio do 2,133 ataku związanego z Internetem rzezy dziennie, podczas gdy w drugim kwartale nastąpił spadek – do 1,878 zdarzenia dziennie. Zaobserwowano także spadek miedzy kwartałami w kwestii liczby unikalnych adresów IP dokonujących wspomnianych ataków.[22] W raporcie dotyczącym bezpieczeństwa w Internecie za 2019 r.[23] wskazano, że liczba ataków w 2018 r. (po wzroście liczby zdarzeń w 2017 r.) ustabilizowała się na poziomie 5200 miesięcznie. Najczęstszym źródłem ataków, bo aż w

---

[20] M. Abomhara, G.M. Køien, *Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks*, „Journal of Cyber Security and Mobility" 2015, t. 4(1), https://doi.org/10.13052/jcsm2245-1439.414 (dostęp: 30.04.2018).

[21] S. Higginbotham, *The elephant in the room for IoT security*, Stacey on IoT Blog, 18 kwietnia 2017 r., https://staceyoniot.com/the-elephant-in-the-room-for-iot-security/ (dostęp: 30.04.2018).

[22] https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/threat-landscape-trends-q2-2020 (dostęp 3.02.2020).

[23] *Internet Security Threat Report*, t. 24, Broadcom, luty 2019, https://docs.broadcom.com/doc/istr-24-2019-en (dostęp 31.10.2020).

90% przypadków, były routery i kamery, z czego te drugie stanowiły 15% ogółu zdarzeń, w porównaniu do 3,5% w roku 2017. Najczęstszym zidentyfikowanym według autorów raportu źródłem ataku pod względem geograficznym były Chiny (24%), na drugim miejscu USA (10,1%), a podium zamykała Brazylia (9,8%). Dodatkowym, interesującym aspektem jest to, jakie hasła najczęściej padały ofiarami skutecznego ataku. Królowało w tym hasło „123456" (24,6%), drugim w kolejności przypadkiem był brak hasła (17%), a trzecim najczęstszym – hasło „system" (4,3%). Statystyki pokazują, że zagrożenia rokrocznie, jeśli nie wzrastają to utrzymują się na tym samym wysokim poziomie zagrożenia. Jest to niepokojące, szczególnie w aspekcie jakiego rodzaju hasła (lub kwestia ich braku) zabezpieczają urządzenia, których funkcjonalności lub podatności mogą wykorzystać sprawcy.

Wspomniane powyżej, zaznaczone jedynie szczątkowo, zagrożenia rodzą także problemy natury prawnej – regulacyjnej, prawnokarnej, a także w końcu kryminalistycznej. Pierwszy z problemów powstaje w sferze dopuszczalności przez organy państwowe lub certyfikacji urządzeń mogących wchodzić w skład koncepcji Internetu Rzeczy. Pytanie zasadnicze brzmi czy jakakolwiek certyfikacja powinna mieć miejsce, czy też nie i ewentualnie w jakim zakresie – czy jedynie w sektorach strategicznych dla państwa jak energetyka lub obrona narodowa, czy też szerzej także dla produktów konsumenckich. Drugi problem dotyczyć będzie kwestii odpowiedzialności producentów i użytkowników za szkody powstałe w wyniku korzystania tychże urządzeń lub przestępstw z ich wykorzystaniem. W tej kwestii problematyczne, z punktu widzenia organów ścigania i wymiaru sprawiedliwości, może być aktualność przepisów w stosunku do pojawiających się nowych metod i sposobów popełniania przestępstw. Czy aktualne przepisy karne pozwalają na efektywne ściganie przestępczości? Czy znamiona wskazane w kodeksie adekwatnie odzwierciedlają tak zamierzenia ustawodawcy, jak i rzeczywistość? Ostatnim aspektem jest problem kryminalistycznej analizy technik, taktyk i procedur sprawców nowych, pojawiających się dopiero przestępstw. W tym tych wykorzystujących podatności lub funkcjonalności koncepcji Internetu Rzeczy. W tym kontekście powstaje pytanie – czy organy ścigania są świadome zagrożenia i czy są na nieprzygotowane już w tym momencie? Czy dysponują zapleczem intelektualnym i materiałowym do zwalczania nowych form cyberprzestępczości?

Odpowiedź na powyższe pytania i związane z tym kwestie problematyczne na początku powinny zostać zaspokojone poprzez zdefiniowanie cyberprzestępczości, tak

przez polski jak i międzynarodowy oraz ponadnarodowy porządek prawny. W wyniku tego możliwym będzie umiejscowienie nowego typu zdarzeń – wykorzystujących podatności lub funkcjonalności koncepcji Internetu Rzeczy – w systematyce cyberprzestępczości. To być może umożliwi identyfikacje najbardziej narażonych obszarów i wskazanie możliwych środków łagodzenia negatywnych skutków nowego rodzaju przestępczości metodami już znanymi i skutecznymi wobec innego rodzaju zdarzeń.

Rozdział 3. Cyberprzestępczość

3.1 Ogólna charakterystyka cyberprzestępczości

Cyberprzestępczość jest stosunkowo nowym aspektem przestępczości. Przestępstwa utożsamiane z zakłócaniem przetwarzania danych lub systemów informatycznych istotnie zmieniane lub wprowadzane były do kodeksu karnego w roku 2004[24] oraz 2008[25]. Te lata ukształtowały je w taki sposób, jaki znamy je dziś. Naturalnie cyberprzestępczość to nie jednowymiarowe zjawisko. W potocznym rozumieniu kojarzona jest z wykorzystaniem komputerów do popełniania przestępstw, np. do wysyłania spamu lub szkodliwego oprogramowania, a także do wyłudzania lub kradzieży środków z kont bankowych. W wyniku tego, cyberprzestępczość jest kojarzona głównie z rozwojem i działaniem komputerów. Na gruncie polskiego kodeksu karnego[26] mogą to być jednakże również czyny związane z rozpowszechnianiem lub nagrywaniem materiałów o charakterze pedofilskim np. art. 200a i 200b k.k. czy też szpiegostwem - art. 130 k.k., a konkretnie § 3.

Mimo faktu, że początków koncepcji działania współczesnych maszyn komputerowych można szukać już w latach 30. XX wieku, konkretnie w pracy A. Turinga napisanej w 1936 r.[27], to dla indywidualnego odbiorcy wszechobecność komputerów lub urządzeń o podobnych możliwościach jest zjawiskiem stosunkowo nowym. Nie zagłębiając się w historię i rozwój techniki oraz informatyzacji należy zaznaczyć, że postępował on z każdym rokiem coraz bardziej intensywnie. Ostatnie lata przyniosły nieporównywalnie większy niż we wcześniejszych latach postęp w rozwoju technicznym, szczególnie w kwestii ilości urządzeń elektronicznych wyposażonych w możliwości komunikacji bezprzewodowej lub wykorzystujący któryś z dostępnych standardów tego

[24] Ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. Nr 69, poz. 626).

[25] Ustawa z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. Nr 171, poz. 1056) oraz ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344).

[26] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2020 r., poz. 1444 z późn. zm.).

[27] A.M. Turing, *On computable numbers, with an application to the Entscheidungsproblem*, „Proceedings of the London Mathematical Society" 1937, https://londmathsoc.onlinelibrary.wiley.com/doi/epdf/10.1112/plms/s2-42.1.230 (dostęp: 23.12.2016).

rodzaju komunikacji. Wraz ze wzrostem liczby i typów urządzeń zwiększyło się także spektrum ich możliwości oraz funkcji, a co za tym idzie – także podatności.

Rozwój telefonii komórkowej okazał się jednym z kamieni milowych dla rozwoju technicznego w kwestii mobilności i komunikacji. Przy względnie niewielkiej masie i wielkości telefonów komórkowych połączonej z miniaturyzacją ich podzespołów, urządzenia te były wyposażone w ogromne możliwości techniczne. Nierzadko wcześniej porównywalne możliwości były dostępne tylko dla dysponentów stacjonarnych urządzeń lub stacji roboczych. Rosnąca liczba aplikacji mobilnych i programów także zwiększa spektrum możliwości urządzeń, które prawie każdy z nas ma codziennie ze sobą. Jednakże zarówno postępy w kwestii specyfikacji sprzętu, jak i funkcjonalności oprogramowania niosą za sobą także wzrost liczby potencjalnych błędów, braków w zabezpieczeniach i podatności.

3.2 Przegląd definicji cyberprzestępczości

Rozwój techniczny sprzętu komputerowego oraz sieciowego jak przykładowo Internetu lub infrastruktury przesyłowej, stanowi podstawę i impuls dla ustawodawców krajowych oraz organów unijnych do aktualizowania i dostosowywania prawa. Nie da się zaprzeczyć, że cyberprzestępczość ulega dynamicznym i gwałtownym nierzadko zmianom – są to zmiany możliwe do zaobserwowania na co dzień. Konsekwencją takiego stanu rzeczy jest wiele różnych definicji lub charakterystyk jej specyfiki, o różnych zakresach znaczeniowych i wyróżniających różne główne cechy. Wiele źródeł i dokumentów zawiera definicje cyberprzestępczości. Należy dodać, że wskazana poniżej lista źródeł nie jest wyliczeniem enumeratywnym, jednak przytoczone niżej przykłady można uznać niejako za sztandarowe i ugruntowane w nauce przykłady.

- **Konwencja Rady Europy o cyberprzestępczości**, sporządzona w Budapeszcie dnia 23 listopada 2001 r.[28] wraz z Protokołem dodatkowym do Konwencji Rady Europy o cyberprzestępczości dotyczącym penalizacji czynów o charakterze

[28] Dz.U. z 2015 r., poz. 728.

rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzonym w Strasbourgu w dniu 28 stycznia 2003 r.[29].

- **Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 22 maja 2007 r. – w kierunku ogólnej strategii zwalczania cyberprzestępczości**[30].
- **Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów z 7 lutego 2013 r. – Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń**[31].
- Definicje zebrane na stronie internetowej **Centrum Doskonalenia Obrony Cybernetycznej NATO** (ang. *NATO Cooperative Cyber Defence Centre of Excellence*, w skrócie NATO CCDCOE)[32].
- **Definicja Interpolu**[33]

Konwencja Rady Europy o cyberprzestępczości (dalej jako „Cyberkonwencja") definiuje cyberprzestępczość poprzez wyróżnienie rodzajów zdarzeń, które można określić jako cyberprzestępstwo. Chodzi o przestępstwa: **przeciwko poufności, integralności i dostępności danych i systemów informatycznych**, **komputerowe** takie jak fałszerstwa i oszustwa komputerowe, **wyróżniane ze względu na charakter zawartych informacji** lub **związane z naruszaniem praw autorskich i pokrewnych**. W dużej mierze pokrywa się to z kategoriami przestępstw znanymi i polskiemu porządkowi prawnemu. Wskazany podział nie powinien w tym zakresie budzić większych wątpliwości co do jego zasadności. Zaznaczyć można jedynie brak rozpoznania lub uwypuklenia możliwości wykorzystania cyberprzestępstw jako wsparcia dla innego typu przestępczości kryminalnej, przykładowo przeciwko życiu i zdrowiu. Szczególnie skoro dokonano już rozróżnienia pomiędzy przestępstwami przeciwko poufności, integralności i dostępności danych i systemów, a tymi komputerowymi noszącymi znamiona przestępczości przeciwko mieniu, a konkretnie wykorzystania środków informatycznych do popełniania przestępstw wyrządzających szkodę w mieniu ofiary.

---

[29] Dz.U. z 2015 r., poz. 730.
[30] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267 (dostęp 3.02.2020).
[31] doc. JOIN (2013)1.
[32] https://ccdcoe.org/cyber-definitions.html (dostęp: 03.01.2013).
[33] https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime (dostęp 3.02.2020).

W podobnym duchu określono definicję cyberprzestępczości w Komunikacie Komisji z 22 maja 2007 r. Różnice w stosunku do Cyberkonwencji polegają głównie na tym, że wyróżniono odrębnie kategorię **tradycyjnych form przestępstw z użyciem elektronicznych sieci informatycznych i systemów informatycznych**, obok **publikacji nielegalnych treści w mediach elektronicznych**, przykładowo materiałów o charakterze pedofilskim czy zawierających treści na tle nienawiści rasowej, czy też **przestępstwa typowych dla sieci łączności elektronicznej**, takich jak ataki przeciwko systemom informatycznym, ataki typu DoS (ang. *Denial of Service*) czy hakerstwo[34]. To wyliczenie zdecydowanie bliższe jest duchowi i charakterystyce współczesnej cyberprzestępczości. Wyróżnia i podkreśla najistotniejsze cechy urządzeń i sieci informatycznych, jednocześnie mogących być celem, narzędziem lub środowiskiem ataku lub przestępstwa. Nie jest to wyrażone wprost, jednak możliwe jest wyodrębnienie tychże cech na drodze interpretacji i logicznego rozumowania.

Spośród definicji zebranych na stronie *NATO Cooperative Cyber Defence Centre of Excellence* najbardziej interesującą wydaje się być definicja niemiecka. Określa cyberprzestępstwa jako aktywność przestępczą, do której wykorzystuje się usługi oraz aplikacje w cyberprzestrzeni. Cyberprzestrzeń może być zarówno źródłem, celem lub środowiskiem ataku[35]. Jest to niewątpliwie, jak to zostało już wskazane wyżej, wartościowe rozróżnienie z punktu widzenia kryminalistycznego i zapewnienia bezpieczeństwa. Brakiem w przypadku tej definicji, niepozwalającym na jej pełne zrozumienie bez odwołania się do innych dokumentów, jest brak definicji czym jest cyberprzestrzeń. Zachodzi w ten sposób konieczność odniesienia się do innego źródła, gdzie takowa będzie zawarta. Komplikuje to do pewnego stopnia wykorzystanie definicji niemieckiej w praktyce. Pozytywnym aspektem pozostaje jednak cały czas fakt, że identyfikuje faktyczne i zgodne z aktualnym stanem wiedzy możliwości cyberprzestępczości. Dostrzeżenie, że cyberprzestrzeń (niezależnie od jej definicji) może być źródłem, celem lub środowiskiem ataku lub przestępstwa jest istotna oraz wartościowa. Pozwala to wskazać różnorodne metody popełniania i ścigania przestępstw.

Definicja Interpolu, czyli Międzynarodowej Organizacji Policji Kryminalnej (ang. *International Criminal Police Organization*) definiuje cyberprzestępczość dzieląc ją na dwa rodzaje: **zaawansowane cyberprzestępstwa** (ang. *Advanced cybercrime* albo *high-*

[34] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267 (dostęp 3.02.2020).
[35] https://ccdcoe.org/cyber-definitions.html (dostęp: 3.01.2013).

tech crime), czyli ataki przeciwko sprzętowi oraz oprogramowaniu komputerowemu, oraz **cyberprzestępstwa**, to znaczy „tradycyjne" przestępstwa, które zyskały nowe sposoby dokonania z uwagi na rozwój technologii, w tym między innymi Internetu. Ponadto Interpol wskazuje na takie cechy cyberprzestępczości jak **wygodę i anonimowość**, która zapewnia Internet, a także **brak** jego **zarówno fizycznych, jak i wirtualnych granic**. Ponadto wskazania Organizacji zawierają ocenę jakoby w przeszłości cyberprzestępstw dokonywali raczej indywidualni sprawcy. Przeciwstawia temu pogląd o charakterze predykcyjnym, że w związku ze zmianą skali cyberprzestępczości obecnie zajmują się nią grupy, nierzadko zorganizowane, ukierunkowane na dokonywanie konkretnych zaawansowanych cyberprzestępstw oraz tradycyjnych przestępstw, wykorzystując przy tym zdobycze nowych technologii.

Zdarzenia z tego roku oraz lat minionych pokazują, że rzeczywiście zaobserwować można zdarzenia prawdopodobnie dokonywane przez zorganizowane, ustrukturyzowane grupy cyberprzestępców, które mogą być także finansowanymi przez państwa grupami. Dowodem na to będą między innymi takie ataki jak WannaCry z maja 2017 r.[36] czy NotPetya z czerwca 2017 r[37]. Pierwszy okazał się być niezwykle dotkliwym w skutkach szczególnie dla brytyjskiego *National Health Service*[38]. Drugi z kolei, wbrew pierwotnym wskazaniom okazał się być atakiem mającym na celu zniszczenie danych, a nie tylko ich zaszyfrowanie dla okupu[39]. Ponadto, wskazuje się według informacji z CIA, że sprawcami była grupa hakerów inspirowana lub sponsorowana przez Rosję lub wręcz specjalna grupa GRU, czyli Głównego Zarządu Wywiadowczego – rosyjskiej instytucji wywiadu wojskowego[40]. Niewątpliwie można i należy się spodziewać podobnych w skali ataków w

---

[36] *WannaCry Ransomware*, EUROPOL, https://www.europol.europa.eu/wannacry-ransomware; *WannaCry Ransomware*, CERT.PL, https://www.cert.pl/news/single/wannacry-ransomware/ oraz *WannaCry/Wcry Ransomware: How to Defend against It*, TrendMicro, https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/wannacry-wcry-ransomware-how-to-defend-against-it (dostęp 30.04.2018).

[37] D. Bisson, *NotPetya: Timeline of a Ransomworm*, Tripwire, https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/notpetya-timeline-of-a-ransomworm/ (dostęp 30.04.2018).

[38] *Investigation: WannaCry cyber attack and the NHS*, National Audti Office, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf (dostęp 30.04.2018).

[39] A. Ivanov, *ExPetr/Petya/NotPetya is a Wiper, Not Ransomware*, Securelist, https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/ (dostęp 30.04.2018).

[40] E. Nakashima, *Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes*, „The Washington Post", https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html (dostęp 30.04.2018).

przyszłości, a także rozszerzania działalności zorganizowanych grup hakerskich. Nie wolno jednak deprecjonować lub umniejszać zagrożenia ze strony pojedynczych hakerów lub sprawców. Bywają oni także niezwykle groźni w swojej działalności i na zagrożenie z ich strony także trzeba zwracać uwagę. Ze *stricte* kryminalistycznego punktu widzenia można też zauważyć, że trudności w namierzeniu lub choćby zidentyfikowaniu działalności pojedynczej osoby w przypadku cyberprzestępczości mogą być większe niż w przypadku grupy. Indywidualni sprawcy mogą korzystać z ogólnie dostępnych zbiorów szkodliwego oprogramowania, podczas gdy grupy często rozwijają swoje własne unikalne typy programów oraz techniki i taktyki działania, pozwalające na powiązanie ich z konkretnymi atakami.

Inną kategorią przypisywaną raczej pojedynczym sprawcom aniżeli grupom jest wykorzystywanie dostępnego w otwartych źródłach lub repozytoriach kodów i programów do popełniania przestępstw. Tak, jak można dostrzec wzrost liczby zorganizowanych ataków najpewniej dokonywanych przez grupy sprawców, tak również zaobserwować można używanie szkodliwego oprogramowania przez pojedyncze osoby, nierzadko o nikłych umiejętnościach programistycznych lub wręcz ich pozbawionych. Szczególnym przypadkiem będzie szkodliwe oprogramowanie Mirai. W kwestii ataków z jego wykorzystaniem mowa o szerszej kategorii działań niż tylko pojedyncze zdarzenie. Najbardziej interesującym, w szczególności z punktu widzenia wykorzystania podatności Internetu Rzeczy, jest tak zwany *2016 Dyn cyber attack*. Ten incydent zostanie omówiony szerzej w części poświęconej studiom przypadków (s. 79). Poza wymienionym zdarzeniem oprogramowanie Mirai wykorzystane zostało do innych ataków typu DDoS: na stronę Briana Krebsa[41] (dziennikarza badającego działanie cyberprzestępców) czy też francuski serwis OVH, dostarczający usług hostowania stron internetowych[42].

Powyżej przytoczone definicje pochodzą z dokumentów i źródeł zagranicznych lub międzynarodowych. Część z nich weszła już nawet do polskiego porządku prawnego, jak przykładowo Konwencja Rady Europy o cyberprzestępczości. Wypada jednak również w tym miejscu przytoczyć definicję znajdującą się w polskich oficjalnych dokumentach. W uchwalonej przez Radę Ministrów w dniu 25 czerwca 2013 r. Polityce Ochrony

---

[41] *The internet of stings*, „The Economist", 8 października 2016 r., https://www.economist.com/science-and-technology/2016/10/08/the-internet-of-stings (dostęp 01.10.2019).

[42] D. Bonderud, *Leaked Mirai Malware Boosts IoT Insecurity Threat Level*, Security Intelligence, 4 października 2016 r., https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/ (dostęp 01.10.2019).

Cyberprzestrzeni Rzeczypospolitej Polskiej[43], można odnaleźć definicję cyberprzestępstwa jako ***czynu zabroniony popełnionego w cyberprzestrzeni***. Cyberprzestrzeń na gruncie tego dokumentu definiowana jest jako *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*. Systemy teleinformatyczne to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego[44]. To ostatnie z kolei definiuje się jako urządzenie telekomunikacyjne przeznaczone do podłączenia bezpośrednio lub pośrednio do zakończeń sieci[45].

Dokument ten definiuje cyberprzestrzeń RP jako cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach gdzie funkcjonują przedstawiciele RP. Definicja skonstruowana w tak rozbudowany i szeroki sposób posiada zarówno zalety, jak i wady. Do pierwszej grupy zaliczyć można fakt, iż pozwala na dostosowanie się do zagrożeń niesprecyzowanych jeszcze na etapie powstawania Polityki Ochrony Cyberprzestrzeni RP. Oznacza to, że definicja nie musi być rokrocznie zmieniana z powodu jej zdezaktualizowania. Sprzyja to stabilizacji i pewności prawa – zasady, która w demokratycznym państwie prawa powinna być uznawana za jedną z nadrzędnych.

Wady lub też wątpliwości mimo wszystko pozostają. Przede wszystkim można mieć zarzuty co do zasadności, przynajmniej pod względem funkcjonalnym a nie formalnym, definiowania cyberprzestrzeni i „zamykania" jej w obrębie terytorium jednego państwa, biorąc pod uwagę jej charakter. Z jednej strony jest to jak najbardziej zasadne z formalnego punktu widzenia jurysdykcji państwowej i biorąc pod uwagę polską definicję cyberprzestępczości. Z drugiej jednak rozpatrując kwestię pod kątem funkcjonalnym już z samej natury Internetu wynika, że jej celem jest odrzucenie granic. Przynajmniej w takim znaczeniu, jak to do tej pory były rozumiane, czyli jako konkretnych, materialnych

---

[43] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013.

[44] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. Nr 64, poz. 565, z późn. zm.

[45] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2016 r., poz. 1489, 1579, 1823, 1948, 1954 i 2003).

i dających się ściśle określić terenów. Starając się zrozumieć intencję ustawodawcy to najprawdopodobniej chodzi o położenie serwerów, komputerów bądź urządzeń korzystających z sieci. Należy rozważyć czy tak ograniczony zakres przedmiotowy definicji nie jest wtedy jednak zbyt wąski. Szczególnie uwzględniając specyfikę współczesnej cyberprzestępczości rozumianej szeroko, a nie tylko pod kątem wykorzystania funkcjonalności lub podatności Internetu Rzeczy do popełniania przestępstw.

Kolejną z wad definicji pochodzącej z polskiego źródła jest brak uwzględnienia aspektu dostrzeżonego w definicji niemieckiej, przytoczonej wyżej. Na gruncie literalnego rozumienia polskiej definicji identyfikuje się cyberprzestrzeń jako środowisko w którym atak lub czyn zabroniony następuje. Natomiast nie uwzględnia się jej, przynajmniej nie wprost i *explicite*, jako źródła i celu ataku lub przestępstwa. Brakuje wprost wyrażonego wskazania, że cyberprzestrzeń może być zarówno źródłem, celem, jak i środowiskiem ataku. W wyniku tego wydaje się, że brakuje także uwzględnienia rozróżnienia wyrażonego w definicji Interpolu na zaawansowane cyberprzestępstwa i cyberprzestępstwa *sensu stricto*. Wskazane braki nie powodują braku przydatności i możliwości wykorzystania polskiej definicji. Jednak jako postulat można przyjąć konieczność uzupełnienia jej o wspomniane aspekty. Choćby z uwagi na to, że dobitniej i w pełniejszy sposób oddają charakter współczesnej cyberprzestępczości jako wielowymiarowego i niejednolitego zjawiska. Niewątpliwie wzmocniłoby to zrozumienie definicji, co wsparłoby starania w celu zapobiegania występowania cyberprzestępczości.

W ramach dodatkowych rozważań o dokumentach unijnych należy odnieść się do jednego z nich. Mimo faktu, że Komunikat Komisji z 7 lutego 2013 r. nie zawiera definicji cyberprzestępczości *per se*, to jego treść należy ocenić pozytywnie. Wskazuje strategiczne priorytety Unii Europejskiej mające na celu zapewnienie bezpiecznego i swobodnego korzystania ze środowiska internetowego. Komunikat ma na celu wytyczenie długo- i krótkoterminowych kierunków działania wielu podmiotów, nie tylko instytucji UE, ale też państw członkowskich oraz podmiotów prywatnych. W tekście wymienionych zostało pięć strategicznych priorytetów: osiągnięcie odporności na zagrożenia cybernetyczne, radykalne ograniczenie cyberprzestępczości, opracowanie polityki obronnej i rozbudowa zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony, rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego, a także ustanowienie spójnej

międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE[46]. Ponadto, określono jakie instytucje są odpowiedzialne za realizację wyżej wymienionych kierunków, a w przypadku ich braku określa niezbędne do powołania organy. Dodatkowo, wskazuje rodzaj i liczbę dokumentów niezbędnych do realizacji powyższych priorytetów wraz z formułowaniem wniosków *de lege ferenda*. Spośród nich należy przywołać przewidziane przepisami dyrektywy powołanie w krajach członkowskich organów, których zadaniem byłoby skoordynowanie działań opisanych Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[47], zwanej także dyrektywą NIS, na obszarze jej działania w dziedzinie bezpieczeństwa sieci i informacji.

Dodatkowo powołany ma być organ funkcjonujący jako punkt kontaktowy w zakresie komunikacji międzynarodowej oraz krajowy punkt kontaktowy w dziedzinie realizacji postanowień dyrektywy NIS. Nie ma przymusu ani obowiązku powoływania nowej instytucji. Istnieje możliwość powierzenia tychże funkcji już istniejącej. W zakresie realizacji własnych zadań miałby również obowiązek odgrywania roli swoistego łącznika między organami krajowymi a siecią zespołów CSIRT (zespół reagowania na incydenty komputerowe, ang. *Computer Security Incident Response Team*)[48], powołanymi na mocy postanowień dyrektywy sieciami współpracy[49]. Częściowy wyraz znaczenia i doniosłości Komunikatu jest fakt, że część wspomnianych wyżej aspektów została zawarta w ustawie o krajowym systemie cyberbezpieczeństwa[50] mającej realizować i implementować postanowienia dyrektywy NIS.

Powyżej dokonany przegląd definicji odnosił się do źródeł i dokumentów międzynarodowych i unijnych, wynikających z ustaleń pomiędzy różnymi instytucjami i krajami. Natomiast w dyskursie naukowym funkcjonują różne definicji, zarówno starsze i nowsze, te bardziej ogólne, jak i szczegółowe. Spośród wielu funkcjonujących

---

[46] doc. JOIN (2013)1.

[47] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016L1148&from=PL (dostęp 3.02.2020).

[48] Sieć zespołów CSIRT – zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo dla przemysłowych systemów sterowania (ICS-CSIRT), za: doc. JOIN (2013)1.

[49] K. Silicki, *Co wynika z dyrektywy NIS?*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna 2016*, Wyższa Szkoła Policji w Szczytnie, Szczytno 2017.

[50] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2020 r., poz. 1369 z późn. zm.).

w literaturze naukowej na wyróżnienie zasługuje koncepcja przedstawiona przez R. Bryant i S. Bryant[51]. Podstawowym pojęciem, kategorią jest według nich **przestępczość cyfrowa** (ang. *digital crime*), do której zaliczają **cyberprzestępczość** oraz **przestępczość komputerową**. Druga metoda definiowania zakłada rozróżnienie według kategorii **nowatorstwa** (ang. *novelty*) i **cyfrowości** (ang. *digitality*). Im wyższy stopień każdej z nich, tym bardziej dany czyn można zaklasyfikować jako przestępstwo cyfrowe. Niewątpliwą wadą tak szerokiej definicji jest jej nieprecyzyjność w pewnych aspektach i możliwość zaklasyfikowania każdego z przestępstw do kategorii przestępstw cyfrowych. Bezrefleksyjne przyjęcie sztywnych kryteriów, czy też ogólnie prób ścisłego określenia wzorów lub matryc, mogłoby w efekcie prowadzić do braku sensu tworzenia jakiejkolwiek klasyfikacji cyberprzestępstw, przestępstw cyfrowych i komputerowych. Sami autorzy zauważają wady przyjętego przez nich sposobu rozumowania i sformułowanej koncepcji.

Natomiast do jej zalet można zaliczyć to, że autorzy wyróżniają różne przestępstwa, mogące być zaklasyfikowanymi jako cyfrowe lub cyberprzestępstwa, które niejednokrotnie bywają pomijane w innych publikacjach. Zaliczenie przez autorów do przestępstw komputerowych różnego rodzaju czynów umożliwia zidentyfikowanie jak największej liczby zagrożeń i wektorów ataku lub technik i taktyk działania sprawców. W powyżej przytoczonym wyszczególnieniu można znaleźć zarówno przestępstwa, w których nowe technologie ułatwiają dokonanie czynu lub jego przygotowanie. Przyjęty podział umożliwia dostrzeżenie wielowymiarowości cyberprzestępczości, niezależnie od przyjętej jej definicji. Niejako oddaje to ducha omówionym wyżej pozytywnym aspektom niektórych definicji, czyli uznania cyberprzestępczości za wielowymiarowe zjawisko, nie tak oczywiste jak mogłoby się wydawać na pierwszy rzut oka. Ponadto potwierdza to po raz kolejny konieczność zapamiętania, że cyberprzestrzeń może być zarówno **źródłem**, **celem** lub **środowiskiem ataku**.

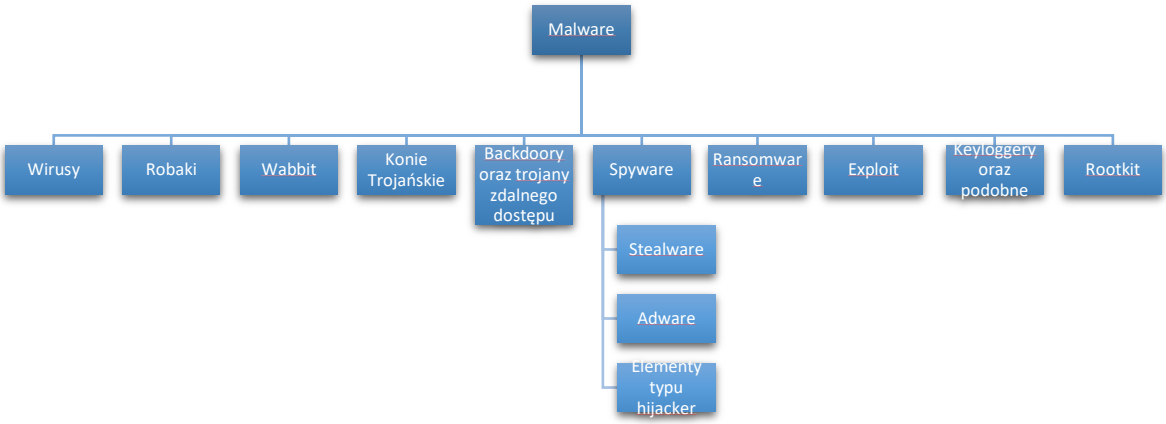
3.3 Typy i definicja szkodliwego oprogramowania

Omawianie istoty i definicji cyberprzestępczości nie byłoby pełne bez określenia wykorzystywanych przez sprawców narzędzi. Jednym z nich jest dosyć szeroka znaczeniowo i funkcjonalnie kategoria szkodliwego oprogramowania. Bez zrozumienia

[51] R. Bryant, S. Bryant, *Policing Digital Crime*, Ashgate, Farnham 2014.

typów i funkcjonalności poszczególnych programów oraz możliwości ich zastosowania do popełniania przestępstw, nie będzie możliwe wskazanie najbardziej istotnych zagrożeń dla bezpieczeństwa.

Szkodliwe oprogramowanie to określenie powstałe w wyniku bezpośredniego tłumaczenia angielskiego określenia *malware*, stanowiące połączenie angielskich słów *malicious* i *software*. Wykorzystywane jest najczęściej do określenia jakiegokolwiek oprogramowania mającego na celu spowodowanie uszkodzenia albo wywołanie innych skutków niż zamierzone przez posiadaczy danych, programu, urządzenia komputerowego, serwera lub sieci komputerowej[52]. Wyróżnić można wiele różnych typów szkodliwego oprogramowania, głównie zależnego od struktury kodu. Rozróżnienia najprościej można dokonać ze względu na przeznaczenie danego typu oprogramowania oraz do jakiego typu działania sprawca chce go wykorzystać.



Rysunek 1. Schemat podziału oprogramowania typu malware – opracowanie własne

Każdy z wyróżnionych powyżej typów szkodliwego oprogramowania posiada swoje własne cechy i funkcjonalności. Zdarza się, że wykorzystywane są pojedynczo lub w ramach zbiorów lub pakietów, czasem nazywanych także „ładunkiem" (ang. *payload*). Zdarza się, że sprawcy wykorzystują właśnie zbiór różnego typu szkodliwego oprogramowania, łącząc jego różne typy w jeden zbiór, czyli ładunek.

[52] J. Kosiński, *Paradygmaty*…, op. cit.

TYP SZKODLIWEGO OPROGRAMOWANIA	OPIS
WIRUSY	programy lub fragmenty kodu wykonywalnego; powielają się samoistnie w celu nadpisywania plików lub zamieniania kod programów na urządzeniu ofiary[53]
ROBAKI	podobne do wirusów, jednak do rozprzestrzeniania się na inne urządzenia wykorzystuje podatności i błędy, sama propagacja odbywa się poprzez komunikację sieciową, przykładowo pocztę elektroniczną lub sieci urządzeń[54]
WABBIT	program, którego celem jest powielanie pliku bądź folderu aż do wyczerpania pamięci urządzenia, na którym działa powodując w efekcie brak dostępu do systemu[55]
KONIE TROJAŃSKIE	oprogramowanie, którego zadaniem jest podszywanie się pod zwyczajne aplikacje, interesujące dla użytkownika, przy okazji instalacji implementuje niepożądane i ukryte dla użytkownika funkcje[56]
BACKDOORY ORAZ TROJANY ZDALNEGO DOSTĘPU	oprogramowanie, które ma na celu umożliwić przejęcie kontroli nad zainfekowanym systemem, pozwalając na wykonywanie na nim wszelkich czynności przez osobę trzecią[57]
SPYWARE	programy komputerowe, których celem jest gromadzenie informacji o użytkowniku i jego danych lub plików oraz przesyłanie ich na zewnętrzny serwer kontrolowany przez osobę trzecią[58]
STEALWARE	typ oprogramowania malware, który w sposób ukryty dokonuje transferu danych lub pieniędzy na inne urządzenie[59]
ADWARE	typ oprogramowania automatycznie generującego niechciane reklamy użytkownikowi, część ponadto zawiera funkcję śledzące jego lokalizację[60]
ELEMENTY TYPU	typ oprogramowania, który zmienia ustawienia przeglądarki internetowej

53 https://en.wikipedia.org/wiki/Computer_virus (dostęp 3.02.2020).

54 https://en.wikipedia.org/wiki/Computer_worm (dostęp 3.02.2020).

55 https://en.wikipedia.org/wiki/Fork_bomb (dostęp 3.02.2020).

56 https://en.wikipedia.org/wiki/Trojan_horse_(computing) (dostęp 3.02.2020).

57 https://en.wikipedia.org/wiki/Backdoor_(computing); https://en.wikipedia.org/wiki/Remote_desktop_software#RAT (dostęp 3.02.2020).

58 M. Górnisiewicz, R. Obczyński, M. Pstruś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną*, Komisja Nadzoru Finansowego, Warszawa 2014.

59 L. Ayala, *Cybersecurity Lexicon*, Apress, New York 2016.

60 *Malware from a to Z*, Adaware, 2017, https://www.adaware.com/knowledge-database/spyware-glossary#Adware (dostęp 01.10.2017).

HIJACKER	użytkownika, powoduje że odwiedza on inne strony niż zamierzał, a także może zmieniać strony startowe bądź domyślne wyszukiwarki[61]
RANSOMWARE	oprogramowanie, które infekuje, a następnie blokuje lub przejmuje kontrolę nad systemem w celu wymuszenia okupu (w postaci pieniędzy, innego środka materialnego lub określonego zachowania) od ofiary ataku[62]
EXPLOIT	to podgrupa szkodliwych programów, które zawierają dane lub kod wykonalny umożliwiające wykorzystanie jedną lub wiele luk w oprogramowaniu działającym na komputerze lokalnym lub zdalnym[63]
KEYLOGGERY	oprogramowanie mające na celu rejestrowanie wciskanych przez użytkownika klawiszy klawiatury
ROOTKIT	dawniej był to tylko zbiór narzędzi, umożliwiający dostęp do systemu na poziomie administracyjnym, obecnie określa się tym mianem szkodliwe (ale nie tylko) oprogramowanie, które w sposób aktywny ukrywa swoje istnienie oraz działania przed użytkownikiem oraz innymi procesami systemowymi[64]

Tabela 1. Typy szkodliwego oprogramowania wraz z charakterystyką funkcjonalności, opracowanie własne

Wskazane powyżej rozróżnienie nie jest zamknięte i ma charakter funkcjonalny. Głównym wyróżnikiem w sferze teoretycznej są możliwe do wykorzystania funkcjonalności szkodliwego oprogramowania. Należy jednak odnieść teorię do praktyki. W przypadku cyberprzestępczości rzadko mamy do czynienia z wykorzystaniem tylko jednego programu lub tylko jednego jego typu. Nierzadko do uzyskania dostępu do urządzenia ofiary sprawca posłuży się jednym, przykładowo exploitem, co z kolei umożliwi mu zaimplementowanie w ramach drugiego ładunku typu spyware, aby zbierać informacje o ofierze i backdoora, w celu utrzymania zdobytego przyczółku w komputerze użytkownika i potencjalnego korzystania z niego do dalszych infekcji. Kombinacji możliwych do zastosowania jest ogromna ilość i pozostają one ograniczone zdolnościami oraz umiejętnościami atakującego i jego wyobraźnią, a także zidentyfikowanymi podatnościami w systemach i sieciach atakowanego.

---

61 *Browser Hijackers – Set Your Browser Free*, Avast, https://www.avast.com/c-browser-hijacker.

62 *Ransomware & Cyber Blackmail*, Oficjalny blog Kaspersky Lab, https://usa.kaspersky.com/resource-center/threats/ransomware (dostęp 3.02.2020).

63 *Co to są exploity i dlaczego są złe*, Oficjalny blog Kaspersky Lab, 2015, https://plblog.kaspersky.com/co-to-sa-exploity-i-dlaczego-sa-zle/3409/ (dostęp 17.08.2015).

64 *McAfee, Rootkits, Part 1 of 3: The Growing Threat*, McAfee 2006, http://download.nai.com/Products/mcafee-avert/whitepapers/akapoor_rootkits1.pdf (dostęp 4.2006).

3.4 Wybrane zagrożenia związane z wykorzystaniem Internetu Rzeczy

Internet Rzeczy do tej pory nie był umiejscowiony w metodologii cyberprzestępczości. Naturalnie jest to spowodowane tym, że konkretne badania pod tym kątem nie były dotychczas prowadzone lub są nieznane. Nie rozpatrywano go dotychczas jako oddzielny, nowy typ zagrożenia. Obecne spektrum możliwości działania przestępców, wykorzystania nowych technologii do przygotowania lub dokonania przestępstwa sprawia, że każde nowe zagrożenie musi być jak najszybciej dostrzegane i zbadane. Dotyczy to także zagrożeń wynikających z rozwoju Internetu Rzeczy. Wymienione w poprzednim podrozdziale zagrożenia należące do szerokiej kategorii złośliwego oprogramowania nie są jedynymi zagrożeniami, które można wykorzystać w połączeniu z tą koncepcją.

RODZAJ ZAGROŻENIA	OPIS
SPAM	Pojęcie to odnosi się do maili lub innego typu wiadomości, których nadawca nie chciał otrzymać lub nie oczekiwał, najczęściej w ogromnej ilości, co ma na celu spowolnienie pracy systemu informatycznego, urządzenia lub sieci internetowej[65]. Do tej kategorii zagrożeń można zaliczyć również inne zjawiska[66], takie jak: o Spam nigeryjski (inaczej: przekręt nigeryjski, oszustwo 419)[67] o Fałszywe reklamy (ang. *false advertising*) – ukrywające pewne warunki sprzedaży lub reklamujące fałszywe lub podrobione produkty o Spam na portalach społecznościowych np. na Facebooku[68]
CLICK FRAUD	Wykorzystuje mechanizm Pay Per Click. Polega na nakłonieniu lub zmuszeniu użytkownika do kliknięcia w reklamę, która zapewnia zysk dla jej właściciela. Ponadto można przy okazji infekować urządzenia ofiar szkodliwymi programami typu exploit (np. exploit kit *Magnitude*[69])
BOTNET	Jest to grupa komputerów zainfekowanych szkodliwym oprogramowaniem, kontrolowanych przez przestępców w sposób zdalny[70], które można wykorzystywać do ataków typu DoS lub DDoS.

[65] S. Hambridge, A. Lunde, *A Set of Guidelines for Mass Unsolicited Mailings and Postings*, https://www.ietf.org/rfc/rfc2635.txt (dostęp 30.04.2018).

[66] J. Kosiński, *Paradygmaty*…, op. cit.

[67] Więcej informacji: http://419scam.org (dostęp 30.04.2018).

[68] *Scams and Spam to Avoid on Facebook*, Symantec Security, https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/scams-spam-to-avoid-facebook-12-en.pdf (dostęp 30.04.2018).

[69] *Magnitude Actor Adds a Social Engineering Scheme for Windows 10*, Proofpoint, https://www.proofpoint.com/us/threat-insight/post/magnitude-actor-social-engineering-scheme-windows-10 (dostęp 30.04.2018).

[70] D. Fischer, *Co to jest botnet?*, Oficjalny Blog Kaspersky Lab, https://plblog.kaspersky.com/botnet/6302/ (dostęp 30.04.2018).

PHISHING	Metoda ataku polegająca na wysyłaniu ofierze maili zainfekowanych złośliwym oprogramowaniem, umożliwiających uzyskanie informacji z urządzenia użytkownika jak np. dane do logowania do konta bankowego. Maile mają naśladować lub imitować te pochodzące z zaufanego i znanego źródła jak np. bank lub operator sieci komórkowej[71]. Swoistą odmianą ataku phishingowego są ataki spearphishingowe (czasem nazywane także kampaniami)[72]. Są to metody szczególnie chętnie wykorzystywane przez grupy cyberprzestępców lub inspirowane i finansowane przez państwa[73].
DOS ORAZ DDOS	Ang. *Denial of Service* i *Distributed Denial of Service*, jest to atak polegający na uniemożliwieniu innym użytkownikom dostępu do informacji lub usług takich jak poczta elektroniczna, witryny internetowe itp.[74]. Różnica w ataku typu *Distributed Denial of Service* polega na wykorzystaniu większej liczby komputerów lub urządzeń niż w przypadku ataku DoS, a więc większej skali..
OSZUSTWA KOMPUTEROWE	Oznaczają wszelkie próby wpływania na automatyczne przetwarzanie, gromadzenie, przekazywanie danych informatycznych lub ich zmienianie bez upoważnienia, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody[75].

Tabela 2. Rodzaje zagrożeń wynikające z funkcjonalności Internetu Rzeczy, opracowanie własne

Wymieniony powyżej katalog nie jest zamkniętym, ponieważ nie sposób wymienić w tym miejscu wszystkich zagrożeń bez zagłębiania się w techniczne szczegóły. Nie byłoby to również celowe, wystarczy wskazanie tych kilku, aby na ich przykładzie omówić ogólnie zjawisko. Powyższe zagrożenia można zaobserwować od dawna, jednak wykorzystując je, a także urządzenia mogące być częścią Internetu Rzeczy stworzy zupełnie nowe niebezpieczeństwa. Najlepszym dowodem na to będzie atak typu DDoS. Do przeprowadzenia największego do tej pory ataku posłużono się wieloma urządzeniami, które wchodzą w skład koncepcji Internetu Rzeczy.

Elementem mogącym znacząco wpływać na poznawanie i wykrywanie nowych typów cyberprzestępstw, a więc także konstruowanie lub modyfikacja definicji i przepisów prawnych, jest możliwość ukrywania lub anonimizowania aktywności. Szczególnie istotnym stało się to dla przestępców wraz z rozwojem urządzeń komputerowych oraz

---

71 P. Stavroulakis, M. Stamp, *Handbook of Information and Communication Security*, Springer, Heidelberg–New York 2010.

72 https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing/ oraz https://blog.trendmicro.com/anatomy-of-a-spear-phishingattack/?_ga=2.147809470.822430326.1609326650-534332073.1609326650 (dostęp 30.04.2018).

73 *Spear-Phishing Email: Most Favored APT Attack Bait*, TrendMicro, https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf (dostęp 30.04.2018).

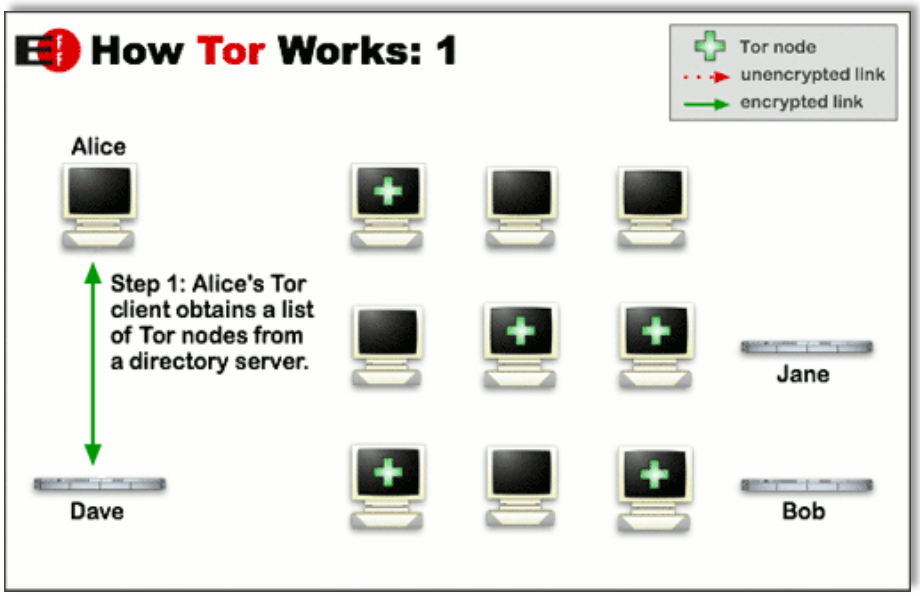
74 https://www.us-cert.gov/ncas/tips/ST04-015 (dostęp: 30.04.2018).

75 Zob. art. 287 k.k.

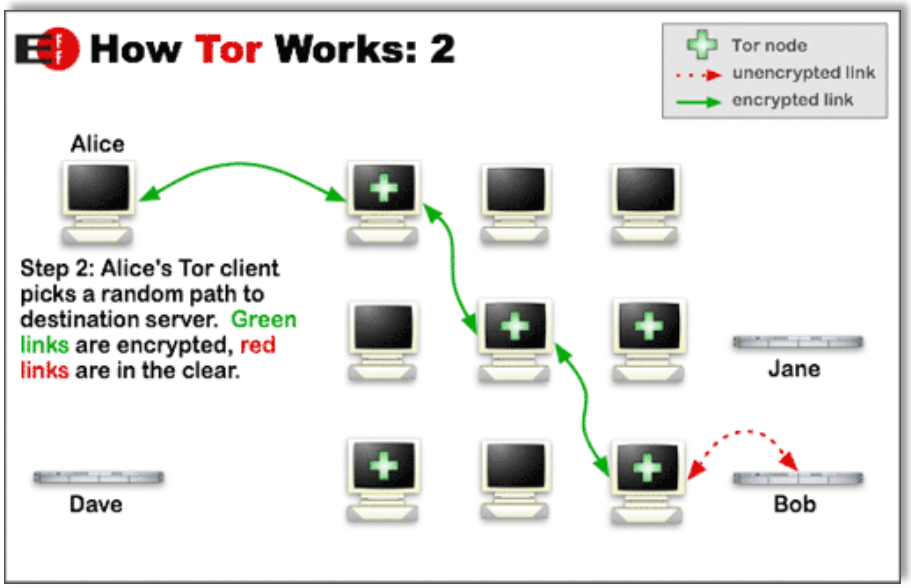
związanym z tym poznaniem i rozwijaniem nowych sposobów komunikacji. Jest to umiejętność, mogąca być ułatwieniem dla sprawców popełniających przestępstwa wykorzystujące funkcjonalności lub podatności Internetu Rzeczy. W związku z tym, że wykorzystanie sieci i komunikacji bezprzewodowej jest główną cechą charakterystyczną wspomnianej koncepcji, a więc także przestępczości z niej potencjalnie wynikającej, możliwości utrudnienia wykrycia działań sprawców przez organy ścigania w wyniku obfuskacji komunikacji sieciowej, są elementarnymi wręcz umiejętnościami. Poznawanie ich także przez organy ścigania oraz rozwijanie metod namierzania użytkowników i monitorowania ruchu sieciowego lub komunikacyjnego sprawia, że coraz trudniej udaje się przestępcom ukryć lokalizację lub historię działań.

Jedną z metod ukrywania tożsamości podczas przeglądania Internetu jest korzystanie z tzw. sieci cebulowej, czyli inaczej sieci TOR (ang. *The Onion Routing*). Jest to grupa serwerów umożliwiająca użytkownikom przeglądanie sieci internetowej z zachowaniem znacznego stopnia anonimowości. Pierwotnie sieć ta została stworzona przez *United States Naval Research Laboratory* wraz z Marynarką Wojenna Stanów Zjednoczonych (*United States Navy*) jako narzędzie zabezpieczające komunikację rządową. Łączenie urządzenia użytkownika z miejscem docelowym w sieci następuje poprzez wysyłanie danych (informacji, maili, plików itp.) przez kilka serwerów (nazywanych przez organizację *Tor Project* wirtualnymi tunelami) zamiast robić to bezpośrednio między wysyłającym a odbierającym[76]. TOR zapobiega namierzeniu i wyśledzeniu miejsca wysłania oraz przeznaczenia danego pakietu danych. Na każdym etapie są one zaszyfrowane w sposób, umożliwiający ich odczytanie dopiero po przejściu przez węzeł nr 3 i z niego bezpośrednio do odbiorcy.

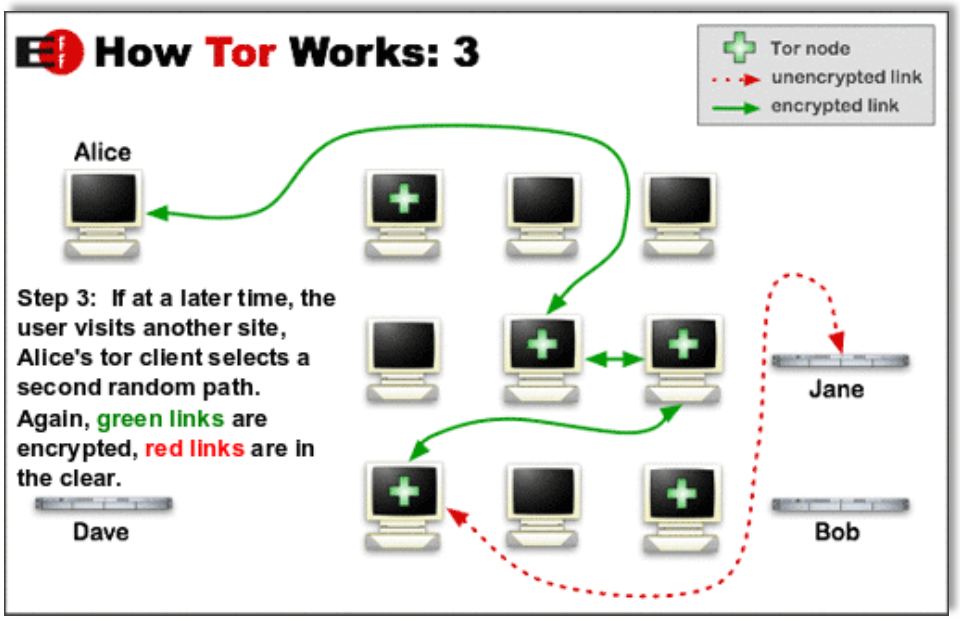
[76] https://www.torproject.org/about/overview.html.en#overview (dostęp 30.04.2018).



Rysunek 2. How Tor works cz. 1 – źródło: https://www.torproject.org/about/overview.html.en#overview



Rysunek 3. How Tor works cz. 2 – źródło: https://www.torproject.org/about/overview.html.en#overview



Rysunek 4. How Tor works cz. 3 – źródło: https://www.torproject.org/about/overview.html.en#overview

Sieć TOR pozwala na częściowe ukrycie tożsamości poprzez nieujawnianie miejsca, z którego następuje połączenie ze stroną. Nie oznacza to jednak, że jest to narzędzie idealne. Nie pozwoli na zachowanie pełni anonimowości w przypadku, gdy wysyłane informacje albo strona, którą odwiedzimy pozwoli na ustalenie tożsamości użytkownika. Przykładowo, w niczym nie pomoże korzystanie z przeglądarki z obsługą sieci TOR, gdy zalogujemy się na swoje konto mailowe, bankowe i będziemy wykonywali wszystkie te czynności, które wykonujemy w normalnej przeglądarce. Wnikliwy obserwator będzie w stanie powiązać tożsamość użytkownika sieci TOR z naszą tożsamością. To samo tyczy się wysyłania lub pobierania plików – pliki naszego autorstwa lub zawierające treści wyraźnie wskazujące na nas, jedynie wysłane za pośrednictwem sieci TOR, z pewnością nakierują na nas, jako użytkownika.

Na marginesie rozważań o anonimowości w sieci i jej związku z cyberprzestępczością należy podkreślić, że samo korzystanie z sieci TOR nie może stawiać osoby w kręgu podejrzeń o działalność niezgodną bądź na granicy prawa. Bywa, że pojawiają się głosy, że korzystanie z tego typu programów bądź podobnych, mających za zadanie zwiększyć anonimowość użytkowników w sieci automatycznie oznaczają, że ta osoba ma „coś" do ukrycia - e domyśle oznacza to coś niezgodnego z prawem lub pozostającego na granicy tegoż. Kompletnie niewłaściwym i nieuprawnionym jest twierdzenie, że sieć TOR ma na celu tylko i wyłącznie maskowanie działalności

przestępczej. W obiegu publicznym funkcjonuje błędne przeświadczenie, że osoby chcące zachować anonimowość w sieci to tylko i wyłącznie przestępcy lub terroryści. Powyższe rozważania nie byłyby pełne bez wyjaśnienia podstawowych różnic między częścią Internetu, z której wszyscy korzystamy na co dzień, a *Deep Web* i *Dark Web*, gdyż każda z tych rzeczy jest czymś innym.

Najprościej będzie opisać każde z tych pojęć posługując się obrazowym, działającym na wyobraźnię, przykładem. Można sobie wyobrazić Internet jako górę lodową. Jej część znajduje się ponad powierzchnią wody i jest doskonale widoczna dla każdego. Natomiast, jak wiadomo powszechnie, jest to tylko jej niewielka część. Reszta góry jest ukryta pod powierzchnią wody i z daleka nie jest widoczna jej całkowita wielkość i skala. Odnosząc tę metaforę do Internetu, część widoczna, czyli tzw. sieć zindeksowana (ang. *Surface Web*) to taka, w której porusza się największa liczba użytkowników. Jej nazwa wzięła się z tego, że jest ogólnodostępna, a strony w niej się znajdujące są indeksowane przez wyszukiwarki sieciowe takie jak Google czy Bing. Znaleźć w niej można ogólnodostępne i najpopularniejsze strony internetowe takie jak Google, Yahoo, YouTube, Wikipedia, Facebook, Twitter i inne, a także wszelkiej maści serwisy i fora informacyjne oraz tematyczne. Brak jest źródeł podających dokładną wielkość sieci zindeksowanej. Wskazuje się, że może to być jedynie 0,03% Internetu lub, że jest ona od 400 do 550 razy mniejsza niż sieć ukryta, czyli *Deep Web*[77].

Sieć ukryta, czyli *Deep Web*. w przeciwieństwie do sieci zindeksowanej obejmuje ona strony niezindeksowane, czyli na które nie można wejść używając wyszukiwarki sieciowej, ponieważ jej zawartość została zakodowana w tym celu[78]. Obejmuje strony umyślnie lub nie ukryte, niewidoczne albo w inny sposób zablokowane przed wyszukiwarkami, a także zastrzeżone dla twórcy i użytkowników ze specjalnymi uprawnieniami[79]. Jedną z popularniejszych metod jest dynamiczne generowanie treści na stronach co uniemożliwia lub utrudnia robotom internetowym (ang. *search engine crawlers* lub *web crawlers*) indeksowanie i zbieranie informacji oraz linków do danej strony, a przez to pozycjonowanie jej i indeksowanie w danej wyszukiwarce sieciowej. Jest

---

77 C. Grannan, *What's the Difference Between the Deep Web and the Dark Web?*, Britannica, https://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web (dostęp 30.04.2018).

78 https://www.pcmag.com/encyclopedia/term/41069/deep-web (dostęp 30.04.2018).

79 https://www.techopedia.com/definition/15653/deep-web (dostęp 30.04.2018).

to największa część Internetu, niektórzy podają, że stanowi nawet 90% Internetu, jednak ciężko jest to dokładnie określić w pełni i z pewnością[80].

Ostatnią częścią jest Darknet, czyli *Dark Web*, najmniejsza pod względem liczby stron. Wbrew pozorom nie jest ona niewidoczna dla użytkowników albo nie wymaga magicznych zdolności do dotarcia do stron w Darknecie, podobnie zresztą jak w przypadku sieci ukrytej. Specyfika jej działania polega na tym, że ukryte są adresy IP serwerów, na których znajdują się konkretne witryny internetowe, czyli trudność nie polega na znalezieniu danej strony, a jedynie na ustaleniu położenia serwera, na którym działa. Najczęściej funkcjonują one wykorzystując sieci TOR albo I2P (oprogramowanie podobne w swoim sposobie działania do tego pierwszego). Konsekwencją takiego stanu rzeczy jest to, że na stronę operującą w sieci TOR może wejść tylko użytkownik przeglądarki działającej w tej samej sieci. Estymuje się, że stanowi jedynie 0,01% sieci ukrytej[81].

Z uwagi na możliwości Darknetu, stał się on miejscem działalności przestępców. Można tu było znaleźć takie serwisy jak Silk Road, Silk Road 2, AlphaBay, Evolution, Atlantis czy Agora. Najbardziej rozpowszechnioną na tych platformach sferą działalności był handel narkotykami i bronią oraz strony służące do prania brudnych pieniędzy. Z powyższych znane były głównie Silk Road (dwukrotnie likwidowane) oraz AlphaBay. Ta druga strona była chętnie wykorzystywana ze względu na swoją renomę po zamknięciu Silk Road i stabilność serwerów. Serwis Silk Road 2 został ostatecznie zlikwidowany w listopadzie 2014 roku w ramach operacji „Onymous". Została ona przeprowadzona wspólnie przez Europol, FBI oraz Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych (ang. *Department of Homeland Security*)[82]. AlphaBay z kolei przestała nagle działać 5 lipca 2017 r. Serwery tego serwisu zostały zarekwirowane w Kanadzie przez Kanadyjską Królewską Policję Konną (ang. *Royal Canadian Mounted Police*) na prośbę FBI oraz przez organy właściwe w takich krajach jak Litwa, Wielka Brytania, Tajlandia i Francja. W tym samym czasie w Bangkoku zatrzymano właściciela serwisu A. Cazesa, obywatela Kanady, który 12 lipca odebrał sobie życie w tajskim więzieniu

---

[80] A. Greenberg, *Hacker Lexicon: What Is The Dark Web?*, WIRED.com, https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (dostęp 30.04.2018).

[81] Ibidem.

[82] A. Greenberg, *Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains*, WIRED.com, https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/ (dostęp 30.04.2018).

w oczekiwaniu na ekstradycję do USA[83]. Według p.o. dyrektora FBI w owym czasie, A. McCabe'a, AlphaBay był 10 razy większy niż zamknięty w 2013 r. Silk Road. Wyraził przy tym obawę, że pomimo zlikwidowania jednej strony to w jej miejsce powstanie kolejna, tak jak w miejsce Silk Road powstała AlphaBay i inne strony[84]. Nie sposób nie zgodzić się z tą refleksją.

Przykład Silk Road, jego dwukrotnego zamknięcia oraz powstania w jego miejsce kilku serwisów, często prowadzących działalność na o wiele większą skalę pokazuje, że największym wyzwaniem nie jest jedynie zamykanie tego typu serwisów. Przed organami ścigania, wymiaru sprawiedliwości oraz władzy publicznej stoi również zapobieganie powstawania nowym albo ich monitorowanie w momencie rozpoczęcia przez nie działalności. W tym pierwszym przypadku wydaje się być to nierealne, ponieważ brak jest narzędzi i środków do monitorowania wszelkich powstających w sieci stron.

Inna refleksja odnosi się do Darknetu, *Deep web* oraz sieci TOR – nie należy utożsamiać ich jedynie z przestępczą działalnością w cyberprzestrzeni. Są jedynie narzędziami, które mogą posłużyć do wielu działań, tak legalnych jak i nielegalnych. Ich funkcjonalność i działanie umożliwiają wielu osobom dostęp do sieci z miejsc, gdzie jest on ograniczony, przykładowo z uwagi na panujące warunki i ustrój polityczny. Pozwala obywatelom donosić o łamaniu prawa w krajach, gdzie kontakt ze światem zewnętrznym może być utrudniony bądź ze stref konfliktu zbrojnego. Pozwala też dziennikarzom i tzw. sygnalistom (ang. *whistleblowers*) na komunikację, a tym drugim dodatkowo na jakąkolwiek, choćby szczątkową, anonimizację swoich działań[85]. Przykładowo użytkowanie sieci TOR do komunikacji rekomendują takie organizacje jak Reporterzy Bez Granic i Human Rights Watch[86].

---

[83] S, Gibbs, L. Beckett, *Dark web marketplaces AlphaBay and Hansa shut down*, „The Guardian", 20 lipca 2017 r., https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down (dostęp 30.04.2018).

[84] Ibidem.

[85] TOR jest częścią systemu SecureDrop, umożliwiającego przesyłanie tajnych dokumentów i danych bezpośrednio do dziennikarzy np. przez sygnalistów. System został pierwotnie uruchomiony przez „The Guardian", jednak według informacji na stronie TOR korzystają z niego również Associated Press, „The Washington Post", „The New York Times", The CBC, ProPublica, Dagbladet i inni; za: J. Ball, *Guardian launches SecureDrop system for whistleblowers to share files*, „The Guardian", 5 czerwca 2014 r., https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents (dostęp 30.04.2018).

[86] https://www.torproject.org/about/torusers.html.en (dostęp 30.04.2018).

Istnieje jeszcze inna refleksja dotycząca warstwy językowej nazwy „cyberprzestępczość". Według J. Kosiński: „cyber" jest idealnym prefiksem (w słowie cyberprzestępstwo – przyp. autor) – większość czytelników i słuchaczy nie ma pojęcia, co znaczy, ale może poprzedzać dowolne słowo, aby całość wydawała się nowa, atrakcyjna i jednocześnie dziwna, straszna lub naukowa"[87]. Nie sposób nie zgodzić się, że przedrostek „cyber-" bywa nadużywany, co powoduje pewien chaos terminologiczny, a także zupełnie niepotrzebne uogólnienia. Wprowadza się nowe pojęcie zbiorcze dla kategorii, które swoją definicją już mają i to w dodatku zakorzenioną od jakiegoś czasu w badaniach naukowych i doktrynie. Ujednoliceniu terminologii powinno towarzyszyć doprecyzowanie definicji „cyberprzestępstwa" w stopniu wyższym niż odniesienie go do przestępstw komputerowych i sieciowych. Uwzględniając powyższe należy się zastanowić: w jakim celu używana jest definicja „cyberprzestępstwa". Czy z powodu wygody i łatwiejszego nazywania pewnej grupy zjawisk zbiorczo, nie zagłębiając się w ich istotę? Czy jednak dlatego, że dążymy do ujednolicenia terminologicznego w kwestii przestępstw doby komputerów, Internetu i nowych technologii, uwzględniając niuanse każdego z możliwych nowych typów przestępstw? Prawdą jest fakt, że w obecnie powstającej literaturze i aktach prawnych dominującym pojęciem staje się określenie przestępstw komputerowych i sieciowych mianem „cyberprzestępstw". Z jednej strony należy stwierdzić, że rzeczywiście przedrostek „cyber-" jest nadużywany. Jednak nie sposób zgodzić się ze stwierdzeniem, że w wyniku tego pojęcie „cyberprzestępstwa" jest zdyskwalifikowane. Określenie „cyberprzestępstwo" może z powodzeniem funkcjonować jako ujednolicone pojęcie dla takich kategorii przestępstw jak przestępstwa komputerowe, sieciowe i cyfrowe. Może to nastąpić jedynie w przypadku, gdy po pierwsze uda się wypracować w miarę zbliżone stanowiska co do definicji, a po drugie niezbędne jest trzymanie się przyjętej definicji i terminologii. Wydaje się to być najbardziej efektywny sposób na zmianę w tej kwestii w odniesieniu do cyberprzestępczości. Podsumowując, należy stwierdzić, że jeżeli przedrostek „cyber-" stosowany będzie w konkretnym celu, a nie jako uatrakcyjnienie określeń w potocznym języku to w takim wypadku będzie to z istotną korzyścią dla rozwoju badań odnośnie związków przestępczości z rozwojem nowych technologii i ich użycia do popełniania przestępstw.

Przytoczone wyżej aspekty, tak te dotyczące szkodliwego oprogramowania, metod anonimizacji ruchu sieciowego oraz zagrożeń związanych z możliwościami wykorzystania

[87] J. Kosiński, *Paradygmaty*…, op. cit.

funkcjonalności lub podatności Internetu Rzeczy ukazują, jak wielkim zagrożeniem jest połączenie wszystkich powyższych aspektów i sprzężenie ich w ramach wspomnianej koncepcji. Niesie to ze sobą znaczące wyzwania dla organów ścigania, wymiaru sprawiedliwości, a także władzy publicznej. Także w wymiarze stanowienia prawa i tworzenia procedur kryminalistycznych. Przede wszystkim będzie to miało wpływ na efektywność i skuteczność prowadzonych przez nie postępowań karnych.

Rozdział 4. Internet Rzeczy a polskie prawo karne

4.1 Wprowadzenie

Cyberprzestępczość, z uwagi na to, że jest dosyć szeroką kategorią i składać się na nią może wiele działań, nie jest opisana w polskim ustawodawstwie karnym w jednym dziale. Natura cyberprzestępczości nakazuje wręcz rozpoznawanie wieloaspektowości tego zjawiska i potencjalnego wykorzystania urządzeń, systemów lub sieci informatycznych do popełnienia tzw. klasycznych przestępstw. W polskim ustawodawstwie kwestia cyberprzestępczości rozproszona jest pośród wiele aktów prawnych. Najbardziej obszerne regulacje ustawodawca umieścił w Kodeksie karnym (dalej jako k.k).

W pierwszej kolejności należy skupić się na przestępstwach dotyczących bezpieczeństwa informacji i ich przetwarzania. Mimo faktu, że funkcjonalności lub podatności Internetu Rzeczy można wykorzystać do popełnienia szerszej kategorii przestępstw, w tym także tych przeciwko życiu i zdrowiu czy porządkowi publicznemu, to na gruncie rozważań wstępnych odnośnie zagrożeń należy się na razie skupić na przestępstwach *stricte* związanych z zapewnieniem bezpiecznego przetwarzania danych informatycznych. W k.k. są to przepisy dotyczące przestępstw przeciwko Rzeczypospolitej Polskiej (Rozdział XVII), bezpieczeństwu powszechnemu (Rozdział XX) oraz ochronie informacji (Rozdział XXXIII).

Na potrzeby analizy najistotniejszych i aktualnie potencjalnie najbardziej powszechnych zagrożeń należy dokonać analizy konkretnych artykułów z tych rozdziałów. Ich wybór oparty jest o to, czy w ich treści (znamionach) występują elementy dotyczące systemów, sieci, urządzeń informatycznych, lub przetwarzania w nich danych informatycznych. Umożliwia to także omówienie do kwestii powiązania i możliwości wykorzystania przestępstw komputerowych (tzn. takich, gdy środowisko komputerowe, informatyczne czy sieciowe może być źródłem, środkiem lub celem ataku) do czynów kojarzonych aktualnie z możliwymi do dokonania jedynie w świecie rzeczywistym.

4.2 Analiza wybranych przepisów kodeksu karnego

Przepisy dotyczące bezpieczeństwa informacji dotyczą także bezpieczeństwa przetwarzania danych informatycznych znajdujących się na urządzeniach lub w systemach i sieciach informatycznych. Analiza doktrynalna i semantyczna przepisów polskiego prawa karnego dostarcza wniosków, że ustawodawca umieścił w kodeksie określenia dotyczące urządzeń, sieci i systemów informatycznych, co oznacza też dostrzeżenie ich istoty we współczesnej rzeczywistości, a także z punktu widzenia systemu prawnego. Głównymi artykułami, na których należy się skupić są art. art. 130 §3, 165 §1 pkt 4, 267, 268, 268a, 269, 269a oraz 269b k.k.

ARTYKUŁ	ZACHOWANIA KARALNE WYNIKAJĄCE ZE ZNAMION
ART. 130 §3	Działanie, to znaczy uzyskanie informacji, poprzez gromadzenie, przechowywanie informacji lub wchodzenie do systemu informatycznego aby je zdobyć i przekazanie ich następnie obcemu wywiadowi. Nazywane też może być szpiegostwem komputerowym.
ART. 165 §1 PKT 4	Sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach poprzez zakłócenie, uniemożliwienie lub w inny sposób wpływanie na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych
ART. 267	Nielegalne uzyskanie lub ujawnienie informacji poprzez uzyskanie dostępu do komunikacji w wyniku podłączenia się do sieci telekomunikacyjnej lub przełamania albo ominięcia jej zabezpieczeń (elektronicznych, magnetycznych, informatycznych lub innych szczególnych). Także w wyniku założenia lub posłużenia się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem. Karalne jest także uzyskanie dostępu do całości lub części systemu informatycznego bez wymaganego uprawnienia. Jest to przestępstwo ścigane na wniosek pokrzywdzonego.
ART. 268	Niszczenie, uszkadzanie, usuwanie lub zmiana zapisu informacji (także znajdującego się na informatycznym nośniku danych) przez osobę nieuprawnioną do tego albo udaremnienie lub znaczące utrudnienie zapoznania się z nią przez osobę uprawnioną. Wymiar kary zależy od stopnia wyrządzonej szkody przez sprawcę. Jest to przestępstwo ścigane na wniosek pokrzywdzonego.
ART. 268A	Niszczenie, uszkodzenie, usunięcie, zmiana lub utrudnienie dostępu do danych informatycznych przez osobę nieuprawnioną do tego, albo zakłócenie (w istotnym stopniu) lub uniemożliwienie *automatycznego przetwarzania, gromadzenia lub przekazywania takich danych.* Wymiar kary zależy od stopnia wyrządzonej szkody przez sprawcę. Jest to przestępstwo ścigane na wniosek pokrzywdzonego.
ART. 269	Niszczenie, uszkodzenie, usunięcie lub zmiana danych informatycznych o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego. Karalne jest także

	zakłócenia lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania takich danych oraz niszczenie albo wymiana informatycznego nośnika danych lub niszczenie albo uszkodzenie urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania wspomnianych wyżej danych informatycznych. Ten czyn bywa też określany mianem sabotażu komputerowego.
ART. 269A	Zakłócenie pracy systemu informatycznego, teleinformatycznego lub sieci teleinformatycznej poprzez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, nie będąc przy tym do tego uprawnionym.
ART. 269B	Potocznie nazywane przestępstwem hackingu. Polega na wytwarzaniu, pozyskiwaniu, zbywaniu lub udostępnianiu innym osobom urządzenia, programów haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej i przystosowanych do popełnienia między innymi wskazanych wyżej przestępstw. Przepis ten jednakże zawiera także kontratyp działania wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej przed popełnieniem przestępstwa wymienionego w tym przepisie albo opracowania metody takiego zabezpieczenia. Tego typu działalność bywa także określana mianem aktywności typu *white hat*.

Tabela 3. Przestępstwa zawierające w znamionach określenie urządzeń, sieci lub systemów informatycznych, opracowanie własne na podstawie treści przepisów kodeksu karnego.

Wszystkie powyższe przestępstwa łączy fakt, że są związane w mniejszym lub większym stopniu poprzez znamiona z urządzeniami, sieciami lub systemami informatycznymi. Są one albo konstytutywnym elementem, niezbędnym do ich spełnienia albo są co najmniej znaczącym dla kwalifikacji prawnej czynu. W powyższych przepisach można znaleźć tak różne określenia jak system informatyczny, system teleinformatyczny, sieć teleinformatyczna, sieć telekomunikacyjna, dane informatyczne, hasła komputerowe, kody dostępu, dane umożliwiające nieuprawniony dostęp do informacji przechowywanych w systemach informatycznych, teleinformatycznych lub sieci teleinformatycznej, urządzenia lub programy komputerowe oraz automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych. Jest to duża liczba określeń, czasem bliskoznacznych w potocznym języku, a mających różne desygnaty w języku prawnym. Należałoby się zastanowić, czy zasadnym nie byłoby dokonanie przeglądu występujących w dokumentach prawnych określeń, wraz z ujednoliceniem ich biorąc pod uwagę pierwotne desygnaty, jak i rozwój techniki i technologii informatycznych. Dokładna analiza pełnej treści przepisów prawnych umożliwia przedstawienie i sprecyzowanie związków z możliwościami wykorzystania funkcjonalności lub podatności koncepcji

Internetu Rzeczy do popełniania przestępstw. Treść przepisów wyraźnie wskazuje na nierozerwalność przedmiotu ochrony tzn. informacji, z faktem gdzie i jak jest ona przetwarzana oraz w jakiej formie. Niezależnie czy będzie to się odbywało w sieci teleinformatycznej czy telekomunikacyjnej, systemach informatycznych czy teleinformatycznych lub w postaci danych informatycznych, danych autoryzujących dostęp jak kody dostępu czy hasła komputerowe czy programów komputerowych.

Na kanwie przeprowadzonej analizy dogmatycznej i semantycznej należy zauważyć jak licznie występują zróżnicowane określenia systemów, danych i urządzeń. Z jednej strony jest to zaleta, gdyż nie ogranicza to skuteczności wykładni przepisów do wąskiego grona lub grupy przedmiotów. Niweluje to potencjalne zarzuty o brak wymienienia niektórych kategorii urządzeń, systemów lub sieci występujących w innych aktach prawnych polskiego porządku prawnego. Wymienienie aż tylu określeń umożliwia powiązanie z przepisami ustawy jak największej liczby potencjalnych zdarzeń i działań.

Z drugiej strony, powoduje to rozbicie znaczeniowe w sytuacji, w której być może nie jest ono konieczne. Istnieje szansa na skodyfikowanie i ujednolicenie nazewnictwa w tym zakresie. Naturalnie oznaczałoby to konieczność zmiany innych aktów prawnych poprzedzonej gruntowną analizą systemową polskiego porządku prawnego. Należy już w tym miejscu zwrócić uwagę na kilka problematycznych kwestii. Słusznie zauważa A. Adamski na kanwie analizy wykładni językowej przepisów k.k. oraz Cyberkonwencji, a konkretnie art. 269b k.k. oraz art. 6 Cyberkonwencji, należy zauważyć, że polski ustawodawca dokonuje transpozycji przepisów do polskiego porządku prawnego w sposób długotrwały[88], niepełny i niespójny logicznie. Przykładowo brzmienie art. 269b k.k. nie odpowiada brzmieniu art. 6 Cyberkonwencji, a według ustawodawcy ma być właśnie takim odpowiednikiem[89]. Przytaczając jedynie część argumentacji prof. Adamskiego odnoszącej się do sfery *stricte* terminologicznej, logicznej i językowej - nie ma hasła dostępu umożliwiającego „nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, systemie teleinformatycznym lub sieci teleinformatycznej", ponieważ hasło dostępu może być tylko właściwe albo nie, poprawne albo nie. Jedyne co może być przedmiotem zainteresowania organów ścigania jest fakt, w jaki sposób dana

[88] Cyberkonwencja została podpisana w roku 2001, jej ratyfikacja w Polsce nastąpiła dopiero w roku 2014, jednak nie została ona w pełni zaimplementowana – przyp. autor.

[89] A. Adamski, *Europejskie standardy prawnokarnej ochrony sieci i informacji oraz ich implementacja do ustawodawstwa polskiego*, w: G. Szpor, A. Gryszczyńska (red.), *Internet. Strategie bezpieczeństwa*, C.H. Beck, Warszawa 2017.

osoba weszła w jego posiadanie i czy ta osoba jest uprawniona do dysponowania tymże hasłem[90].

Uzasadnionym byłby postulat dokładniejszego formułowania przez ustawodawcę treści przepisów, w szczególności przepisów zawierających sankcję karną z uwagi na ich doniosłe znaczenie w systemie prawnym w ogóle oraz dla sytuacji jednostek żyjących w danym systemie prawnym. W szczególności w sytuacji, gdy mamy do czynienia z przepisami które należy transponować do polskiego porządku prawnego. Zasadnym byłoby dokładne uwzględnienie intencji przyświecających osobom kształtującym umowy międzynarodowe oraz tworzącym konkretne przepisy. Uwzględniając wszystkie okoliczności oraz podstawowe zasady tworzenia przepisów i norm polski ustawodawca powinien być w stanie stworzyć przepisy będące zgodne z tymi, które podlegają transpozycji z międzynarodowych aktów prawnych i dokumentów. Choćby miało to dotyczyć jedynie warstwy semantycznej przepisów. Pominięcie podstawowych założeń, dla których dane przepisy zostały ustanowione spowoduje, że tworzone, dostosowywane lub wprowadzane do polskiego systemu prawnego regulacje nie będą spełniały swojej pierwotnej roli w ogóle albo nie będą tego robiły w sposób wystarczający. Koniecznym wydaje się poświęcenie większej uwagi kwestiom definicyjnym odnośnie cyberprzestępczości w odniesieniu do sposobu ich działania, a mianowicie posługiwanie się w miarę możliwości jak najdokładniej już funkcjonującą nomenklaturą techniczną. Opisana przez prof. Adamskiego oraz przedstawiona w tym podrozdziale różnorodność definicyjna i nadmiar określeń technicznych w występujących w k.k. powinny zwrócić uwagę na potrzebę dbałości i zachowania staranności w tworzeniu przepisów. Istotną kwestią jest ich kompleksowość, określenie w ramach ich treści w jak najbardziej pełny sposób sytuacji i zdarzeń, mogących wystąpić w teraźniejszości i w przyszłości. Naturalnie także nie należy zapominać przy tym o potrzebie tworzenia przepisów generalnych i abstrakcyjnych, jednak na tyle dosadnych szczególnie w sferze prawnokarnej, że nie ich błędne lub niepełne sformułowanie nie spowoduje naruszenia praw jednostek. W ramach tego postulatu należy także zwrócić uwagę na dbanie o aktualność przepisów w odniesieniu do rozwoju techniki, choć bez nadmiernej i zbyt częstej ingerencji w ich treść, aby zapewnić stabilność i pewność prawa. Zasadnym i potrzebnym byłoby przy konstruowaniu tego typu przepisów skonsultowanie ich treści nie tylko z prawnikami-

[90] Ibidem.

specjalistami z zakresu legislacji, ale również osobami zajmującymi się informatyką lub cyberbezpieczeństwem, także od strony technicznej.

Kodeks karny penalizuje czynności, które nie ograniczają się jedynie do ochrony informacji o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innych organów lub instytucji państwowych albo samorządu terytorialnego. Dotyczy ona również wszelkich informacji do których dana osoba nie ma dostępu, niekoniecznie z uwagi na doniosłość znaczenia informacji z wymienionych powyżej powodów. Często ma znaczenie element techniczny jakiego typu jest to informacja – cyfrowego czy też, wobec braku innego określenia, analogowa lub jaka jest jej lokalizacja. Na przykład to czy znajduje się w systemie informatycznym, czy na nośniku danych elektronicznych jakim jak dysk twardy, karta pamięci lub pamięć USB. Ma to znaczenie drugorzędne, ponieważ ważniejszą kwestią jest, co zostało już zaznaczone wyżej, czyli sama informacja i jej ochrona.

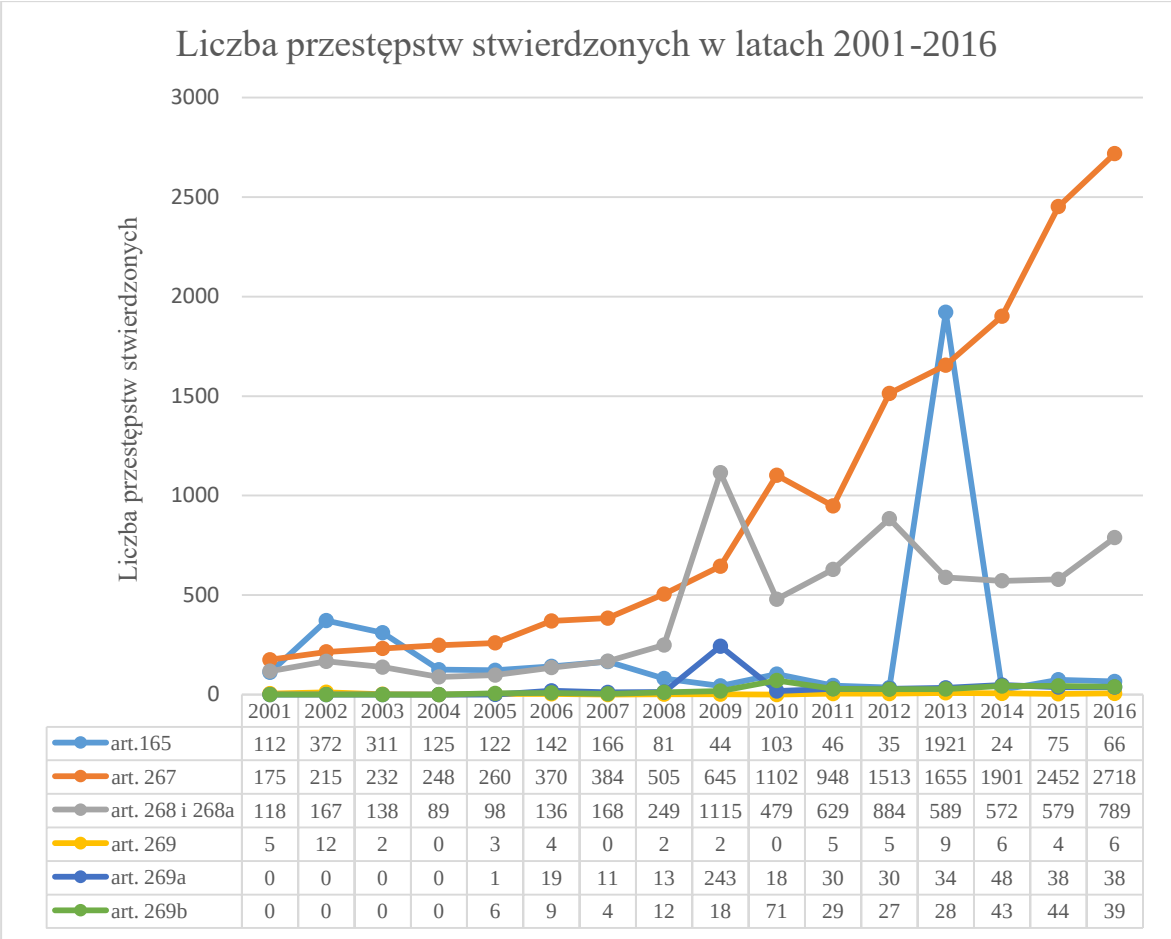
4.3 Statystyka wybranych cyberprzestępstw

Rok	art. 165		art. 267		art. 268 i 268a		art. 269		art. 269a		art. 269b	
	A	**B**	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**	**A**	**B**
2016	159	66	3401	2718	712	789	11	6	44	38	36	39
2015	149	75	3515	2452	759	579	4	4	52	38	58	44
2014	125	24	2868	1901	743	572	10	6	27	48	47	43
2013	106	1921	2203	1655	765	589	14	9	37	34	42	28
2012	84	35	1657	1513	796	884	9	5	35	30	21	27
2011	76	46	1583	948	885	629	3	5	38	30	38	29
2010	67	103	1194	1102	690	479	7	0	22	18	35	71
2009	93	44	982	645	555	1115	6	2	34	243	23	18
2008	132	81	694	505	366	249	6	2	13	13	12	12
2007	225	166	616	384	244	168	6	0	11	11	4	4
2006	230	142	538	370	201	136	3	4	19	19	9	9
2005	196	122	430	260	152	98	2	3	1	1	6	6
2004	184	125	378	248	105	89	12	0	-	-	-	-
2003	151	311	362	232	114	138	2	2	-	-	-	-
2002	192	372	294	215	89	167	6	12	-	-	-	-
2001	209	112	259	175	60	118	9	5	-	-	-	-

Tabela 4. Tabela przedstawiająca statystyki dotyczące wybranych przestępstw w XXI wieku, literą A oznaczono liczbę postępowań wszczętych, literą B oznaczono liczbę przestępstw stwierdzonych, źródło danych: Dane Statystyczne Komendy Głównej Policji

Dostępne publicznie dane statystyczne nie pozwalają stwierdzić jak duża w rzeczywistości jest skala przestępstw przeciwko bezpieczeństwu informacji, a tym bardziej wskazania tylko tych związanych tylko z urządzeniami, systemami i danymi informatycznymi. Nie sposób jest określić szczegółów dotyczących prezentowanych w statystyce spraw bez dokładnych i szeroko zakrojonych badań aktowych. Na podstawie powyższych danych statystycznych zaobserwować można generalny trend wzrostowy liczby przestępstw stwierdzonych w przypadku każdego z wymienionych wyżej artykułów k.k. W skali ogółu dokonywanych w Polsce przestępstw nie jest to być może pokaźna liczba - w 2017 roku w Polsce stwierdzonych zostało 753 963 przestępstw według danych GUS, w tym 463 907 o charakterze kryminalnym. Jednak zaobserwowany wzrostowy trend, w najbliższych latach będzie się najprawdopodobniej utrzymywał. To w konsekwencji przełoży się na większą liczbę postępowań i stwierdzonych przestępstw. Będzie to wynikało częściowo zapewne z jeszcze większego upowszechnienia urządzeń elektronicznych i informatycznych, większej ilości danych informatycznych, a także wzrostu szeroko pojętej świadomości technicznej obywateli oraz funkcjonariuszy Policji. Można przewidywać, że przełoży się to też na bardziej adekwatną kwalifikację prawną czynów.

W kwestii rekomendacji dotyczących prowadzenia statystyk przez Policję to wspomniana już tendencja wzrostowa wymienionych w tabeli rodzajów przestępstw, ale także ewentualne wprowadzenie do porządku prawnego nowych przepisów karnych będzie stanowić największe wyzwanie dla organów ścigania i wymiaru sprawiedliwości. Bez odpowiedniej wiedzy, nawet na minimalnym poziomie, oraz bez konsultacji ze specjalistami nie będzie możliwe adekwatne sformułowanie przepisów lub ich nowelizacja. To z kolei może doprowadzić do wadliwych kwalifikacji prawnych czynów, planowania czynności na miejscu zdarzenia lub w toku postępowania oraz orzekania następnie przez sąd kary sprawcy.



	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016
art.165	112	372	311	125	122	142	166	81	44	103	46	35	1921	24	75	66
art. 267	175	215	232	248	260	370	384	505	645	1102	948	1513	1655	1901	2452	2718
art. 268 i 268a	118	167	138	89	98	136	168	249	1115	479	629	884	589	572	579	789
art. 269	5	12	2	0	3	4	0	2	2	0	5	5	9	6	4	6
art. 269a	0	0	0	0	1	19	11	13	243	18	30	30	34	48	38	38
art. 269b	0	0	0	0	6	9	4	12	18	71	29	27	28	43	44	39

Wykres 1. Wykres przedstawiający statystyki liczby stwierdzonych przestępstw w latach 2001-2016, źródło danych: Dane Statystyczne Komendy Głównej Policji

W przyszłości należy też oczekiwać większej liczby czynów związanych z rozwojem nowych i aktualnie implementowanych aspektów takich jak Internet Rzeczy, sztuczna inteligencja, blockchain czy też rozwój kryptowalut. Towarzyszące temu wyzwania dla organów ścigania i wymiaru sprawiedliwości będą obejmowały konieczność nieustannego doszkalania się funkcjonariuszy, prokuratorów i sędziów w celu efektywniejszego ścigania oraz zapobiegania przestępstwom. Szczególnie dotyczy to rozwoju Internetu Rzeczy, zjawiska eklektycznie łączącego w sobie specyfikę przestępstw komputerowych i sieciowych. Wymaga to odpowiednich kwalifikacji lub świadomości typu aktualnych i rzeczywistych oraz potencjalnych i przyszłych zagrożeń, w celu odpowiedniego pokierowania czynnościami w postępowaniu przygotowawczym i sądowym.

4.4 Kierunki rozwoju

Punktem odniesienia w przyszłych badaniach naukowych dotyczących cyberprzestępczości, szczególnie dla państw członkowskich Unii Europejskiej, będzie niewątpliwie przyjęta w dniu 6 lipca 2016 roku Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[91]. Dyrektywa ma na celu, między innymi, wprowadzenie obowiązku przygotowania krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych. Ponadto ustanawia nowe środki współpracy i wymiany informacji między państwami członkowskimi takie jak grupa współpracy czy sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieć CSIRT). Mają one na celu ułatwienie wymiany informacji dotyczących usług, operacji i zdolności współpracy pomiędzy różnymi sieciami w obrębie jednego oraz wielu Państw Członkowskich. Dodatkowo mają stanowić platformę wymiany informacji innych niż poufne w celu dyskusji, analizy, wymiany poglądów i omawiania wniosków z działań i ćwiczeń dotyczących bezpieczeństwa sieci i systemów informatycznych w celu poprawy ich działania[92].

Regulacje unijne niewątpliwie stawiają w pierwszym rzędzie na zapewnienie bezpieczeństwa sieci i systemów informatycznych poprzez wymianę informacji pomiędzy Państwami Członkowskimi, co jest słusznym krokiem i postulatem. Ponadto w ramach dyrektywy zaznaczone jest dążenie do ustanowienia we wszystkich Państwach adekwatnego minimum zdolności do zapewnienia tego bezpieczeństwa i podejmowania działań w celu przeciwdziałaniu zagrożeniom. Najważniejszymi środkami, które mają zostać podjęte w celu zapewnienia wysokiego poziomu bezpieczeństwa będzie przyjmowanie przez poszczególne Państwa krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych. Oprócz określenia podstawowych priorytetów działania i powołania zespołów sieci CSIRT, mają zostać określone kompetencje organów krajowych. Ponadto ma nastąpić ustanowienie, w razie potrzeby, punktów kontaktowych, pełniących funkcję łącznikową w razie zbytniego rozproszenia kompetencji pośród różne krajowe organy odpowiedzialne za bezpieczeństwo informatyczne. Dyrektywa podkreśla

[91] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016L1148 (dostęp 30.04.2018).

[92] https://cyberpolicy.nask.pl/cp/inicjatywy/unia-europejska/csirt-network/71,Siec-CSIRT-CSIRT-network.html (dostęp 30.04.2018).

również konieczność zapewnienia i określenia wymogów w zakresie bezpieczeństwa oraz zgłaszania incydentów przez operatorów usług kluczowych. Są to podmioty zapewniające dostęp do usług z zakresu energetyki, transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną i jej dystrybucję oraz infrastruktury cyfrowej[93].

Specyfika Internetu Rzeczy wynika ze jego eklektyzmu. Nie jest to koncepcja będąca całkowicie nowym narzędziem lub sposobem działania, ale raczej platformą umożliwiającą połączenie już istniejących i to zdywersyfikowanych, różniących się od siebie w swoich funkcjonalnościach rozwiązań technicznych. Ułatwia to przygotowywanie i dokonywanie bardziej skomplikowanych oraz wyrafinowanych przestępstw. Większa liczba potencjalnych urządzeń wchodzących w skład koncepcji umożliwia wykorzystanie podatności w większej liczbie urządzeń, przykładowo do zbudowania sieci botnet. Więcej typów maszyn lub komputerów z kolei pozwala na zastosowanie podwyższonej liczby rodzajów i typów szkodliwego oprogramowania niezbędnego do przełamania zabezpieczeń lub zwiększenia skali ataku.

Przytoczone wyżej wnioski płynące z Dyrektywy są na tyle ogólne, że pozwalają na rozpatrywać koncepcję Internetu Rzeczy jako części systemu, mającego zwiększyć poziom bezpieczeństwa sieci i systemów informatycznych. Mimo faktu, że nie jest on wspomniany *explicite* w treści Dyrektywy to może stanowić zagrożenie dla kwestii będących jej przedmiotem. Internet Rzeczy stanowi zagrożenie dla bezpieczeństwa sieci i systemów informatycznych w stopniu nieznanym wcześniej. Struktura budowy i sposób działania urządzeń mogących być częścią tego zjawiska, powoduje, że konieczne jest szersze spojrzenie na problematykę bezpieczeństwa, aniżeli było to dotychczas czynione. Jest to spowodowane ich stopniem skomplikowania oraz połączeniem w ramach kocnecji Internetu Rzeczy wielu aspektów łączności oraz komunikacji bezprzewodowej, przewodowej, a także kwestii informatyzacji, automatyzacji i autonomiczności działania urządzeń i maszyn. Najbardziej palącą i istotną kwestią w tym kontekście jest wspomniana autonomiczność urządzeń umożliwiająca im nie tylko zbieranie danych, ale także wymienianie się nimi. Mogą to czynić także bez wiedzy użytkownika lub jedynie po jego uprzedniej, jednorazowej zgodzie. Skomplikowanie odnoszące się budowy urządzeń

[93] Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016L1148 (dostęp 30.04.2018).

wykorzystujących funkcjonalności koncepcji Internetu Rzeczy dotyczyć może nie tylko fizycznej konstrukcji *per se*, ale także liczby różnych zastosowanych technologii. Nierzadko ich dokładną specyfikę działania rozumie wąska grupa specjalistów, dysponująca kierunkowym wykształceniem informatycznym.

Biorąc pod uwagę powyższe będzie to problematyczną kwestią dla prawników oraz przedstawicieli organów ścigania i wymiaru sprawiedliwości. Pierwszym krokiem powinno być podniesienie świadomości społecznej w zgodzie z poglądami doktrynalnymi, praktycznymi, a także określonymi w ustawach i dokumentach krajowych, wspólnotowych oraz międzynarodowych zasadami. Mogą to być działania *stricte* o charakterze naukowym i badawczym w postaci projektów badawczych, grantów i wystąpień na jak najszerszym forum, ale również o charakterze bardziej społecznym, jak szkolenia skierowane do społeczeństwa, otwarte dla wszystkich lub przygotowane dla konkretnych, specyficznie określonych grup zawodowych. Kwestia uświadomienia zagrożeń w efekcie bezkrytycznego rozwoju urządzeń, wykorzystujących funkcjonalności koncepcji Internetu Rzeczy, a więc także wiedza odnośnie związanych z tym podatności, jest fundamentalną sprawą. Działania podejmowane w następstwie procesu budowania świadomości powinny obejmować pogłębione lub nowe badania naukowe w dziedzinach nauk prawnych, informatycznych oraz innych. Ich efektem z kolei powinno być sformułowanie wniosków *de lege ferenda*, mogące stanowić źródło wiedzy dla ustawodawcy w celu albo dostosowania istniejących przepisów albo napisania nowych oraz *de lege lata*, oceniające skuteczność dotychczas funkcjonujących mechanizmów i przepisów.

Rozdział 5. Internet Rzeczy a kryminalistyka

Kryminalistyka jako nauka o taktycznych sposobach i technicznych metodach oraz środkach służąca do wykrycia przestępstw, a także ustalenia i ujęcia sprawcy oraz możliwości udowadniania istnienia lub braku związku pomiędzy osobami (w tym również sprawcą), miejscami i zdarzeniami z punktu widzenia nowych, rozwijających się przestępstw istotna. Możliwość wypełniania przedstawionej wyżej roli, a także zadań z zakresu przewidywania, rozpoznawania oraz zwalczania przestępczości bywa w przypadku cyberprzestępczości utrudniona. Szczególnie widoczne jest to w przypadku przestępczości związanej z rozwojem komunikacji bezprzewodowej, a więc także Internetu Rzeczy. Omówione poprzednio metody i zdolności do anonimizacji ruchu sieciowego przez użytkowników negatywnie wpływają na możliwości organów ścigania do zwalczania oraz przewidywania przestępstw. Nierzadko stosowane dotychczas, nawet w przypadku cyberprzestępczości, procedury oraz techniki mogą się okazać nieskuteczne lub niewystarczające wobec liczby i jakości potencjalnych dowodów. Wpływ na te aspekty mogą mieć między innymi ulotność niektórych danych informatycznych, brak adekwatnego wyposażenia względem urządzeń wykorzystywanych przez sprawców, a także wobec potencjalnych braków normatywnych i proceduralnych.

Kwestia dowodowa niewątpliwie jest istotna dla procesu karnego, a według niektórych głosów wręcz stanowi problem fundamentalny[94]. Ważność dla procesu karnego implikuje ją także i dla kryminalistyki. W pierwszej kolejności należy zdefiniować pojęcie „dowodu", także w celu lepszego zrozumienia czym może on być w postępowaniach dotyczących przestępczości wykorzystującej podatności lub funkcjonalności Internetu Rzeczy,. Użyte niżej sformułowanie „dowody" będzie oznaczało **środki dowodowe, rozumiane jako „nośnik informacji o fakcie podlegającym udowodnieniu"**[95]. W doktrynie brak jest jednolitego stanowiska, co do desygnatu znaczeniowego pojęcia dowodu lub dowodów. Sam P. Horoszowski, którego definicja została przytoczona wyżej, przedstawia osiem możliwości rozumienia tego pojęcia. Sygnalizuje przy tym, że w istocie najlepszym byłoby zarezerwowanie tego pojęcia dla rezultatu dowodzenia. Pozwoliłoby to

[94] T. Gardocka, *Zasady postępowania dowodowego w polskim procesie karnym*, w: T. Gardocka, D. Jagiełło (red.), *Zagadnienie dowodowe w procesie karnym*, C.H. Beck, Warszawa 2017.

[95] S. Waltoś, P. Hofmański, *Proces karny. Zarys systemu*, Wolters Kluwer, Warszawa 2016.

na uporządkowanie chaosu terminologicznego, funkcjonującego w przestrzeni nazewnictwa w tej materii[96]. S. Waltoś przyznaje mu rację w kwestii, że istnieje zbyt dużo znaczeń tego pojęcia. Jednakże jednocześnie stwierdza, że postulat uporządkowania kwestii w tym wymiarze jest niemożliwy do spełnienia z uwagi na „zbyt silne przyzwyczajenia językowe" i zbyt wiele „różnych koncepcji terminologicznych"[97]. Niewątpliwie należy uznać, że nadmierny chaos w posługiwaniu się terminologią oraz wieloznaczność i brak ujednolicenia siatki pojęciowej jest szkodliwy z punktu widzenia nauk z zakresu kryminalistyki, prawa karnego materialnego i procesu karnego. Powstające w ten sposób nieścisłości wpływają negatywnie na prowadzone badania naukowe z dziedziny prawa, a także w działalności dydaktycznej. W konsekwencji prowadzi to do sytuacji, gdy osoby wydawałoby się mówiące o tym samym, używają do tego innych określeń. Możliwą do wyobrażenia sobie jest sytuacja, gdy sędzia w sprawie karnej posługuje się inną siatką pojęciową niż adwokat lub prokurator. To z kolei może implikować trudności w realizacji praw wynikających z przepisów prawa karnego, jak przykładowo pełną realizację prawa do obrony lub niedopuszczanie niektórych wniosków dowodowych. Waga postępowania dowodowego w realizacji zadań procesu karnego jako zorganizowaniu go w taki sposób, „aby toczyło się ono rzetelnie i uczciwie w stosunku do stron, względnie innych uczestników"[98] jest nie do przecenienia. Realizuje się również w ten sposób także postanowienia Konstytucji RP, a konkretnie art. 45 ust. 1 – prawo do sprawiedliwego procesu[99].

Podsumowując dywagacje dotyczące semantycznej strony pojęcia „dowód" należy stwierdzić, że zarówno P. Horoszowski, jak i S. Waltoś w swoich analizach nie odbiegają od angielskiego znaczenia słowa *evidence*. Według *Longman Dictionary of Contemporary English* słowo *evidence* można rozumieć dwojako: jako **fakt lub znak, który jasno pokazuje, że coś istnieje lub jest prawdziwe** bądź jako **informacja przedstawiana w sądzie, mająca stanowić dowód na winę lub niewinność**[100]. Biorąc poprawkę na

---

[96] P. Horoszowski, *Nazwa i pojęcie „dowodu" w teorii i praktyce prawa sądowego*, „Państwo i Prawo" 1956, nr 10.

[97] S. Waltoś, P. Hofmański, *Proces*…, op. cit.

[98] J. Skorupka, *Sprawiedliwość proceduralna jako cel procesu karnego*, w: J. Skorupka (red.), *Rzetelny proces karny. Księga jubileuszowa Profesor Zofii Świdy*, Wolters Kluwer,Warszawa 2009.

[99] A. Skowron, *Rzetelny proces karny w ujęciu Karty Praw Podstawowych Unii Europejskiej oraz Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, „Prokuratura i Prawo" 2017, nr 11.

[100] *Longman Dictionary of Contemporary English*, https://www.ldoceonline.com/dictionary/evidence (dostęp 30.04.2018).

niedoskonałości wynikające z tłumaczenia z języka angielskiego na polski można stwierdzić, że przyjęte w niniejszej pracy znaczenie słowa „dowód" zbliżone jest do angielskiego znaczenia słowa *evidence*. Istniejące nie tylko w Polsce, ale również i za granicą rozbieżności w rozumieniu znaczenia pojęcia „dowód", wskazują na potrzebę dążenia do jednolitości w warstwie semantycznej. Nawet mimo występujących i naturalnych przeszkód w postaci ugruntowanych przekonań i przyzwyczajeń. Rolą doktryny i praktyki jest także przezwyciężanie szkodliwych, choć ugruntowanych, limitacji.

Biorąc pod uwagę charakter przestępczości wykorzystującej funkcjonalności lub podatności Internetu Rzeczy niewątpliwie podstawowym pojęciem będącym w kręgu zainteresowań jest dowód cyfrowy. Rozumiany on będzie jako **informacja w formie cyfrowej o znaczeniu dowodowym**[101]. Departament Sprawiedliwości Stanów Zjednoczonych Ameryki posługuje się z kolei następującą definicją: „informacje i dane mające wartość dla postępowania, przechowywane, pobierane lub wysyłane przy pomocy urządzenia elektronicznego"[102]. Jest to być może bardziej szczegółowa definicja, jednak niepełna, ponieważ nie obejmuje wszystkich możliwych czynności, którymi dane informatyczne czy też szerzej informacje mogą podlegać. Wartościowym wydaje się, że określenie „mające wartość dla postępowania", gdyż w ten sposób nie determinuje się czy chodzi o pozytywną czy też negatywną wartość lub czy chodzi o wartość dla oskarżenia, obrony czy też sądu.

Z perspektywy możliwości Internetu Rzeczy oraz potencjału do wykorzystania tego zjawiska do popełniania przestępstw, pojęcie i kwestia dowodu cyfrowego jest sprawą fundamentalną. W przypadku cyberprzestępczości dowód cyfrowy jest często najważniejszym lub jedynym źródłem informacji dla organów ścigania o znaczeniu dowodowym. To samo dotyczyć będzie przestępstw wykorzystujących podatności lub funkcjonalności Internetu Rzeczy. W przypadku tego zjawiska niewątpliwie najważniejszym elementem, który należy brać pod uwagę jest fakt, że za sprzęt komputerowy nie należy uznawać tylko jednostek komputerowych, laptopów i urządzeń podobnych. Wszelkiego rodzaju sprzęt elektroniczny wyposażony w zdolność komunikacji

---

[101] A. Lach, *Dowody elektroniczne w postępowaniu karnym*, Towarzystwo Naukowe Organizacji i Kierownictwa, Toruń 2004.

[102] M.B. Mukasey, J.L. Sedgwick, D.W. Hagy, *Electronic Crime Scene Investigation: A Guide for First Responders*, U.S. Department of Justice, Office of Justice Programs, Washington 2008, za: P. Karasek, *Dowód cyfrowy – aspekty kryminalistyczne*, praca mgr niepubl., Warszawa 2014.

bezprzewodowej i posiadający funkcjonalności spełniające warunku przynależności do koncepcji Internetu Rzeczy powinny być rozpatrywane przez śledczych jako potencjalne źródło dowodów w postępowaniu karnym. Korzystnym z punktu widzenia rozważań dotyczących źródeł dowodów i informacji jest wskazanie klasyfikacji oraz typologii dowodów cyfrowych. Jedną z nich jest rozróżnienie na *dane cyfrowe uzyskane w czasie rzeczywistym, w drodze podsłuchu elektronicznego lub gromadzenia danych o ruchu sieciowym z komputera użytkownika (faza dynamiczna)*[103]. Natomiast drugą kategorią są *dane uzyskane już w fazie ich przechowywania w systemie komputerowym lub na nośnikach danych (faza statyczna)*[104]. Z kryminalistycznego punktu widzenia obie powyższe kategorie z uwagi na ich funkcjonalność i przydatność w postępowaniu dowodowym są wystarczające jako ogólne kryterium podziału typologicznego dowodów cyfrowych. Rozróżnienie to pozwala na wskazanie, że istnieją dane o charakterze ulotnym, wymagające innego podejścia i procedur ich zabezpieczania niż dane, które można zabezpieczyć w fazie statycznej. Wskazanie tej dyferencjacji jest istotne, szczególnie w przypadku cyberprzestępczości. Nadrzędnym celem przyświecającym osobom zabezpieczającym dowody cyfrowe jest przeprowadzenie działań w sposób umożliwiający wykorzystanie ich w postępowaniu przygotowawczym, a następnie na etapie postępowania sądowego. Wartość dowodów wykorzystywanych w trakcie obu wyżej wymienionych etapów procesu karnego zależy od ich zapewnienia **autentyczności**, **poufności** oraz **integralności** zabezpieczonych danych oraz informacji.

W odniesieniu do kwestii zabezpieczania dowodów cyfrowych w przypadku przestępstw wykorzystujących podatności lub funkcjonalności Internetu Rzeczy, powstaje przede wszystkim pytanie co do typu i liczby urządzeń niezbędnych do zabezpieczenia, aby zapewnić prawidłowy i zgodny z zasadami oraz prawem przebieg postępowania. Czy powinien to być jedynie sprzęt komputerowy, który zostanie skierowany na dokładne badania, a następnie do ekspertyzy informatycznej według określonych procedur? Czy też należy zabezpieczyć jedynie informacje znajdujące się na serwerze lub serwerach używanych przez sprawcę, zbadanie jego ruchu sieciowego, a następnie analiza uzyskanych w ten sposób informacji? W myśl zdrowego rozsądku zdawałoby się, że najodpowiedniejszym byłoby wyważenie obu tych stanowisk i wykorzystanie w pełni możliwości oraz potencjału jaki dają dowody cyfrowe, ich zabezpieczanie oraz wnioski z

[103] A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000.
[104] Ibidem.

przeprowadzonej analizy. Wpierw jednak istotnym do rozważenia jest problem podstaw prawnych czynności podejmowanych w toku postępowania przygotowawczego oraz sądowego, ze szczególnym uwzględnieniem tych istotnych dla prowadzenia postępowań wobec przestępstw wykorzystujących podatności lub funkcjonalności Internetu Rzeczy. Oznacza to także ocenę, jakie już w tym momencie istnieją problemy natury dogmatycznej lub proceduralnej uniemożliwiające lub oddziałowujące negatywnie na skuteczność podejmowanych czynności śledczych oraz dowodowych.

5.1 Podstawy prawne zabezpieczania dowodów cyfrowych

Podstawą prawną dla podejmowania czynności kryminalistycznych na miejscu zdarzenia w przypadku przestępstw komputerowych są przepisy kodeksu postępowania karnego (dalej jako k.p.k.)[105]. Dla zabezpieczenia dowodów cyfrowych, czyli najistotniejszych z punktu widzenia charakteru cyberprzestępczości, najważniejsze będą przepisy działu V (Dowody) k.p.k., a konkretnie rozdziałów: 19 (Przepisy ogólne działu V), 22 (Biegli, tłumacze, specjaliści), 23 (Oględziny. Otwarcie zwłok. Eksperyment procesowy) oraz 25 (Zatrzymanie rzeczy. Przeszukanie). Nie są to jedyne źródła mogące służyć za podstawę podejmowania szeroko pojętych czynności kryminalistycznych, zarówno czynności procesowych, jak i pozaprocesowych.

W polskim porządku prawnym dane elektroniczne (także cyfrowe) ogólnemu reżimowi przepisów dotyczących dowodów. Przepisy dotyczące danych elektronicznych zostały wprowadzone do polskiego systemu prawnego w wyniku implementacji Cyberkonwencji. Najważniejsze regulacje k.p.k. to art. 218a i 236a kodeksu postępowania karnego, które określają obowiązek urzędów, instytucji i podmiotów prowadzących działalność telekomunikacyjną do niezwłocznego zabezpieczenia danych informatycznych i elektronicznych na żądanie sądu lub prokuratora. To samo dotyczy administratora lub użytkownika urządzenia zawierającego dane informatyczne lub elektroniczne oraz systemu informatycznego. Wykładnia literalna przepisów nie dostarcza żadnych szczegółów. Zamiast tego k.p.k. odsyła do rozporządzenia Ministra Sprawiedliwości z dnia 28 kwietnia

[105] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz. U. z 2020 r., poz. 30 z późn. zm.).

2004 r. [106] jako źródła szczegółowego odnośnie zabezpieczania danych informatycznych w urządzeniach oraz w systemach i przechowywanych na informatycznych nośnikach danych[107]. Nie określa ono szczegółowych sposobów zabezpieczenia technicznego danych informatycznych, tak jak można by było oczekiwać po treści art. 218b k.p.k. Rozporządzenie wydane jako uszczegółowienie procesu zabezpieczania dowodów cyfrowych nie wybiega treścią o wiele dalej niż przepisy Cyberkonwencji z 2001 r. Podobnie doktryna w komentarzach do k.p.k. odnosi się jedynie do wspomnianego rozporządzenia[108]. Co więcej, rozporządzenie nie było od czasu jego wydania zmieniane.

Skąpe i nie wychodzące poza obowiązki implementacyjne umowy międzynarodowej sformułowanie przepisów dotyczących procesu pozyskiwania dowodów cyfrowych może oddziaływać negatywnie na zdolności śledcze organów ścigania. Głównym negatywnie wpływającym na ten fakt czynnikiem jest odesłanie do dokumentu, rzekomo uszczegółowiającego proces, który *de facto* nie spełnia tej funkcji. Wskazanie w treści wspomnianego wyżej rozporządzenia jedynie wymogów dokumentacyjnych, nie odbiegających znacznie od tych obowiązujących w przypadku innych czynności zabezpieczania dowodów kryminalistycznych, nie jest korzystne. Nie wprowadza nic z kryminalistycznego, a więc także praktycznego punktu widzenia. Zainteresowany technik musiałby sam podjąć decyzję, bazując na swojej wiedzy oraz doświadczeniu lub wytycznych od zwierzchnika, który model zabezpieczenia dowodów powinien zastosować. Uszczegółowienie rozporządzenia wraz ze wskazaniem być może więcej niż jednego modelu postępowania w przypadku zabezpieczania dowodów cyfrowych byłoby korzystne. W perspektywie może wzmocnić zdolności śledcze i efektywność prowadzenia postępowań organów ścigania. Na poziomie przepisów prawa nie wydaje się, żeby była konieczna ogromna zmiana. Postulatem przydatnym może być za to dokonanie przeglądu regulacji prawnych i ewentualna aktualizacja ich w razie zaistnienia takiej potrzeby.

---

[106] Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz. U. Nr 100, poz. 1023).

[107] Art. 218b *in fine* k.p.k.

[108] Por. K. Eichstaedt, *Art. 218(b),* w: D. Świecki (red.), *Kodeks postępowania karnego. Tom I. Komentarz aktualizowany*, LEX/el. 2020 lub R.A. Stefański, S. Zabłocki, *Art. 218(b)* w: R.A. Stefański, S. Zabłocki, *Kodeks postępowania karnego. Tom II. Komentarz do art. 167–296,* Wolters Kluwer Polska, Warszawa 2019.

5.2 Przegląd wybranych modeli i procedur zabezpieczania dowodów cyfrowych

W Polsce brak jest skodyfikowanych i ujednoliconych szczegółowych procedur odnoszących się do zabezpieczania dowodów cyfrowych. Z uwagi na to należy sięgać do fragmentów z wielu różnych procedur stosowanych w przypadku przestępstw. Jednym z nich są wytyczne stosowane w przypadku przestępstw o charakterze gospodarczym i korupcyjnym do stosowania przeznaczone są procedury *European Anti-Fraud Office* - OLAF[109], czyli biura Komisji Europejskiej zajmujące się zwalczaniem korupcji w unijnych instytucjach oraz oszustwom na szkodę budżetu Unii Europejskiej. W odniesieniu do napotkanych w toku postępowań urządzeń lub danych informatycznych najważniejszymi czynnościami do wykonania na miejscu zdarzenia są udokumentowanie zastanego stanu rzeczy i dokonywanych czynności, w tym sporządzenie spisu sprzętu cyfrowego, ocena zabezpieczonych wstępnie urządzeń w celu ustalenia, które należy poddać dalszym czynnościom, stworzenie bezpiecznej kopii uzyskanych danych, sporządzenie dokumentacji końcowej opisującej sposób uzyskania nośników i urządzeń zabezpieczonych w trakcie czynności, sposób ich zabezpieczenia i przechowywania oraz zawarcie w dokumentacji wszelkich uwag i sugestii co do przeprowadzanych czynności. Dodatkowo jako odpowiedni sposób przechowywania sprzętu wymienia się zaszyfrowanie dysków twardych, plastikowe worki antystatyczne zabezpieczone pieczęciami oraz inne ochronne opakowania i torby umożliwiające transport zabezpieczonych urządzeń w sposób bezpieczny oraz nie wywołujący uszkodzenia nośników i potencjalnych dowodów. Na każdym etapie czynności powinny być wykonywane oraz nadzorowane przez pracowników dysponujących odpowiednimi kwalifikacjami i akredytacjami, w celu zapewnienia pewności i integralności postępowania dowodowego, tzw. „łańcucha dowodów" (ang. *chain of evidence*).

Oprócz wspomnianego wyżej wyróżnić można następujące funkcjonujące i opisane modele zabezpieczania dowodów cyfrowych:

1. **SRDFIM** (ang. Symantec Digital Forensic Investigation Model), w którym wyróżniono 11 faz działania: przygotowania, zabezpieczenia miejsca zdarzenia,

[109] *Guidelines on Digital Forensic Procedures for OLAF Staff*, https://ec.europa.eu/anti-fraud/sites/antifraud/files/guidelines_en.pdf (dostęp 30.04.2018).

wstępnej oceny sytuacji, udokumentowania miejsca zdarzenia odcięcia środków komunikacji, zebrania dowodów cyfrowych, zabezpieczenia dowodów cyfrowych, analizy wstępnej, analizy właściwej, prezentacji i oceny następczej[110],

2. **DFRW** (ang. Digital Forensics Research Workshop) wyróżnia 7 kroków: identyfikacji problemu, zabezpieczenia miejsca, zebrania dowodów, analizy danych, przygotowania opinii, prezentacji dowodu i decyzji końcowej[111],
3. **The Abstract Digital Forensics Model** rozróżnia 9 etapów postępowania: identyfikacji problemu, przygotowania, planowania, zabezpieczenia miejsca, zebrania dowodów, wstępnej analizy danych, przygotowania opinii, prezentacji dowodu, prezentacji dowodu oraz zwrotu zatrzymanego sprzętu właścicielowi[112],
4. **ADAM** (ang. Advanced Data Acquisition Model) dokonuje rozróżnienia jedynie na 3 etapy: planowania wstępnego, ponownego planowania (dokonywanego na miejscu zdarzenia) i zabezpieczenia danych[113],
5. **ACPO** (ang. *Association of Chief Police Officers*) wymienia 4 fazy jako główne i zasadnicze dla dokonywania czynności zabezpieczania dowodów cyfrowych: planowania, zabezpieczania, analizy i prezentacji[114].

Wymienione powyżej modele postępowania w sprawie zabezpieczania dowodów cyfrowych odnoszą się w dużej mierze do taktyki dokonywania czynności

[110] Część wyszczególnionych w ramach tej procedury faz działania pokrywa się z ogólnymi zasadami dokonywania oględzin miejsca zdarzenia, co sprawia, że jest wymienionych aż 11 faz; ponadto w celu większej efektywności dokonywania tej procedury można by zrezygnować z wyszczególniania niektórych faz. A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta, *Systematic digital forensic investigation model*, „International Journal of Computer Science and Security" 2011, t. 5(1).

[111] Kroki wyróżnione w tej procedurze wydają się zbyt ogólne, aby mogły być szczegółowymi wytycznymi dokonywania czynności dowodowych *sensu largo*, jednak są odpowiednie jako swoisty wstęp do rozważań nad postępowaniem z dowodami cyfrowymi, ale także ze wszelkimi innymi dowodami, choć bardziej na poziomie akademickim aniżeli specjalistycznym. M. Kohn, J.H.P. Eloff, M.S. Olivier, *Framework for a Digital Forensic Investigation*, Information and Computer Security Architectures Research Group (ICSA), Department of Computer Science, University of Pretoria, https://www.researchgate.net/publication/220803284_Framework_for_a_Digital_Forensic_Investigation, (dostęp 30.04.2018), za: National Institute of Justice, *Results from Tools and Technology Working Group*, Governors Summit on Cybercrime and Cyberterrorsism, Princeton 2002.

[112] Wobec tej procedury można wysnuć podobne zarzuty jak wobec poprzednio wymienionej, choć niewątpliwie byłoby ich mniej z uwagi na jej większe rozbudowanie i położenie większego nacisku na szczegóły. M. Reith, C. Carr, G. Gunsch, *An examination of digital forensic models*, „International Journal of Digital Evidence" 2002, t. 1(3).

[113] R.B. Adams, *The Advanced Data Acquisition Model (ADAM): a Process Model for Digital Forensic Practice*, Murdoch University 2012.

[114] J. Williams, *ACPO Good Practice Guide for Digital Evidence*, Association of Chief Police Officers, marzec 2012, http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf (dostęp 30.04.2018).

kryminalistycznych. Można zauważyć podobieństwa między nimi, posiadają one wspólne punkty, a wszystkie z nich w pewien sposób starają się odpowiedzieć na 7 złotych pytań kryminalistyki. Zdecydowanym postulatem każdej z nich jest to, aby czynności w odniesieniu do zabezpieczania dowodów cyfrowych dokonywane były przez osoby odpowiednio wyszkolone i wykwalifikowane do ich podejmowania. Bez tego istnieje ryzyko braku możliwości wykorzystania ich w postępowaniu dowodowym z uwagi na ich nikłą jakość, wartość dowodową lub niedochowanie procedur, a więc możliwe niespełnienie wymogów legalności.

Jak to zostało już zaznaczone powyżej, w Polsce nie ma jednolicie przyjętego systemu lub modelu czynności dotyczących dowodów cyfrowych. P. Karasek wskazuje, że w piśmiennictwie polskim najczęściej przywoływanym modelem jest ACPO[115], który wyróżnia cztery główne fazy podejmowanych czynności. Ograniczenie się do określenia głównych, objętościowo dużych, etapów zamiast wyróżnienia większej liczby, bardziej szczegółowych, pozwala z jednej strony na wykorzystanie ich częściej, do większe liczby postępowań. Natomiast z drugiej brakuje im szczegółowości, nierzadko oczekiwanej od konkretnych, szczegółowych modeli procedur, które mają się różnić od przepisów prawa. Brak specyfikacji i większej konkretyzacji powoduje, że procedury niewiele różnią się od ogólnych przepisów prawa dotyczących zabezpieczania dowodów cyfrowych i mają przez to nikły wpływ oraz znaczenie dla nauk kryminalistycznych. Oczekiwać należy albo uszczegółowiania istniejących ogólnych modeli zabezpieczania dowodów cyfrowych albo przy tworzeniu nowych dookreślania ich w sposób pozwalający na wykorzystanie w praktyce bez sięgania do innych źródeł lub opracowań. W ten sposób spodziewać się można pozytywnych zmian, wpływających na efektywność postępowań prowadzonych przez organy ścigania.

Przyjmując lub adaptując któryś z modeli jako ogólnonarodowy lub międzynarodowy standard postępowania w sprawach dotyczących cyberprzestępczości, należy odchodzić od tych zbyt generalnych lub wręcz wtórnych treściowo wobec przepisów prawa. O ile przepisom generalność i lakoniczność semantyczna jest potrzebna i nierzadko niezbędna, o tyle procedury kryminalistyczne w wyniku zbyt dużego poziomu ogólności tracą na swojej funkcjonalności. Określenie obowiązków oraz opatrzenie ich wskazaniem odpowiednich technicznych metod i sposobów zabezpieczania dowodów

[115] P. Karasek, *Dowód cyfrowy – aspekty kryminalistyczne*, praca mgr niepubl., Warszawa 2014.

cyfrowych, należy uznać za pożądany kierunek, szczególnie w przypadku cyberprzestępczości. Dodać do tego można postulat nieustannego aktualizowania przyjętych modeli lub modelu w związku z postępem technicznym i technologicznym oraz wykrywanymi zagrożeniami dla bezpieczeństwa.

5.3 Ogólne zasady kryminalistycznego zabezpieczania dowodów

Najważniejsze zasady informatyki kryminalistycznej są stosunkowo uniwersalne, niezależnie od ich źródła. W polskiej literaturze wartymi odnotowania są wyróżnione przez A. Lacha „zasady naczelne informatyki śledczej". Obejmują takie wnioski jak wskazanie kompetencji z zakresu informatyki śledczej specjalisty lub biegłego, a także jego wiedzy i doświadczenia, wykonywanie wszelkich czynności na kopiach nośników, dokonywanie zabezpieczenia danych w sposób umożliwiający zweryfikowanie ich integralności, w szczególności z zastosowaniem sumy kontrolnej, należyte udokumentowanie wszelkich czynności podjętych w toku zabezpieczenia dowodów cyfrowych, odpowiednią priorytetyzację dowodów w trakcie ich zabezpieczania w celu uniknięcia ich utraty oraz inne, które są ogólne dla ogólnego postępowania odnoszącego się do zabezpieczania śladów kryminalistycznych do celów dowodowych. Ogólne zasady informatyki kryminalistycznej mają wpływ na formułowane w doktrynie ogólne zasady zabezpieczania dowodów cyfrowych, a wręcz w ogromnej części są ze sobą tożsame. w ich myśl w celu zabezpieczenia śladów cyfrowych powinno się wezwać eksperta z zakresu informatyki kryminalistycznej[116]. Wszelkie osoby uczestniczące i biorące udział w zabezpieczanie śladów cyfrowych powinny posiadać wiedzę z zakresu informatyki oraz specyfikacji urządzeń lub urządzenia, na którym dokonywane będą czynności, aby zniwelować lub zminimalizować ryzyko utraty, uszkodzenia lub nieprawidłowego zabezpieczenia danych znajdujących się na nośniku. Informacje, które będą niezbędne dla eksperta to m.in. rodzaj sprzętu i środowiska komputerowego tzn. rodzaj systemu operacyjnego, pamięci konfiguracji sieci, ilości i typu urządzeń. Konieczne będzie również zdeterminowanie w jakich warunkach dokonywane będzie zabezpieczanie śladów, czy w ramach czynności przeszukania, w czasie obecności lub nie administratorów danych systemów i urządzeń, ale także stwierdzenie stanu działania systemu – czy jest włączony, czy nie, w trakcie

[116] W. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Difin, Warszawa 2015.

tworzenia kopii zapasowej, aktualizacji lub innej czynności. Urządzenia wyłączonego nie należy włączać, a gdy dokonuje ono jakichś czynności należy pozwolić mu je dokończyć i nie należy zamykać uruchomionych programów. Dostosowanie działań ma też na celu uniknięcie utraty danych albo czy istnieje możliwość ich zdalnego usunięcia przez użytkownika danego urządzenia.

Kryminalistyczna analiza Internetu Rzeczy obejmuje zarówno rozważania w obrębie techniki i taktyki kryminalistycznej. Prof. Hanausek definiuje technikę kryminalistyczną jako *dział obejmujący metody, środki i sposoby wykorzystywania zdobyczy nauk technicznych i przyrodniczych oraz własnych osiągnięć kryminalistyki do realizacji funkcji tej nauki, głównie w sferze badania informacji i ich źródeł pochodzących od dowodów rzeczowych i śladów*[117]. Natomiast taktyka kryminalistyczna to *dział obejmujący naukę o celowych i skutecznych metodach szybkiego oraz zgodnego z etyką zawodową i prawem osiągania zamierzonych celów określonych funkcjami kryminalistyki*. Obejmuje ona także *zasady celowego i efektywnego wykorzystania środków technicznych w walce z przestępczością*[118].

Z punktu widzenia techniki kryminalistycznej i jej znaczenia dla postępowania dowodowego, a szerzej także dla procesu karnego, najistotniejsze jest odpowiednie zabezpieczenie śladów kryminalistycznych w celu wykorzystania ich jako dowody w postępowaniu. Cyberprzestępczość niesie ze sobą nowe wyzwania w powyższym aspekcie. Aktualnie wykorzystywane są nie tylko znane od wielu lat metody takie jak analiza kryminalna, ale również nowe narzędzia, inne niż w przypadku tradycyjnych dziedzin kryminalistyki takich jak daktyloskopia, mechanoskopia czy balistyka. Zabezpieczanie i analiza tego typu śladów wymaga innego zestawu umiejętności oraz posiadania wiedzy także z zakresu informatyki, chociażby w zakresie umożliwiającym rozróżnienie podstawowych pojęć. Do bardziej zaawansowanych technicznie czynności można skorzystać z wiedzy specjalistycznej np. biegłego czy też odpowiednio wykwalifikowanego i wykształconego pracownika lub eksperta.

Internet Rzeczy jako zjawisko i koncepcja jest czymś nowym, jednak w ramach swojego działania wykorzystuje rozwiązania znane z innych urządzeń elektronicznych i komputerowych. Głównie są to technologie łączności internetowej i bezprzewodowej

[117] T. Hanausek, *Kryminalistyka*…, op. cit.
[118] Ibidem.

takie jak na przykład WiFi[119], Bluetooth[120] oraz UPnP[121]. Ich głównym punktem wspólnym jest umożliwienie, i w znacznym stopniu ułatwienie, komunikacji bezprzewodowej i internetowej, a przez to wymianę i zbieranie danych o urządzeniach podłączonych do tych sieci. W kontekście przestępczości wykorzystującej funkcjonalności lub podatności Internetu Rzeczy należy zwrócić szczególną uwagę na UPnP. W samym założeniu leżącego u podwalin działania tego zestawu protokołów sieciowych jest możliwość wykrywania i odnajdywania innych urządzeń czy też punktów, te protokoły obsługujących oraz znajdujących się w tej samej lokalnej sieci LAN (ang. *Local Area Network*). Wykorzystuje się go w wielu tysiącach przedmiotów i urządzeń, co przekłada się na ich liczbę liczoną nawet w milionach, jak wskazuje raport Rapid 7[122]. Według przeprowadzonych przez nich testów i badań, na żądanie wysłane przy użyciu UPnP komunikat zwrotny przesłało 81 milionów unikalnych adresów IP. Tak jak to zostało wspomniane wyżej, mogą to być różnego typu urządzenia takie jak routery, drukarki, kamery bezprzewodowe, serwery, telewizory, systemy sieciowego przechowywania plików, zautomatyzowane systemy zarządzania domem oraz inne. Ku zaskoczeniu badaczy aż 20% z 81 milionów adresów IP udostępniło również SOAP (*Simple Object Access Protocol*)[123], protokół komunikacyjny umożliwiający osobom trzecim wykrycie potencjalnych celów do przeprowadzenia ataku na system.

Sama możliwość zidentyfikowania jest już wystarczającym zagrożeniem dla użytkownika, natomiast kwestia braku zabezpieczenia urządzeń i systemów przed wysyłaniem protokołu SOAP stwarza jeszcze większe niebezpieczeństwo. Wykorzystanie tej podatności niesie ze sobą znamienne negatywne skutki. Po pierwsze zwiększa się liczba

---

[119] WiFi, inaczej Wi-Fi – technologia służąca tworzeniu bezprzewodowych lokalnych sieci internetowych za pomocą urządzeń opartych na specyfikacji IEEE 802.11, za: Wikipedia, https://en.wikipedia.org/wiki/Wi-Fi (dostęp 30.04.2018).

[120] Bluetooth – technologia służąca do bezprzewodowego przesyłania i wymiany danych na krótkich odległościach, za pomocą fal decymetrowych (fal radiowych UHF) między urządzeniami stacjonarnymi lub mobilnymi, za: Wikipedia, https://en.wikipedia.org/wiki/Bluetooth (dostęp 25.04.2018).

[121] *Universal Plug and Play* – zestaw protokołów sieciowych, który umożliwia urządzeniom sieciowym, m.in. komputerom, drukarkom, routerom, bramkom sieciowym, punktom dostępu Wi-Fi i urządzeniom mobilnym, wykrywanie nawzajem swojej obecności w sieci i ustanawianie połączeń sieciowych do wymiany danych i komunikacji, za: Wikipedia, https://en.wikipedia.org/wiki/Universal_Plug_and_Play (dostęp 25.04.2018).

[122] *Security Flaws in Universal Plug and Play*, Rapid 7 White Paper, https://information.rapid7.com/rs/411-NAK-970/images/SecurityFlawsUPnP%20%281%29.pdf (dostęp 30.04.2018).

[123] *Simple Object Access Protocol* – protokół komunikacyjny, zaprojektowany w celu wymiany i przekazywania informacji odnośnie do implementacji usług sieciowych w sieciach komputerowych, za: Wikipedia, https://en.wikipedia.org/wiki/SOAP (dostęp 25.04.2018).

potencjalnych celów, a przez to urządzeń wymagających łatania luk w zabezpieczeniach lub przeszukania i przeanalizowania w razie dokonania przestępstwa. Zakładając, co nie jest oczywiste, że funkcjonariusz wykonujący lub nadzorujący czynność oględzin sprzętu elektronicznego oraz prokurator kierujący nimi mają wiedzę i świadomość, jak wiele sprzętów może być wykorzystywanych do popełnienia tego typu przestępstwa, to można sobie wyobrazić jak wiele wyzwań ta sytuacja implikuje. Może to wpływać na całkowitą zmianę taktyki dokonywania oględzin, priorytetyzacji przedmiotów mających być zabezpieczonych. Liczba przedmiotów wyposażonych w moduły komunikacji bezprzewodowej jest obecnie ogromna. Przywołany wyżej raport wspomina o kilku tysiącach różnego typu sprzętów obsługujących zestaw protokołów UPnP. Stwarza to zupełnie nowe wyzwania z punktu widzenia taktyki kryminalistycznej. Wymaga to zaplanowania czynności na miejscu zdarzenia przez organy ścigania w sposób zapewniający możliwość zabezpieczenia wszystkich urządzeń, mogących być źródłami dowodów, dbając przy tym jednocześnie o aspekt czasowy. Liczba urządzeń determinuje także dobór specjalistów wchodzących w skład ekipy mającej dokonać czynności lub wymaganej do sprowadzenia na miejsce oględzin. Istotnym aspektem jest także wyposażenie, którym dysponują organy ścigania w danym momencie i miejscu – nie w każdym będzie to identyczna sytuacja. Prawidłowa identyfikacja problemów oraz określenie powyższych problemów w wysokim stopniu daje rękojmię prawidłowego i wartościowego z punktu widzenia procesu karnego przebiegu oględzin.

Na marginesie rozważań o dowodach cyfrowych należy odnieść się do kwestii zaufania odnośnie zabezpieczonych plików. Szczególnie w dobie szerokiego dostępu do wszelkiego rodzaju programów umożliwiających modyfikację graficzną, tekstową, skryptową lub jakąkolwiek inną związaną z manipulowaniem albo zmienianiem przeznaczenia lub struktury plików i danych. Najistotniejszymi wpływającymi na poziom zaufania do zabezpieczonych dowodów cyfrowych będą choćby takie czynniki jak brak wiedzy odnośnie podejmowanych przez techników lub ekspertów czynności lub ogólnie sposobu działania urządzeń i oprogramowania, a także niewłaściwe nastawienie lub zbytnia ufność w stosunku do zabezpieczonego materiału dowodowego[124]. W skrajnej formie oznacza to nadawanie mu przymiotu faktów, bez przeprowadzenia procesów analitycznych czy interpretacyjnych, jak ekspertyza z zakresu informatyki śledczej.

[124] E. Casey, *Trust in digital evidence*, „Digital Investigation" 2019, t. 31, https://doi.org/10.1016/j.fsidi.2019.200898.

Kwestia braku lub niedostatku wiedzy odnośnie procesów informatycznych, cyfrowych lub sieciowych może mieć doniosłe znaczenie z prawnego punktu widzenia. Nie sposób dokonywać adekwatnej i realizującej prawo do obrony walidacji zaprezentowanego materiału zebranego w sprawie bez choćby podstawowej wiedzy w zakresie działania urządzeń. Częściowo obowiązek przedstawienia dowodów w sposób zrozumiały dla organów ścigania oraz wymiaru sprawiedliwości spoczywać będzie na ekspercie lub wyznaczonym specjaliście, choćby spośród przedstawicieli policji. Podejmowane przez niego czynności powinny być utrwalone i następnie przekazane w sposób zrozumiały i odpowiadający na jak największą liczbę potencjalnych pytań lub wątpliwości osób nieposiadających wiedzy specjalistycznej. Z tej perspektywy istotne jest, aby nie wpaść w pułapkę wiedzy eksperta (przyjęcia, że odbiorca ma tę samą wiedzę o danym zjawisku co przekazujący informacje) lub przyjęcie informacji znalezionych za fakty, co spowoduje nie przeprowadzenie choćby sprawdzenia wiarygodności materiału dowodowego, sposobu w jaki mógłby zostać wprowadzony do urządzenia lub innych. Niezadbanie o zapewnienie wiarygodności dowodom cyfrowym lub sieciowym prezentowanym w sprawie może prowadzić do niewłaściwego z nimi postępowania, nieujawnienia istotnych faktów, błędnej interpretacji, a w efekcie błędnego wyjaśnienia stanu faktycznego sprawy.

5.4 Wybrane aspekty zabezpieczania dowodów sieciowych

W kontekście rozważań dotyczących zabezpieczania dowodów sieciowych, Są to dowody zabezpieczone w toku czynności określanych mianem kryminalistyki sieciowej (ang. *Network Forensics*). Jest to wykorzystanie naukowych metod do gromadzenia, badania, korelowania, analizowania, identyfikacji i dokumentowania dowodów cyfrowych z wielu, aktywnie przetwarzających i przekazujących dane źródeł cyfrowych. Ma to na celu wykrycie faktów lub działań zmierzających do zakłócania, uszkodzenia lub naruszenia integralności i bezpieczeństwa elementów systemu lub urządzenia. Ponadto ma służyć dostarczeniu informacji służących działaniom podejmowanym w reakcji na te działania lub umożliwiających usunięcie ich skutków[125].

[125] Digital Forensic Research Workshop, *Road Map for Digital Forensic Research*, New York 2001, http://dfrws.org/sites/default/files/session-files/a_road_map_for_digital_forensic_research.pdf (dostęp 30.04.2018).

Dowody sieciowe to dane sieciowe mające lub mogące mieć znaczenie dowodowe. Mogą przybierać różne formy i pochodzą niekoniecznie z jednego konkretnego typu urządzeń. Najbardziej istotnymi z kryminalistycznego punktu widzenia w odniesieniu do przestępczości wykorzystującej podatności lub funkcjonalności Internetu Rzeczy będą modemy, routery, karty sieciowe, przełączniki sieciowe (ang. *switch*) i koncentratory sieciowe (ang. *hub*). Źródłem dowodów sieciowych z kolei mogą być logi plików generowane przez serwery aplikacji takie jak *HTTP*, *FTP* i *SMTP*, logi IDS (ang. *Intrusion Detection System*), logi firewalla, serwerów pośredniczących (ang. *proxy*) i pamięci podręcznej (ang. *cache*), ruch sieciowy zarejestrowany przy użyciu programu typu *sniffer*. Ponadto źródłem są także wyniki kryminalistycznej analizy przy użyciu urządzeń podłączonych do komputera w celu wykonania konkretnych czynności, zawierające informacje o śladach sieciowych takich jak komunikacja sieciowa, trasowanie (ang. *routing*) oraz tablice ARP (ang. *Address Resolution Protocol*)[126]. Z uwagi na potencjalną ilość danych, liczbę urządzeń oraz źródeł dowodów sieciowych, niemożliwym jest zabezpieczenia wszystkich danych. Ogólne zasady zabezpieczania i postępowania z dowodami cyfrowymi mogą jednak dostarczyć wskazań i dyrektyw, umożliwiających odpowiednią priorytetyzację działań podejmowanych przez organy ścigania w stosunku do dowodów sieciowych.

W literaturze wyróżnia się wiele typów danych sieciowych mogących być źródłem dowodów i mających znaczenie w sensie kryminalistycznym. Najciekawszym oraz umożliwiającym proste, acz jednocześnie kompletne rozróżnienie jest podział na:

- **Dane sesji sieciowej** (ang. *Session Data*), czyli podsumowanie konwersacji sieciowych mających miejsce w konkretnej wymianie komunikacji sieciowej, to znaczy sesji sieciowej; najczęściej zbierane są rutynowo i w najbardziej podstawowym przypadku zebrane informacje zawierać będą wiadomość, rodzaj użytego protokołu sieciowego, oznaczenie czasu w postaci godziny i daty, źródłowy i docelowy adres IP oraz źródłowy i docelowy numer portu,
- **Dane powiadomień …** (ang. *Alert Data*), to znaczy podzbiór danych sesji sieciowej, zawierający jedynie dane oznaczone i zdefiniowane jako mające znaczenie lub ważne,

[126] R. Bryant, S. Bryant, op. cit.

- **Dane całościowe ruchu sieciowego** (ang. *Full Content Data*), czyli zapis wszystkich pakietów informacji przesłanych w sieci,
- **Dane statystyczne ruchu sieciowego** (ang. *Statistical Data*), dostarczają ogół informacji o związkach i powiązaniach różnych aspektów aktywności w sieci[127].

Wymieniony podział danych w sposób obrazowy pokazuje jakiego typu danych sieciowych mogą szukać organy ścigania w ramach kryminalistycznego badania z zakresu kryminalistyki sieciowej.

Dane zawierające informacje o komunikacji sieciowej oraz jej artefaktów takich jak data, miejsce i urządzenia w niej uczestniczące mają ogromne znaczeni dowodowe z punktu widzenia organów ścigania badających cyberprzestępstwa. Pozwalają na identyfikacje lub określenie rzeczywistej lokalizacji sprawcy wykorzystującego narzędzia anonimizujące lub ukrywające ruch sieciowy. Podobną wartość, a niejednokrotnie nawet większą cechę indywidualizującą, mają elementy charakterystyczne *stricte* dla poszczególnych sesji jak zapis pakietów wysyłanych informacji w postaci plików i ich rozmiaru oraz daty wysłania bądź odebrania. Należy twierdzić także, że w związku z rozwojem mediów społecznościowych wzrasta znaczenie analizy aktywności sieciowej niewymagającej dokonywania specjalistycznych badań z zakresu kryminalistyki sieciowej lub cyfrowej. Zastosowanie choćby tylko metod białowywiadowczych nierzadko pozwala na weryfikację wersji kryminalistycznych , a także zeznań lub wyjaśnień. Umożliwia to również zdobycie cennych informacji o codziennej aktywności, zainteresowaniach jednostek, a także tworzenie sieci powiązań i relacji między osobami. Należy jednak zwrócić uwagę na to, że tego typu metody mają mniejsze znaczenie w przypadku zaawansowanej cyberprzestępczości, w przypadku której sprawcy częściej posiadają umiejętności techniczne pozwalające na anonimizację i ukrywanie aktywności w sieci.

Istotnym aspektem identyfikacji ruchu sieciowego lub gromadzenia dowodów sieciowych jest obecnie także proces określany mianem monitorowania sieci. Wyróżnia się dwa typy tego działania: proaktywny i reaktywny. Pierwszy odnosi się do wszelkich działań monitorujących, zebranych danych i rutynowego sprawdzania działania sieci przed niepożądanym działaniem lub incydentem takim jak przykładowo atak na system lub urządzenie, natomiast ten drugi do działań już po, w reakcji na wydarzenie. Ten stosunkowo prosty podział, nie budzący przy tym większych kontrowersji, jest

[127] Ibidem, tłum. własne autora.

wystarczający na potrzeby rozważań kryminalistycznych odnośnie przestępstw sieciowych, do których należy zaliczyć przestępstwa wykorzystujące funkcjonalności lub podatności Internetu Rzeczy. Umożliwia on także określenie dwóch głównych zadań organów ścigania co do cyberprzestępczości. Należy rozwijać umiejętności tak w zakresie prewencji, jak i zdolności śledczych i dowodowych już po zaistnieniu społecznie negatywnego zjawiska jakim jest przestępstwo. Szczególnie pożądanym, choć jednocześnie trudnym i wymagającym pod względem technicznym oraz prawnym, jest proces rozwijania zdolności proaktywnych w stosunku do cyberprzestępczości.

5.5 Modele zabezpieczania dowodów cyfrowych oraz sieciowych w przypadku funkcjonalności Internetu Rzeczy

Wraz z rozwojem Internetu Rzeczy oraz technologii komunikacji bezprzewodowej, a także związanej z tym cyberprzestępczości, pojawiły się nowe modele lub podejścia do zabezpieczania dowodów cyfrowych oraz sieciowych. Mają za zadanie uwzględniać specyfikę i ewolucję technik oraz technologii, a także sposobów działania sprawców. Szczególnie ważne aspekty to zabezpieczenie danych ulotnych, rejestrowanie ruchu sieciowego, a także różnorodne działania podejmowane w zależności od liczby i typu urządzeń. Śledczy i technicy kryminalistyki brać muszą pod uwagę wielokrotnie większą liczbę czynników w przypadku przestępczości z wykorzystaniem funkcjonalności lub podatności Internetu Rzeczy, jak choćby czynności kryminalistyczne wobec urządzeń wykorzystujących technologię przechowywania danych w chmurze. Pośród modeli postępowania z i zabezpieczania dowodów w związku z rozwojem Internetu Rzeczy można zauważyć dwie tendencje: następuje dostosowywanie modeli lub ich przeformułowywanie, a więc w konsekwencji tworzenie nowego[128]. Warto wskazać niektóre z procedur kryminalistycznych aktualnie przyjętych w dyskursie naukowym.

Często przywoływanym, a przez to popularnym, modelem jest model Badania Obszarów 1-2-3 (ang. *The 1-2-3 Zones Approach*). Zakłada on podział czynności kryminalistycznych wobec urządzeń wykorzystujących funkcjonalności Internetu rzeczy

[128] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, E.K. Markakis, *A Survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues*, „IEEE Communications Surveys & Tutorials" 2020, t. 22, nr 2.

na trzy etapy, nazywane obszarami lub strefami. W pierwszej zbierane są dowody z warstwy technicznej, oprogramowania oraz sieciowej poszczególnych urządzeń pozostających bezpośrednim przedmiotem zainteresowania śledczych. Znajdują się w tak zwanej strefie wewnętrznej. Druga strefa obejmuje badanie urządzeń pośredniczących między tymi w strefie wewnętrznej (strefa pierwsza), a tymi w zewnętrznej (strefa trzecia). Mogą to być publiczne nadajniki, infrastruktura przesyłowa i sieciowa, a także systemy detekcji i zapobiegania incydentom bezpieczeństwa informatycznego. Nierzadko na tym etapie wymagana jest współpraca z dostarczycielami usług sieciowych. Strefa trzecia, czyli zewnętrzna, obejmuje warstwę techniczną i oprogramowania urządzeń nieznajdujących się bezpośrednio w sferze zainteresowania działań śledczych. Są one jednak powiązane z tymi ze sfery pierwszej, choćby poprzez obiekty ze strefy drugiej. Przykładami dowodów możliwych do zabezpieczenia ze strefy trzeciej to dane pochodzące od dostawców usług przechowywania danych w chmurze, na portalach społecznościowych, ruchu i usług sieciowych, a także dowody cyfrowe z zabezpieczonych urządzeń[129].

Inna popularna metodologia to model FAIoT (ang. *FAIoT: Forensics-Aware Model for the IoT*). Zakłada podejmowanie czynności kryminalistycznych wobec urządzeń wykorzystujących funkcjonalności Internetu Rzeczy sprzęgnięte ze scentralizowaną, zaufaną bazą (repozytorium) dowodów. Ma to na celu ułatwienie procesu gromadzenia, zabezpieczania i analizy dowodów oraz zapewnienie im wiarygodności[130]. To ostatnie osiągane jest poprzez stosowanie zabezpieczonego hybrydową metodą szyfrowania logowania, pozwalającego na zachowanie poprzednich logów z ruchu sieciowego, rejestrów czy danych z rejestratorów lub sensorów. Pozwala on dodatkowo na bezpieczne i uwierzytelnione odczytywanie (to znaczy w trybie odczytu, ang. *read only*, niewpływające na zabezpieczony materiał) danych przez organy ścigania[131].

Do jednych z nowszych metodologii zaliczyć z kolei można dwa modele postępowania: DFIF-IoT (ang. *DFIF-IoT: A Digital Forensics Investigation Framework*) oraz koncentrujący się na dowodach lub danych znajdujących się warstwie aplikacji (ang.

---

[129] E. Oriwoh, D. Jazani, G. Epiphaniou, P. Sant, *Internet of Things forensics: Challenges and approaches*, The 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013.

[130] S. Zawoad, R. Hasan, *FAIoT: Towards building a forensics aware eco system for the Internet of Things*, Proceedings of The 12th IEEE International Conference on Services Computing (SCC 2015), 2015.

[131] S. Zawoad, A.K. Dutta, R. Hasan, *SecLaaS: Secure logging-as-a-service for cloud forensics*, Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, 2013.

Application-Specific Digital Forensics). Pierwszy stanowi swoistą ogólną i generalną propozycję metodologii możliwej do zastosowania w przypadku zdarzeń, w których mamy do czynienia z tak zwanymi potencjalnymi dowodami cyfrowymi (PDC, ang. PDE, *Potential Digital Evidence*) wynikającymi z działania ekosystemu urządzeń Internetu Rzeczy[132]. Wskazuje się, że jego zaletą jest dostosowanie do zapisów zawartych w ISO/IEC 27043:2015. Jest to ważne z uwagi na międzynarodowy i aktualny charakter normy, mającej nieprzerwanie zastosowanie do czynności śledczych w razie wystąpienia incydentów. Drugi z przytoczonych wyżej modeli koncentruje się na danych i potencjalnych dowodach możliwych do uzyskania z urządzeń *stricte* kojarzonych z Internetem Rzeczy: urządzeniami smart home, smart city oraz tak zwanymi *wearables,* jak na przykład choćby zegarki i produkty do monitorowania aktywności sportowej. Są to trzy główne domeny, co do których podejmowane są czynności kryminalistyczne. Model ten składa się z trzech głównych komponentów, niezależnych od siebie: czynności podejmowanych wobec aplikacji bezpośrednio, zabezpieczania dowodów cyfrowych oraz podejmowania działań kryminalistycznych *sensu largo*.

W ramach ciekawostki przytoczyć można model przeznaczony do stosowania w toku czynności wobec przestępstw wykorzystujących koncepcję blockchain[133]. W wyniku zastosowania analogii zakłada przeniesienie koncepcji Internetu Rzeczy do formy zdecentralizowanej, jak to ma miejsce choćby w przypadku kryptowalut. Ma to się przyczynić do łatwiejszego i wydolniejszego procesu zabezpieczania dowodów z urządzeń wykorzystujących funkcjonalności Internetu Rzeczy. Niezmienność, związana z koncepcją blokchain, ma zapewnić wiarygodność oraz integralność danych cyfrowych i sieciowych. Ponadto, zagwarantowana ma być dostępność zapieczonych danych dla organów ścigania, praktycznie z każdego miejsca i o dowolnym czasie. Koncepcja wykorzystania technologii blockchain do czynności kryminalistycznych wobec urządzeń wykorzystujących funkcjonalności Internetu Rzeczy jest aktualnie cały czas rozwijana przez wielu

[132] V.R. Kebande, I. Ray, *A generic digital forensic investigation framework for Internet of Things (IoT)*, Proceedings of 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016.

[133] H.F. Atlam, G.B. Wills, A. Alenezi, M.O. Alassafi, *Blockchain with Internet of Things: Benefits, challenges, and future directions*, „International Journal of Intelligent Systems and Applications" 2018, t. 10, nr 6.

naukowców, choćby do celów dowodowego zabezpieczenia danych z kryptowaluty Ethereum[134].

Wskazane modele nie są jedynymi rozwijanymi lub dostoswanymi modelami postępowania w przypadku podejmowania czynności kryminalistycznych w przypadku przestępczości wykorzystującej funkcjonalności Internetu Rzeczy. Niezależnie od ich liczby pozostają kwestie dyskusyjne i problemy do rozwiązania. Z ogromu istniejących modeli wynika przyjęcia jednej lub kilku konkretnych metodologii za powszechnie obowiązujące standardy. Podjęcie działań standaryzujących prowadzących w efekcie do certyfikacji najbardziej adekwatnych rozwiązań prowadzić może do wzrostu efektywności prowadzanych postępowań w sprawach cyberprzestępstw. Z tym wiążą się takie czynniki jak dobór kryteriów włączania danych w poczet materiału dowodowego lub wykluczania go oraz podstaw dla tych decyzji. Rozwój komunikacji bezprzewodowej implikuje także konieczność zastanowienia się na ewentualnymi granicami wykorzystania aktualnie stosowanych narzędzi i rozwiązań technicznych do czynności kryminalistycznych. Wraz z rozwojem technicznym, koniecznym jest wypracowywanie i przygotowywanie oprogramowania i narzędzi umożliwiających organom ścigania efektywne prowadzenie postępowań. Nie jest to wyczerpująca lista zagadnień problematycznych, które należy wziąć pod uwagę. Każdy z przytoczonych czynników ma jednak bezpośredni wpływ na postępowania w sprawach cyberprzestępstw. Podejmowanie działań harmonizujących, a więc także współpraca międzynarodowa na poziomie organów ścigania, jak i naukowców jest pożądana. Umożliwi to wypracowanie uniwersalnych i akceptowalnych propozycji standardów, a następnie ich udane wdrożenie.

[134] Por. A.H. Lone, R.N. Mir, *Forensic-chain: Ethereum blockchain based digital forensics*, „Scientific and Practical Cyber Security Journal" 2017, t. 1–2, lub K. Wang, M. Du, Y. Sun, A. Vinel, Y. Zhang, *Attack detection and distributed forensics in machine-to-machine networks*, „IEEE Network" 2016, t. 30(6).

Rozdział 6. Studia przypadków

6.1 Wprowadzenie

Przestępstwa wykorzystujące podatności lub funkcjonalności Internetu Rzeczy mogą przybrać różne formy, jak pokazują zarówno badania teoretyczne, praktyczne, jak i już konkretne zdarzenia. Zasługującym na szczególne zainteresowanie jest cyberatak na spółkę Dyn z października 2016 roku (ang. *2016 Dyn cyber attack*). Przykłady teoretyczne oraz praktyczne wymagają wzbogacenia o rozważania dotyczących ich prawnych oraz kryminalistycznych konsekwencji oraz doniosłości dla rozwoju cyberprzestępczości i zdolności organów ścigania do przeciwdziałania jej. Omówione niżej przykłady nie będą katalogiem enumeratywnym. Ich wybór, choć subiektywny, jest także odpowiednio uzasadniony z punktu widzenia kryminalistyki i prawa karnego. W ramach tego rozdziału zabraknie dokładnego opisania niektórych z eksperymentów dotyczących urządzeń takich jak lodówki[135], elektroniczne nianie[136], telewizory[137], oraz system ZigBee, czyli jeden z wykorzystywanych w ramach koncepcji tzw. smart-domu[138]. Przykłady omówione pozostają z nie mniejszym wpływem na bezpieczeństwo niż wymienione wyżej przykłady. Dobór oparty był głównie o ilość i poziom szczegółowości dostępnych materiałów, umożliwiających bardziej niż jedynie powierzchowną analizę. Wskazane podatności i zagrożenia pozostają w ścisły związku z potencjałem oraz funkcjonalnościami wykorzystywanymi przez koncepcję Internetu Rzeczy. Niosą ze sobą także największe zagrożenie już na obecnym etapie ich rozwoju, w czasie gdy inne podobne projekty lub

---

135 *Hacking DefCon 23's IoT Village Samsung fridge*, Pen Test Partners, 2015, https://www.pentestpartners.com/security-blog/hacking-defcon-23s-iot-village-samsung-fridge/ (dostęp 30.04.2018).

136 T. Beardsley, M. Stanislav, *Hacking IoT: a Case Study on Baby Monitor Exposures and Vulnerabilities*, Rapid7 2015, https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf (dostęp 30.04.2018).

137 D. Goodin, *Smart TV hack embeds attack code into broadcast signal – no access required*, Ars Technica, 2017, https://arstechnica.com/information-technology/2017/03/smart-tv-hack-embeds-attack-code-into-broadcast-signal-no-access-required/ (dostęp 30.04.2018).

138 T. Zillner, *ZigBee Exploited, The good, the bad and the ugly*, Cognosec 2015, https://www.blackhat.com/docs/us-15/materials/us-15-Zillner-ZigBee-Exploited-The-Good-The-Bad-And-The-Ugly-wp.pdf (dostęp 30.04.2018).

urządzenia pozostają jeszcze nierzadko na etapie rozwojowym lub badawczo-rozwojowym.

6.2 Urządzenia medyczne

Urządzenia medyczne (ang. *Medical Devices*) to instrument, aparatura, narzędzie, maszyna, urządzenie, implant, odczynnik *in vitro* (ang. *in vitro reagent*) lub inne podobne lub powiązane obiekty, takie jak części komponentów lub akcesoria (…) przeznaczone do diagnozy chorób, stanu zdrowia, terapii lub w celu zapobiegania, leczenia lub łagodzenia objawów chorób (…)[139]. Należy do tego także dodać również oprogramowanie będące integralną częścią urządzenia medycznego mające na celu wspieranie ich funkcjonowania i działania[140]. Problem podatności tego typu maszyn jest na tyle poważny, że zwróciło to nawet uwagę amerykańskiego Federalnego Biura Śledczego (FBI). Wydało ono komunikat o możliwym wzroście liczby ataków i czynów o charakterze przestępczym wykorzystujących podatności urządzeń medycznych[141]. FBI wypowiedziało się głównie w kontekście planowanego wówczas przejścia z papierowych baz danych zawierających dane o zdrowiu pacjentów na ich wersje elektroniczne (EHR, ang. *Electronic Health Records*). W pierwszej połowie 2013 r. ponad dwa miliony rekordów z baz danych zostało ujawnionych w wyniku ataków, co stanowiło 31% wszystkich naruszeń bezpieczeństwa danych. FBI wskazało, że według innych badań z lutego 2014 r. strategie ochronne systemów stosowanych w placówkach ochrony zdrowia są źle wyposażone oraz zbyt słabo zabezpieczone, aby poradzić sobie z zagrożeniami wynikającymi z rozwoju cyberprzestępczości[142]. Do kategorii urządzeń medycznych zaliczyć można wiele różnych aparatur, typów sprzętu i oprogramowania. W ramach omówienia możliwych implikacji połączenia podatności urządzeń medycznych oraz funkcjonalności Internetu Rzeczy na

---

[139] US Food and Drug Administration, *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework*, 2014, za: A. Woodward, P. Williams, *Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem*, „Medical Devices: Evidence and Research" 2015, t. 8, https://www.dovepress.com/cybersecurity-vulnerabilities-in-medical-devices-a-complex-environment-peer-reviewed-fulltext-article-MDER (dostęp 30.04.2018).

[140] A. Woodward, P. Williams, op. cit.

[141] US Federal Bureau of Investigation Cyber Division, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, FBI Cyber Division Private Industry Notification, 2014, https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf (dostęp 30.04.2018).

[142] Ibidem.

szczególne zainteresowanie zasługują przykłady automatycznych dozowników leków dla każdego pacjenta oraz rozruszniki serca wyposażone w możliwość zdalnej defibrylacji przez lekarza w sytuacji zagrożenia zdrowia lub życia pacjenta.

Pierwszym istotnym przykładem będą dozowniki leków. Są to urządzenia odpowiedzialne za zautomatyzowane podawanie leków pacjentom szpitali w odpowiednich dawkach. Dawki leków określone są w bibliotece plików zapisanej w urządzeniu. Współcześnie tego typu maszyny wyposażone są jednocześnie także w funkcje łączenia się z Internetem bądź wewnętrznymi sieciami w sposób przewodowy lub bezprzewodowy. Najczęściej połączone są z sieciami zlokalizowanymi będącymi częścią infrastruktury szpitala. W przypadku sieci bezprzewodowych nierzadko są to słabo lub w ogóle niezabezpieczone sieci, dostępne również dla pacjentów i gości placówki leczniczej. W 2015 r. specjalista od zabezpieczeń B. Rios przeprowadził dwa eksperymenty, badając podatność dozowników leków na zewnętrzne ataki hakerskie za pośrednictwem połączenia bezprzewodowego[143]. W ramach pierwszego udało się uzyskać dostęp do urządzenia i zwiększyć dawkę w graniach określonych w fabrycznej bibliotece plików Wszelkie zmiany powyżej skutkowały alarmem. Natomiast w ramach drugiego powiodło się nie tylko uzyskanie dostępu, manipulowanie dawkami, ale także i podmiana biblioteki plików na zawierające zmienione dopuszczalne normy leków. Taki sposób działania pozwolił na dowolne dostosowanie aplikowanej ilości środków medycznych, także w granicach stwarzających ryzyko utraty przez pacjenta zdrowia lub życia, a co najmniej narażenia go na taką sytuację. Zidentyfikowaną przyczyną, a więc podatnością dozowników leków było akceptowanie każdej aktualizacji oprogramowania. Także tych odpowiednio przygotowanych lub spreparowanych przez osobę trzecią oraz nie posiadających cyfrowo podpisanego certyfikatu bezpieczeństwa, przykładowo należącego do producenta oprogramowania lub sprzętu medycznego. Wykorzystanie tej podatności ponadto umożliwia także wyświetlanie na ekranie dozownika błędnych informacji, jakoby podawana była ta odpowiednia.

Kolejnymi implikacjami związanymi ze zidentyfikowaną podatnością jest brak koniecznego kontaktu sprawcy z urządzeniem, z uwagi na wykorzystywane przez urządzenie połączenie z siecią szpitala i za jej pośrednictwem z Internetem. Ma to

---

143 K. Zetter, *Hacker can send fatal dose to hospital drug pumps*, WIRED, https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/ (dostęp 30.04.2018).

zastosowanie choćby w przypadku potrzeby wysłania aktualizacji oprogramowania urządzenia. Natomiast podłączenie się do szpitalnej sieci powiązane z opisaną powyżej podatnością wskazuje na poważne wątpliwości co do bezpieczeństwa urządzeń przed ingerencją zewnętrzną osób trzecich, choćby w sposób opisany powyżej. W momencie połączenia z siecią, choćby będącą częścią infrastruktury szpitala, urządzenie jest tak bezpieczne jak zabezpieczona jest sieć z którą się połączyło. Oznacza to, że nieadekwatne zapewnienie bezpieczeństwa jednego elementu powoduje stan zagrożenia dla innych. Połączenie takiego stanu rzeczy z indywidualnymi podatnościami każdego z urządzeń może doprowadzić do skutków wręcz niejednokrotnie tragicznych. Natomiast z punktu widzenia kryminalistycznego oznacza to więcej potencjalnych dowodów do zabezpieczenia, więcej czynności oraz ekspertyz do przeprowadzenia, a także trudności natury logistycznej z tym związane jak przykładowo wymóg współpracy z personelem zabezpieczającym szpital, a także producentem sprzętu lub oprogramowania.

Kolejnym groźnym przykładem jest możliwość przeprowadzenia ataku na rozruszniki serca wyposażone w funkcje bezprzewodowego łączenia się z siecią. Celem wyposażenia w moduły bezprzewodowe tego typu urządzeń była możliwość zdalnego monitorowania przez lekarza stanu pacjenta w czasie rzeczywistym, bez konieczności zapraszania go na wizytę. W razie sytuacji awaryjnej mógłby także uratować mu życie zdalnie wysyłając impuls przywracający prawidłową pracę serca. Małe rozmiary rozruszników powodują, że nie są one wyposażone w odpowiednie zabezpieczenia, które szyfrowałyby bezprzewodowe połączenie z lekarzem, co udowodniono w badaniach przeprowadzonym przez studentów *University of South Alabama*. Przedmiotem eksperymentu był zaawansowany fantom szkoleniowy iStan dla adeptów studiów medycznych. W celu realnej symulacji stanu chorobowego jego zachowania i reakcje mają być zbliżone do tych człowieka. Wachlarz jego możliwości obejmuje takie zachowania jak płacz, mówienie, pocenie się. Dodatkowo reaguje na 300 różnych leków w taki sam sposób jak organizm ludzki. Jednym z głównych elementów wyposażenia fantomu jest wbudowany rozrusznik mechanicznego serca. Eksperyment udowodnił, że możliwym było wpływanie w dowolny sposób na tętno, a w razie wyposażenia rozrusznika w zdalnie aktywowany defibrylator udałoby się wysłać za pośrednictwem komunikacji bezprzewodowej komendy, wywołujące kontrolowane wstrząsy elektryczne manipulujące pracą sztucznego serca. W wyniku poczynionych obserwacji ten sam zespół podjął się

opracowania adekwatnej metody szyfrowania, której brak został zidentyfikowany jako główna podatność.

Aktualnie wśród specjalistów oraz agencji federalnych przeważają opinie, że zagrożenie tego typu atakami nie jest powszechne. Nie znaczy to jednak, że nowe zagrożenia powiązane z wyposażaniem sprzętu medycznego w możliwości komunikacji bezprzewodowej, pojawią się dopiero w odległej przyszłości. Szczególnie istotnym jest zwrócenie uwagi na podatność wynikającą z braku stosowania szyfrowanego połączenia. Potencjalne skutki wykorzystanie tych braków mogą mieć ogromne znaczenie, biorąc pod uwagę typ przetwarzanych przez urządzenia medyczne danych. Nie mówiąc już o potencjalnych konsekwentnych podatnościach i błędach w urządzeniach. Powiązanym z tym aspektem jest także brak zabezpieczeń sprzętowych, a nie tylko w postaci oprogramowania szyfrującego lub monitorującego stan bezpieczeństwa. Problemy tego typu mogą zostać rozwiązane w przyszłości, gdy miniaturyzacja sprzętu rozwinie się w sposób umożliwiający wyposażenie najmniejszych nawet urządzeń w adekwatne metody, systemy i czujniki odpowiedzialne za integralność danych i ich bezpieczeństwo. Jednak bez dostrzeżenia istniejącego już w tym momencie problemu, nie będzie możliwym zaradzenie tym problemom w przyszłości.

Podsumowując zagrożenia wynikające z podatności w urządzeniach medycznych należy zauważyć tendencje do dostrzegania i wskazywania na potencjalne wektory tego typu ataków. FBI w komunikacie z września 2015 r.[144] dotyczącym zagrożeń ze strony ataków wykorzystujących podatności lub funkcjonalności Internetu Rzeczy skierowanych przeciwko urządzeniom medycznym zwraca uwagę na szeroki wachlarz możliwości sprawców. Mimo faktu, że pozostaje on w tonie nadzwyczaj ogólnym, niewskazującym konkretnych aspektów technicznych lub podatności, to jest to cenny i potrzebny głos. W przyszłości w wyniku prowadzonych aktualnie eksperymentów i badań należy się spodziewać bardziej szczegółowego określenia możliwych wektorów i metod ataku. Stwierdzenie, że systemy wykorzystywane w służbie zdrowia nie są odpowiednio zabezpieczone do radzenia sobie z ówczesnymi zagrożeniami ze strony cyberprzestępców, zarówno pod względem oprogramowania jak i sprzętu, nie napawają optymizmem. Należy przypuszczać, że skoro wtedy nie były na to przygotowane to i dziś jest podobnie. Wynika to z faktu, że cyberprzestępczość ulega nieustannym zmianom i dynamicznemu rozwojowi.

[144] *Internet of Things poses opportunities for cyber crime*, FBI Public Service Announcement, 10 września 2015 r., https://www.ic3.gov/media/2015/150910.aspx (dostęp 30.04.2018).

Ocena potencjalnej kwalifikacji prawnej zdarzeń wykorzystujących podatności urządzeń medycznych jest trudna. Najpewniej, w razie wystąpienia konkretnego zdarzenia ocena należeć będzie do organów ścigania. Spodziewać się można kwalifikacji prawnej z przestępstw przeciwko zdrowiu i życiu, gdyż opisane powyżej podatności do takiej konkluzji prowadzą. NAtomaist w przypadku przestępstw przeciwko bezpieczeństwu informacji występujacych niejako obok głównej kwalifikacji prawnej, jednak istotnych z punktu widzenia wykorzystania Internetu Rzeczy do popełniania przestępstw, można sproówać dokonać dodatkowych wskazań co do potencjalnego wypełnieniea znamion przestępstw z tej kategorii właśnie. Niewątpliwie spodziewać by się można było zarzutów o bezprawne uzyskanie dostępu do informacji (art. 267 § 1 k.k.) oraz systemu informatycznego (art. 267 § 2 k.k.) posługując się do tego oprogramowaniem lub urządzeniem (art. 267 § 3 k.k.), a także za zmienianie, niszczenie lub uszkadzanie informacji (art. 268 k.k.). Dodatkowo możliwe, że w przypadku wtargnięcia i manipulacji danymi informatycznymi lub wpływania na działanie systemów zlokalizowanych w szpitalach i placówkach medycznych może nastąpić wypełnienie znamion także przestępstwa sabotażu komputerowego, charakteryzującego się tym, że przedmiotem ochrony są dane *o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego*[145]. Szpitale i placówki zajmujące się ochroną zdrowia są elementem infrastruktury krytycznej, a przez to zapewnienie ich bezpieczeństwa jest istotne z punktu widzenia bezpieczeństwa państwa.

Zasadność tej tezy wspiera także ustawa o krajowym systemie cyberbezpieczeństwa, implementująca postanowienia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Wskazano w niej podmioty lecznicze, tzn. podmioty realizujące świadczenia szpitalne, które miały więcej niż 18 000 hospitalizacji rocznie, jako operatorów usług kluczowych. Implikuje to jednocześnie nałożenie na rzeczony podmiot obowiązków oraz określa jego dodatkowe znaczenie w systemie bezpieczeństwa państwa. Należy założyć, że ma to także na celu wzmocnienie ochrony z punktu widzenia prawa karnego. Niezależnie od tego, wracając do rozważań odnośnie potencjalnej kwalifikacji prawnej czynu zabronionego, należy stwierdzić, że istnieje możliwość wypełnienia przez

[145] Kodeks karny.

sprawców także znamion przestępstwa sabotażu komputerowego w przypadku ataku na systemu lub urządzenia należące do lub zarządzane przez szpitale i placówki medyczne.

Na podstawie powyższych można postawić tezę, że urządzenia medyczne nie są zabezpieczone w odpowiedni sposób wobec wyzwań wynikających z rozwoju Internetu Rzeczy. Niewątpliwie stanowi to ogromne wyzwanie dla organów ścigania mających nie tylko zwalczać przestępstwa, ale również im zapobiegać poprzez zwracanie uwagi na możliwe i potencjalne zagrożenia. Ponadto jest to istotne dla osób zajmujących się ochroną zdrowia w celu zabezpieczenia bezpieczeństwa pacjentów, ale także dla producentów sprzętu medycznego. Ci drudzy powinni w szczególności dołożyć wszelkich starań w celu zapewnienia zabezpieczeń umożliwiających korzystanie z ich sprzętu w sposób bezproblemowy i zapewniający odpowiedni poziom zabezpieczeń przed zewnętrznymi atakami. Natomiast w razie zaistnienia incydentów lub przestępstw wykorzystujących podatności w ich urządzeniach powinni współpracować z organami ścigania. Rolą państwa w tym procesie, w szczególności organów ustawodawczych oraz wykonawczych, byłoby wypracowanie legislacji lub procedur dotyczących współpracy, wymiany informacji oraz udostępniania danych na potrzeby prowadzonych postępowań karnych, naturalnie z poszanowaniem istniejących przepisów dotyczących prywatności i ochrony danych osobowych. Nawet jeżeli obecnie nie możemy mówić o żadnym przypadku wykorzystania luk w zabezpieczeniach do dokonania rzeczywistego przestępstwa, to nie należy tego potencjalnego zagrożenia deprecjonować. Potencjał nowych technologii oraz Internetu Rzeczy do popełniania przestępstw implikuje potrzebę dostrzegania potencjalnych niebezpieczeństw oraz dokonywania oceny i szacowania ryzyka. Mimo faktu, że aktualnie część z predykcji pozostanie jedynie w sferze problemów *stricte* teoretycznych, to koniecznym jest zwrócenie uwagi na potencjalne zagrożenia.

6.3 Samochody i akcesoria do pojazdów

Kolejnym z istotnych i zagrożonych atakiem elementów lub urządzeń są tzw. elektroniczne moduły sterujący lub kontrolne (ang. ECU, *Electronic Control Unit*). Mianem tym określane są wbudowane w pojazdach moduły odpowiadające za kontrolę

jednego lub więcej systemów bądź podsystemów elektronicznych pojazdu[146]. Do takich systemów bądź podsystemów można zaliczyć jednostki odpowiedzialne za sterowanie zamkiem w drzwiach, prawidłowe działanie silnika samochodowego, systemu kierowania i hamowania pojazdem oraz wspomagających prowadzenie systemów elektronicznych. Ogółem w obecnych pojazdach są to praktycznie wszystkie systemy i funkcje w jakie są wyposażone samochody. Zależnie od klasy i roku produkcji samochodu ich liczba, przy obecnym stanie rozwoju technologicznego, może wynosić w jednym pojeździe od kilku do nawet kilkudziesięciu[147].

Możliwości wykorzystania podatności ECU obrazuje częściowo eksperyment z 2014 r. dotyczący możliwości przejęcia przez hakerów kontroli nad samochodem marki Jeep. W jego wyniku dokonano ataku na samochód Jeep Cherokee prowadzony na drodze międzystanowej przez dziennikarza magazynu WIRED[148]. Sprawcy znajdowali się w domu oddalonym kilka kilometrów od celu i wykorzystali do tego zdolności komunikacji bezprzewodowej ECU z Internetem. We wcześniejszym eksperymencie przeprowadzonym w 2013 roku, w celu przeprowadzenia ataku badacze musieli siedzieć w samochodzie, ponieważ atak na systemy elektroniczne samochodu był możliwy jedynie po podłączeniu komputera do samochodu przez port wykorzystywany przez mechaników w trakcie przeglądów technicznych. Po roku pracy i przygotowań możliwe było rozwinięcie tej metody na tyle, udało się przeprowadzić atak na systemy nowego samochodu za pośrednictwem Internetu bez konieczności fizycznego przebywania w środku. W ramach eksperymentu możliwe było manipulowanie systemem klimatyzacji, radiem, komputerem pokładowym, wycieraczkami i spryskiwaczami. Dwoma ostatnimi do tego stopnia, że uniemożliwiało to obserwację drogi przed kierowcą. Ostatecznym działaniem było tzw. „zabicie" silnika – zablokowanie pedału przyspieszania i zwolnienie samochodu do bardzo niskiej prędkości. Pełnia możliwości atakujących obejmuje także możliwość pełnego przejęcia kontroli nad sterowaniem torem jazdy pojazdu przy niskiej prędkości a także możliwość całkowitego wyłączenia silnika, a także włączenie lub wyłączenia działania

[146] https://en.wikipedia.org/wiki/Electronic_control_unit (dostęp 30.04.2018).

[147] W kilku źródłach podaje się, że ta liczba w 2015 roku sięgała 80 ECU w nowszych pojazdach, jednak z uwagi na dynamiczny rozwój technologii nietrudno sobie wyobrazić, że ich możliwa potencjalna liczba w nowych samochodach obecnie jest już większa, https://www.computerhope.com/jargon/e/ecu.htm (dostęp 30.04.2018).

[148] A. Greenberg, *Hackers remotely kill a jeep on the highway – with me in it*, WIRED, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (dostęp 30.04.2018).

hamulców Naturalnie przejęcie kontroli nad systemami elektronicznymi pojazdu umożliwiała zlokalizowanie samochodu dzięki wbudowanemu systemowi lokalizacji GPS.

Podatności wykorzystywane w tym ataku wynikają z implementacji coraz większej liczby systemów elektronicznych w samochodach, w teorii mających ułatwić użytkownikowi korzystanie z pojazdu oraz umożliwić producentowi monitoring zużycia poszczególnych części w trakcie eksploatacji. W praktyce oznacza to także brak adekwatnych zabezpieczeń ECU przed zewnętrznymi atakami, stwarzając tym samym okazję do wykorzystania takich luk przez przestępców. Uzyskanie kontroli nad samochodem może być w takiej sytuacji możliwe z jakiekolwiek miejsca, pod warunkiem że zna się jego adres IP. Natomiast pozyskanie tegoż nie jest szczególnie skomplikowane dla osób posiadających wiedzę i doświadczenie z łamaniem zabezpieczeń. Podsumowaniem skuteczności eksperymentu, jak i podatności samochodów na ataki oraz skali zagrożenia, niech będzie informacja, że po tym eksperymencie firma Chrysler (wytwórca samochodów marki Jeep) wycofała z rynku 1,4 miliona aut.

Wbudowane systemy nie są jedynymi, które posiadają podatności wpływające na poziom bezpieczeństwa systemów elektronicznych pojazdów. Przejęcie kontroli nad poszczególnymi systemami, jak również nad całym samochodem, możliwe jest także w wyniku wykorzystania braków w zabezpieczeniu elementów i gadżetów dołączanych do pojazdu, funkcjonujących po podłączeniu jako dodatkowe ECU. Na ten wektor potencjalnego zagrożenia zwróciło uwagę FBI w komunikacie z 17 marca 2016 r.[149] W komunikacie służby zwracają zarówno producentom samochodów oraz części samochodowych, jak również konsumentom uwagę na podatność komponentów elektronicznych na ataki w sytuacjach, gdy nie będą one w odpowiedni sposób zabezpieczone. Jednym z przywołanych przykładów jest urządzenie francuskiej firmy Mobile Devices - OBD2. Przeznaczeniem tego gadżetu była kontrola lokalizacji pojazdów i liczby kilometrów pokonanych przez klienta po podłączeniu urządzenia do deski rozdzielczej. W badaniu podatności tego typu urządzeń zespół z Uniwersytetu Kalifornijskiego w San Diego (UCSD) na przykładzie Corvetty z 2013 r. udowodnił, że istnieje możliwość przejęcia kontroli nad nimi i wysyłania komend mających wpływ na działanie ECU samochodu. Było to możliwe poprzez przesyłanie odpowiednio napisanych wiadomości SMS, zawierających komendy przeznaczone dla i trafiające do magistrali

[149] *Motor vehicles increasingly vulnerable to remote exploits*, FBI Public Service Announcement, 17 marca 2016 r., https://www.ic3.gov/Media/Y2016/PSA160317 (dostęp 30.04.2018).

CAN, czyli wewnętrznej sieci pozwalającej kontrolować fizyczne elementy samochodu. Mimo faktu, że w ramach eksperymentu naukowcy byli w stanie kontrolować system działania wycieraczek oraz hamulców, to zdaniem kierownika zespołu badaczy S. Savage'a dzięki tym małym gadżetom można by przejąć kontrolę praktycznie nad wszystkimi elektronicznymi elementami samochodu[150].

Dokonując analizy powyższych zagrożeń pod kątem potencjalnej odpowiedzialności na gruncie polskiego kodeksu karnego, należy stwierdzić że w razie wykorzystania wskazanych powyżej podatności lub funkcjonalności do popełnienia przestępstw sprawcy mogliby odpowiadać za bezprawne uzyskanie dostępu do informacji (art. 267 § 1 k.k.) oraz systemu informatycznego (art. 267 § 2 k.k.) posługując się do tego oprogramowaniem lub urządzeniem (art. 267 § 3 k.k.), a także za zmienianie lub uszkadzanie informacji (art. 268 k.k.). Możliwości wypełnienia znamion innych przestępstw jak choćby przeciwko życiu i zdrowiu, bezpieczeństwu w komunikacji lub przeciwko mieniu zależałoby od oceny każdorazowej sytuacji przez uprawnione do tego organy.

Przytoczone wyżej przykłady są jedynie niewielkim papierkiem lakmusowym możliwości wykorzystania funkcji komunikacji bezprzewodowej, w tym funkcjonalności i podatności Internetu Rzeczy do popełniania przestępstw. Skala możliwych zagrożeń nie ogranicza się jedynie do przestępstw kryminalnych skierowanych przeciwko pojedynczej osobie, ale również czynów o charakterze terrorystycznym. Szczególnie w przypadku samochodów, które jak większość produktów obecnie, produkowanych jest seryjnie. Z tego względu podatność na ataki nie jest ograniczone do jednego, wadliwego egzemplarza, a raczej do całej serii. Dodatkowo niekoniecznie ogranicza się to do jednego modelu pojazdu danej marki, ponieważ część podzespołów jest taka sama we wszystkich samochodach danego producenta. Z tego powodu błędy lub wady konstrukcyjne bądź programistyczne mogą być powielone w wielu pojazdach. Korelacja rosnącej skali z brakiem świadomości społecznej oraz przedstawicieli organów ścigania i wymiaru sprawiedliwości w kwestii dotkliwości ewentualnych zagrożeń wymaga szczególnego podkreślenia. Im większy jej brak, tym dotkliwsze skutki przestępstwa z wykorzystaniem Internetu Rzeczy i tym większe będą szkody spowodowane tymi czynami.

---

150 A. Greenberg, *Hackers cut a Corvette's brakes via a common car gadget*, WIRED, https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/ (dostęp: 30.04.2018).

6.4 Dyn cyber attack

Pierwsze dobrze udokumentowane zdarzenie noszące wszelkie znamiona przestępstwa i jednocześnie wykorzystujące funkcjonalności lub podatności Internetu Rzeczy, czyli *Dyn cyber attack,* miało miejsce 21.10.2016 r. Składało się na niego wiele ataków typu DDoS, których celem były serwery spółki Dyn. Jest to dostawca usług typu DNS (ang. Domain Name System) polegającej na przechowywaniu danych na temat adresów domen przez system serwerów. Umożliwia to posługiwanie się przez użytkowników adresami stron www w postaci tekstowej, zamiast adresów IP. Innymi słowy, DNS dokonuje „tłumaczenia" wpisanego adresu w formie tekstu na odpowiadający mu adres IP i na odwrót[151]. Z usług Dyn korzystają największe internetowe serwisy informacyjne, rozrywkowe i usługowe w Ameryce Północnej. Do przeprowadzenia ataku wykorzystano dziesiątki milionów adresów IP, z czego dużą ich liczbę stanowiły urządzenia mające połączenie z Internetem takie jak drukarki, kamery IP, elektroniczne nianie oraz urządzenia wykorzystywane w domach do łączenia sieci lokalnej z Internetem jak na przykład modemy czy routery. Możliwość ich wykorzystania do ataku typu DDoS była możliwa w wyniku zakażenia ich szkodliwym oprogramowaniem o nazwie Mirai. Zamieniało ono urządzenia w tzw. „urządzenia-zombie", czyli elementy sieci typu botnet. Jest to grupa zhakowanych komputerów, które są kontrolowane w sposób zdalny. Autorem botnetu może być jedna lub kilka osób; infekują oni komputery ofiar szkodliwym programem. Poszczególne komputery wchodzące w skład botnetu często są nazywane „botami" lub „komputerami-zombie". Botnet nie musi mieć określonej liczby komputerów: mniejsze mogą składać się z setek lub tysięcy zainfekowanych maszyn, a większe — nawet z milionów[152]. Obecnie zasadnym byłoby, na kanwie rozważań dotyczących Internetu Rzeczy, aby mówić o grupie zhakowanych urządzeń, aniżeli tylko grupie zhakowanych komputerów. Mechanizm ataku DDoS jest prosty i opiera się na wysyłaniu takiej ilości żądań dostępu do witryny sieci internetowej, która doprowadza do przeciążenia serwera i uniemożliwia przez to dostęp do niej zwykłym użytkownikom. Kwestią wyróżniającą atak z października 2016 r. było wykorzystanie nie komputerów, ale

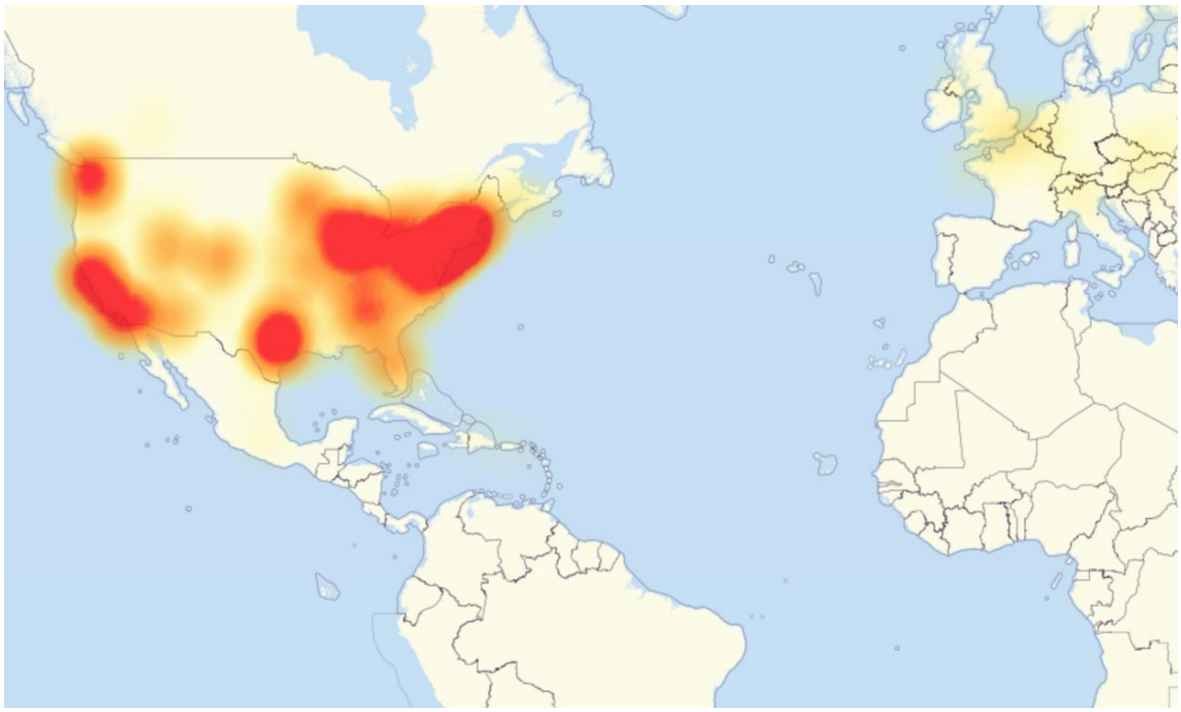
[151] https://pomoc.nazwa.pl/baza-wiedzy/produkty-i-uslugi/domeny/o-domenach-bardziej-technicznie/co-to-jest-dns/ (dostęp: 30.04.2018).

[152] D. Fischer, op. cit.

urządzeń i przedmiotów połączonych z Internetem innych niż komputery, a także skala tego ataku, wynikająca pośrednio z zastosowanej metody. Według krótkiej analizy opublikowanej na stronie spółki Dyn zaobserwowano żądanie połączenia przychodzące z milionów adresów IP. Brak jest jednak możliwości na stwierdzenia dokładnej ich liczby, a przez to także specyficznej liczby zainfekowanych urządzeń. Według niektórych źródeł ilość przesyłanych danych była w granicach 1,2 TBps (ang. *Terabit per second,* Terabit na sekundę, 1 TBps to ekwiwalent 1000 gigabajtów na sekundę), jednak również i w tym przypadku brak jest ostatecznego potwierdzenia tej prędkości. Jednakże nawet bez tego można stwierdzić, że był to pod względem skali i dotkliwości jeden z najbardziej groźnych i dotkliwych ataków, a dodatkowo niepokoi metoda jego przeprowadzenia[153].

W celu łatwiejszego wyobrażenia czym ten konkretny atak DDoS był oraz jego skali i efektywności, można użyć obrazowego porównania z centrum handlowym. Centrum handlowe będzie serwerem Dyn zapewniającym usługi typu DNS, a poszczególne sklepy w nim się znajdujące – serwerami poszczególnych witryn internetowych. Zazwyczaj atak typu DDoS lub DoS skierowany jest przeciwko jednej konkretnej stronie, a w przypadku niniejszej analogii – jednemu sklepowi w centrum handlowym. W efekcie ataku zwykli klienci nie mogą do niego wejść i skorzystać z jego oferty (przeglądać zawartości przykładowo). Specyfika zdarzenia z października 2016 r. polegała nie na zablokowaniu każdego ze sklepów oddzielnie, co w oczywisty sposób byłoby czaso- i pracochłonne, ale przeprowadzeniu ataku na całe centrum handlowe, czyli system serwerów zapewniających dostęp do wielu stron. Analogicznie posługując się metaforą - poprzez zablokowanie możliwości wejścia klientom do centrum handlowego uniemożliwiono dostęp do wszystkich sklepów naraz. Tak w obrazowy sposób przedstawiają się konsekwencje i zastosowana przez sprawców metoda, co obrazuje możliwości wykorzystania do popełniania przestępstw funkcjonalności lub podatności Internetu Rzeczy.

[153] S. Hilton, *Dyn Analysis Summary Of Friday October 21 Attack*, Dyn 2016, https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ (dostęp 30.04.2018).



Rysunek 1. Mapa przedstawiająca zasięg Dyn cyber attack, wraz z zaznaczeniem obszarów najbardziej dotkniętych brakiem dostępu do konkretnych witryn internetowych bądź Internetu, źródło: DownDetector Level 3 Outage Map, http://downdetector.com/status/level3/map/, [dostęp: 30.04.2018 r.].

Z punktu widzenia możliwości wykorzystania podatności lub funkcjonalności Internetu Rzeczy do dokonywania ataków komputerowych i sieciowych to opisany powyżej atak jest przełomowy. Jest pierwszym tak dobrze opisanym i dotkliwym incydentem wykorzystującym inne niż komputery urządzenia posiadające funkcje komunikacji bezprzewodowej. Nie sposób przecenić wartości doświadczeń i wniosków, wypływających z analizy przebiegu i efektów *Dyn cyber attack*. Wykazały wprost jak groźne są nieodpowiednie zabezpieczone urządzenia mogące być częścią koncepcji Internetu Rzeczy, które zostaną wykorzystane do przeprowadzenia szeroko zakrojonego ataku sieciowego. Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych (ang. Department of Homeland Security) wszczął śledztwo według źródeł w Białym Domu, do dzisiaj brak jest jednak ogólnodostępnych efektów śledztwa. Do przeprowadzenia ataku przyznały się grupy takie jak Anonymous oraz New World Hackers, lecz brak jest potwierdzenia na ich sprawstwo. Według spółki Flashpoint atak został przeprowadzony przez tzw. *script kiddies*, czyli niedoświadczonych hakerów bądź crackerów, używających aplikacji i programów nienapisanych przez siebie, a wytworzonych przez innych, bez

dogłębnej znajomości ich działania[154]. Wskazuje się, że wykorzystali oni do tego udostępniony publicznie kod oprogramowania Mirai[155]. Do dzisiaj nie udało się ustalić sprawcy ataku, dlatego aktualnie można się poruszać jedynie w sferze domysłów. Można jedynie próbować wysnuwać wnioski co do tożsamości sprawcy lub sprawców na podstawie znanych ogólnie faktów lub artefaktów zabezpieczonych w trakcie śledztwa i analizy urządzeń oraz ruchu sieciowego na serwerach ofiary. Z uwagi na zastosowany typ ataku oraz fakt, iż kod złośliwego oprogramowania Mirai był publicznie udostępniony, a więc każdy użytkownik sieci mógł mieć do niego dostęp, można domniemywać, że osoba lub osoby dokonujące ataku niekoniecznie musiały posiadać specjalistyczną wiedzą z zakresu programowania dostępną jedynie dla wąskiego grona. Potencjalni sprawcy jednakowoż musieli znać choćby podstawy programowania lub wykorzystania złośliwego oprogramowania. Biorąc pod uwagę powyższe można przychylić się do wniosków, że bardziej prawdopodobne jest w tym przypadku sprawstwo *script kiddies*, aniżeli tak dobrze zorganizowanych grup hakerskich jak Anonymous.

Kwestia tożsamości konkretnych sprawców ataku na serwery Dyn cały czas pozostaje zagadką. Jednak według doniesień Briana Krebsa, jednej z ofiar oprogramowania Mirai, przeprowadził analizę informacji dostępnych w Internecie oraz wykorzystał wyniki analiz innych badaczy. W wyniku tego ustalił możliwą tożsamość twórców oprogramowania Mirai: Parasa Jha i Josiaha White'a[156]. Organy ścigania dodatkowo ustaliły trzeciego według nich twórcę progrmau: Daltona Normana. Wszyscy trzej przyznali się do winy[157] i zostali skazani na kary pozbawienia wolności z zawieszeniem ich wykonania oraz zostali zobowiązani do zapłaty określonej kwoty za straty w wyniku działania szkodliwego oprogramowania[158]. Ponadto Para Jha przyznał się do ataku na serwery Uniwersytetu Rutgersa, gdzie był studentem, przy użyciu Mirai. Umiejętności sprawców, według informacji zgormadzonych przez Briana Krebsa, świadczy o posiadaniu umiejętności programistycznych. Przykład stworzonego przez nich oprogramowania oraz wynikającego z niego następnie ataku na serwry Dyn wskazuje jak

---

[154] https://pl.wikipedia.org/wiki/Script_kiddie (dostęp 30.04.2018).

[155] N. Lomas, *Dyn DNS DDoS Likely the Work of Script Kiddies, Says Flashpoint*, Techcrunch 2016, https://techcrunch.com/2016/10/26/dyn-dns-ddos-likely-the-work-of-script-kiddies-says-flashpoint/?guccounter=1 (dostęp 30.04.2018).

[156] https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/ (dostęp 31.10.2020).

[157] https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving (dostęp 31.10.2020).

[158] https://krebsonsecurity.com/2018/09/mirai-botnet-authors-avoid-jail-time/ (dostęp 31.10.2020).

wielkim zagrożeniem może być program stworzony przez programistów posiadających wiedzę i doświadczenie. Niezależnie od tożsamości bezpośrednich sprawców ataku z października 2016 r., można spodziewać się podobnych ataków w przyszłości.

Zagrożenie wynikające ze szkodliwego oprogramowania Mirai nie ogranicza się tylko do pojedynczego zdarzenia. Podobne ryzyko i zagrożenie stanowią pochodne i wtórne w stosunku do niego grupy oprogramowania. Przykładem może być na to przypadek zdarzenia z listopada 2017 roku. Wtedy odkryte zostało szkodliwe oprogramowanie Satori, które oparte było o kod Mirai i miało podobne zastosowanie: tworzenie botnetu i dokonanie ataku typu DoS i DDoS. Wykorzystywał podatności interfejsu SOAP oraz luk w oprogramowaniu routera marki Huawei. W grudniu 2017 roku zaobserwowano kolejny wariant Satori. Zauważono także, że botnet stworzony przez to oprogramowanie wyszukiwał koparki kryptowaluty Ethereum. Dokładny cel tego działania nie jest znany, ale brać pod uwagę należy chęć sprawcy do znalezienia luk lub podatności i dokonanie ataku na te urządzenia.[159] W 2019 roku 21-letni Kenneth Currin Schuchman (używający online pseudonimów Nexus i Nexus Zeta) przyznał się do pomocy i współtworzenia razem z dwoma innymi osobami botnetu Satori, który wykorzystywał przepustowość około 100 tyś. urządzeń wykorzystujących funkcjonalności Internetu Rzeczy[160]. Według doniesień jego umiejętności obfuskacji działań pozostawiały wiele do życzenia: domena, na której postawiony został serwer *command & control* zarejstrowany został na adres mailowy „nexuszeta1337@gmail.com". Taki sam został z kolei użyty do rejestracji spółki „ZetaSec Inc." przez osobę o imieniu „Kenny Schuchman" z adresem w Vancouver w stanie Waszyngton[161]. Biorąc pod uwagę tożsamość sprawcy botnetu wykorzystującego oprogramowanie Satori, należy zauważyć jak groźne potrafią być narzędzia w rękach nawet niezbyt wykwalifikowanego hakera. Brak umiejętności programistycznych nie jest wskaźnikiem przekładającym się na automatyczny brak powodzenia ataków na urządzenia lub sieci.

Abstrahując od kwestii możliwości rzeczywistego przypisania sprawstwa za to zdarzenie, to dokonując analizy pod kątem polskiego prawa karnego w przypadku gdyby zdarzenie miało miejsce w jurysdykcji polskich organów ścigania, sprawcy dopuścili by

[159] https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/satori (dostęp 31.10.2020).
[160] https://krebsonsecurity.com/2019/09/satori-iot-botnet-operator-pleads-guilty/ (dostęp 31.10.2020).
[161] https://krebsonsecurity.com/2018/09/alleged-satori-iot-botnet-operator-sought-media-spotlight-got-indicted/ (dostęp 31.10.2020).

się przestępstwa zakłócania pracy w sieci (art. 269a k.k), polegającego na istotnym zakłóceniu pracy systemu lub sieci teleinformatycznej poprzez, tak jak to ma miejsce w tym przypadku, utrudnienie do nich dostępu nie będąc przy tym do tego uprawnionym. Wypełnienie znamion powyższego przestępstwa można z dużym prawdopodobieństwem, wręcz graniczącym z pewnością, przypisać sprawcy lub sprawcom. W doktrynie wskazuje się, że zakłócenie pracy systemu lub sieci to w szczególności atak DDoS, czyli dokładnie taki jak w przypadku *Dyn cyber attack*[162]. W razie ujawnienia innych okoliczności na dalszym etapie postępowania możliwym byłoby zarzucenie dodatkowych czynów, po wypełnieniu ich znamion.

Najistotniejszym faktem wynikającym z *Dyn cyber attack* jest to, że po raz pierwszy zastosowano urządzenia wykorzystujące standardy komunikacji bezprzewodowej oraz posiadające dostęp do Internetu. Co więcej wykorzystano je w ogromnej liczbie i wiodącej roli, umożliwiającej przeprowadzenie ataku, a więc dokonanie przestęstwa. Ukazuje to niezwykły potencjał wykorzystania koncepcji Internetu Rzeczy do popełniania przestępstw, Wskazuje również na fakt, jak bardzo problematyczne może być ustalenie sprawcy czynu, gdy mamy do czynienia z wykorzystaniem funkcjonalności lub podatności Internetu Rzeczy w połączeniu z użyciem ogólnodostępnego szkodliwego oprogramowania lub programów o podwójnym (legalnym i nielegalnym) zastosowaniu. Przykuwa uwagę kwestia jak niewielki, zdezaktualizowany lub wadliwy musiał być poziom zabezpieczeń urządzeń wchodzących w skład koncepcji Internetu Rzeczy, a wykorzystanych do *Dyn cyber attack*. To z kolei umożliwiło dokonanie ataku na tak ogromną ilość różnego typu urządzeń, pochodzących od różnych producentów oraz w efekcie przeprowadzenie ataku na niespotykaną do tej pory skalę. Uświadomiło także zarówno producentom, jak i użytkownikom jak wielkim zagrożeniem może być brak zabezpieczeń lub ich nieadekwatność oraz wynikające z tego niebezpieczeństwa dla potencjalnie każdego użytkownika Internetu.

[162] A. Lach, *Art. 269(a)*, w: V. Konarska-Wrzosek (red.), *Kodeks karny. Komentarz*, Wolters Kluwer, Warszawa 2016.

Rozdział 7. Zagrożenia i wyzwania

Rozwój koncepcji Internetu Rzeczy wymaga zwrócenia uwagi na obecne i przyszłe zagrożenia oraz wyzwania stojące przed organami ścigania, wymiaru sprawiedliwości oraz badaczy z zakresu prawa, jak i kryminalistyki. Niczym nieograniczony rozwój Internetu Rzeczy prowadzić może do zwiększenia zagrożenia atakami skierowanymi zarówno przeciwko bezpieczeństwu państwa bądź państw, ale też poszczególnych osób. Należy wskazać i określić najważniejsze spodziewane kierunki rozwoju tej koncepcji. Nie jest to jednak katalog zamknięty. Dynamizm i brak jednolitości rozwoju Internetu Rzeczy nie pozwala na jednoznaczne i niepozostawiające wątpliwości określenie kierunków rozwoju tej koncepcji. Nowe techniki i technologie informatyczne wpływają na praktycznie każdą sferę życia. Często są to problemy interdyscyplinarne, nieograniczające się do tylko jednego aspektu codziennego życia. Wymagają rozszerzonego, wielopłaszczyznowego podejścia łączącego w sobie niejeden aspekt życia. Wymagana jest współpraca pomiędzy ekspertami z wielu dziedzin, tak prawa jak i informatyki.

Studia przypadków, doniesienia i podsumowania badań naukowych wraz z przykładami pokazują obecny stanu rozwoju koncepcji Internetu Rzeczy. Pozwala to poruszać się w sferze stosunkowo pewnej, nierzadko odpowiednio empirycznie zbadanej lub pozostającej w trakcie tego rodzaju rozważań. Natomiast predykcja przyszłego, potencjalnego stanu rzeczy ma charakter generalny, a przez to także niepewny. Szczególnie w zakresie cyberprzestępczości jest to zadanie niełatwe. Wprost proporcjonalnie do rozwoju technicznych aspektów informatyki, rośnie także liczba potencjalnych zagrożeń oraz wyzwań. Szukanie odpowiedzi na to, co może być zagrożeniem w najbliższej przyszłości, aby w adekwatny sposób realizować prewencyjny cel kryminalistyki, jest niezbędne i konieczne. Branie pod uwagę historycznego aspektu cyberprzestępczości jest niezbędne, jeśli jakakolwiek działalność o charakterze predykcyjnym ma mieć miejsce i ma to być skuteczne.

7.1 Inteligentne miasta i systemy SCADA

Idea tzw. inteligentnych miast jest rozwijana od wielu lat. Wobec rozwoju technicznego i wzrostu popularności wielu metod komunikacji bezprzewodowej ulega ona

na przestrzeni ostatnich lat zmianom. Obecnie koncepcja tzw. inteligentnych miast (ang. smart-city*)* zakłada spełnienie więcej niż tylko warunku szerokiego wykorzystywania nowoczesnych technologii informacyjnych. Konieczne jest ich wykorzystanie jako podstawowego elementu funkcjonalnego i zarządzającego fundamentalnymi elementami miasta jak transportem, gospodarką energetyczną i dystrybucyjną mediów, przykładowo energią elektryczną lub wodą miejską. Kolejnym warunkiem jest też, aby nowoczesnym móc określić model zarządzania miastem przez władze, a także zachowania mieszkańców, instytucji, przedsiębiorstw, uczelni wyższych funkcjonujących w mieście. Dopiero w sytuacji, gdy te wszystkie elementy będą ze sobą harmonijnie współpracować w realizacji koncepcji nowocześnie funkcjonującego i zarządzanego miasta, wtedy będzie można określić je mianem *smart*[163].

W wymiarze dotyczącym mieszkańców chodzi między innymi o przejrzyste zasady funkcjonowania w mieście, budżet partycypacyjny, szeroko pojętą aktywność i oddolność działań mieszkańców. Ma to na celu wspieranie aktywizacji lokalnej osób przebywających na co dzień w jednej okolicy oraz budujących społeczność lokalna w skali mikro – przykładowo dzielnicy – i makro – całego miasta. Niewątpliwie ważna jest współpraca mieszkańców z władzami, partycypacja w projektach miasta, natomiast rolą władz miasta i jego przedstawicieli jest organizowanie debat oraz informowanie o prowadzonych i zaplanowanych projektach. Czynnikami warunkującymi implementację konkretnych rozwiązań będą plany podjęte przez same miasta po przeanalizowaniu warunków i korzyści, a także możliwego wsparcia Unii Europejskiej np. w ramach strategii Europa 2020[164]. Przynajmniej w wymiarze europejskim może mieć to decydujące znaczenie dla wielu europejskich metropolii. Zbudowanie systemu funkcjonowania miasta w pełni odzwierciedlającego wymagania koncepcji inteligentnego miasta wymaga dużych nakładów finansowych. Nierzadko szybkie wdrożenie rozwiązań może przekraczać możliwości przeciętnego miasta, dlatego wsparcie instytucji unijnych może przełożyć się na prężniejszy rozwój tego typu rozwiązań, a przez to może powodować nowe zagrożenia cyberprzestępczością.

---

[163] J. Olbrycht, *Idea smart city*, w: G. Szpor (red.), *Internet Rzeczy*…, op. cit.

[164] Komunikat Komisji Europa 2020. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, COM/2010/2020 końcowy, http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52010DC2020 (dostęp 30.04.2018).

Najistotniejszym i najbardziej wrażliwym punktem, biorąc pod uwagę koncepcję Internetu Rzeczy są systemy SCADA (ang. *Supervisory Control And Data Acquisition*). Dla potencjalnego sprawcy cyberprzestępstwa byłby to najbardziej korzystny do zaatakowania element. Służą one do zarządzania infrastrukturą krytyczną oraz zbierania pomiarów, wizualizowania ich, sterowania działaniami podłączonych urządzeń oraz archiwizowania danych i wykrywania ewentualne nieprawidłowości. Przykładowo system SCADA można wykorzystać do mierzenia i kontrolowania ciśnienia na zaworach w miejskich wodociągach bądź monitorowania przepływu, natężenia i napięcia prądu w miejskiej elektrowni. W Komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 24.04.2011 r. można znaleźć następującą definicję inteligentnych sieci energetycznych jako sieci elektroenergetycznych, zdolnych do integrowania działania wszystkich podłączonych do nich użytkowników. Niezależnie czy będą to wytwórcy, konsumenci i użytkownicy zaliczani do obu tych kategorii. Ma to na celu stworzenie gospodarczo oszczędnego, zgodnego z zasadami zrównoważonego rozwoju systemu energetycznego charakteryzującego się niskim poziomem strat oraz wysoką jakością i bezpieczeństwem dostaw[165].

Stosowanie rozwiązań w postaci systemów pomiarowych, zdolnych do udostępniania zgromadzonych danych dotyczących zużycia prądu użytkownikowi jest bardzo wygodnym rozwiązaniem. Umożliwia to kontrolę wydatków na energię elektryczną. Tego typu inteligentne mierniki danych można spokojnie zaliczyć jako część Internetu Rzeczy. Gromadzenie i przekazywanie na bieżąco tego typu danych przez Internet do użytkownika przykładowo na telefon lub komputer stwarza możliwość ataku. Dotyczy to zarówno urządzenia, na które wysyłany jest sygnał, jak i wysyłającego – czyli w tym przypadku system SCADA. Ponadto dostęp do danych, choćby o poziomie zużycia prądu, może umożliwić potencjalnym sprawcom przestępstwa wnioskowanie o zamożności potencjalnej ofiary. Ponadto, może to pomóc określić czas przebywania celu w domu[166]. Nietrudno sobie wyobrazić taką sytuację: Przestępca zamierzający dokonać

---

[165] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 24.04.2011 r. „Inteligentne sieci energetyczne: od innowacji do wdrożenia", COM/2011/0202 wersja ostateczna, http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52011DC0202 (dostęp 30.04.2018).

[166] M. Czarnecka, *Inteligentne opomiarowanie energii elektrycznej a prawa konsumentów*, w: G. Szpor (red.), *Internet Rzeczy*…, op. cit.

kradzieży z włamaniem, nie wie kiedy właścicieli są w domu. Potrzebuje poznać tę informację, aby mógł w spokoju dokonać czynu. W sytuacji, gdy posiada odpowiednie umiejętności lub wykorzysta ogólnodostępne narzędzia, a potencjalne ofiary korzystają z usług operatora energii elektrycznej, na bieżąco przesyłającego informacje o zużyciu energii za pośrednictwem Internetu i brak jest wystarczających zabezpieczeń, to istnieje kilka możliwości dla sprawcy. Może włamać się do źle lub niezabezpieczonej domowej sieci Wi-Fi (wystarczy, że właściciele nie zmienili domyślnego hasła routera). Automatycznie podłączony do niej telefon, na który wysyłane są dane z elektrowni, staje się podatny na wyciąganie z niego informacji. W wyniku tego atakujący uzyskuje także dostęp do urządzenia, w tym także do aplikacji monitorującej zużycie energii oraz innych informacji. W tym momencie istnieją dwa możliwe scenariusze. Jeżeli aplikacja archiwizuje dane z jakiegoś wycinka czasu, to wystarczy analiza otrzymanego materiału, aby określić, kiedy domownicy są obecni. Natomiast w przypadku, gdy aplikacja takich danych nie archiwizuje to wystarczy, że od tego momentu przez pewien czas sprawca będzie monitorował zużycie prądu. W wyniku analizy pozyskanych danych może wywnioskować pożądane informacje. Tak w jednym, jak i w drugim przypadku umożliwia to dokonanie przestępstwa bez konieczności fizycznej obserwacji celu, co zmniejsza ryzyko wykrycia bądź zaniepokojenia potencjalnych ofiar.

Sytuacja przedstawiona w akapicie powyżej nie jest jedyną możliwą do wyobrażenia sobie sytuacją, w której systemy SCADA zostają wykorzystane do popełniania przestępstw. Poważnym zagrożeniem wynikającym ściśle z ich przeznaczenia jest liczba osób i instytucji mogących być ofiarami potencjalnego ataku. W sytuacji, gdy w mieście lub nawet w państwie istnieje jeden zintegrowany system zarządzający i monitorujący pracę poszczególnych systemów SCADA w elektrowniach, wodociągach, odpowiedzialne za dostęp do miejskiej lub państwowej sieci internetowej, systemów bankowych i giełdy papierów wartościowych, a także wszelkiej maści instytucji oraz organizacji rządowych i samorządowych, to potencjalnymi ofiarami będą nie tylko ich siedziby, ale również potencjalnie każda osoba. Efekty zewnętrznego ataku dokonanego na jeden system zarządzający mniejszymi systemami może taką osobę dotknąć pośrednio lub bezpośrednio - w miejscu pracy, wypoczynku, na zakupach, uczelni, w domu i szkole, bądź w szpitalu. Ucierpieć może na tym nie tylko stan jego konta lub szerzej sytuacja materialna, ale również bezpośrednio zdrowie i życie jego oraz jego bliskich.

Podsumowując część poświęconą systemom SCADA, a w szerszym kontekście również inteligentnym miastom, należy stwierdzić, że przy sprzyjających sprawcy okolicznościach stwarza to ogromne zagrożenie dla bezpieczeństwa tak publicznego, jak i prywatnego. Mówiąc o głównych czynnikach wpływających na zagrożenia należy przez to rozumieć błędne lub brak zabezpieczenia komunikacji bezprzewodowej, nieaktualizowanie systemów odpowiedzialnych za bezpieczeństwo, korzystanie z urządzeń z nienaprawionymi podatnościami lub błąd ludzki, jak na przykład atak socjotechniczny. Połączenie funkcjonalności oraz podatności zarówno Internetu Rzeczy, jak i systemów SCADA, może być katastrofalne w skutkach. Szczególnie wobec ataku wykorzystującego tylko jedną ze wspomnianych koncepcji. Uzasadnieniem dla tego twierdzenia, jest fakt, że w wyniku połączonego ataku możliwa jest jego większa skala, a przez to – większa potencjalna liczba ofiar. Ataki na system SCADA nie są powszechne, jednak historia już zna takie przypadki. Najbardziej znane to wirus Stuxnet, mający powstrzymać rozwój irańskiego programu nuklearnego[167]. Innym przykładem mogą być wydarzenia z grudnia 2015 r. na Ukrainie[168], gdzie wirus BlackEnergy Trojan spowodował awarię systemów SCADA w punktach przesyłowych jednej z firm energetycznych. Przestały one działać, co doprowadziło do tego, że w tysiącach domów zabrakło prądu[169]. Można sobie jedynie wyobrazić, co by było, gdyby połączyć to z atakami wykorzystującymi podatności lub funkcjonalności Internetu Rzeczy. Zaatakowanych mogłoby zostać więcej punktów w tym samym czasie, a sama awaria mogłaby trwać dłużej i obejmować większy obszar. Z kolei wirus Stuxnet obrazuje zdolności i efekty, jakie może wywołać ściśle ukierunkowany atak.

7.2 Terroryzm

Zagrożenie cyberterroryzmem, czyli aktami przemocy przeprowadzonymi przy użyciu komputerów i innych technologii informatycznych, w celu zniszczenia lub zakłócenia działania systemów informatycznych. Mają one wywołać panikę i zamieszanie,

[167] K. Zetter, *An unprecedented look at Stuxnet, the world's first digital weapon*, WIRED, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ (dostęp 30.04.2018).

[168] P. Polityuk, *Ukraine to probe suspected Russian cyber attack on grid*, http://www.reuters.com/article/us-ukraine-crisis-malware-idUSKBN0UE0ZZ20151231 (dostęp 30.04.2018).

[169] D. Goodin, *First known hacker-caused power outage signals troubling escalation*, Ars Technica, 2016, http://arstechnica.com/security/2016/01/first-known-hacker-caused-power-outage-signals-troubling-escalation/ (dostęp 30.04.2018).

a tym samym poczucie zagrożenia wśród ludności, w celu zmuszenia rządu lub innych organizacji do spełnienia politycznych, społecznych czy też ideologicznych żądań[170], jest uznawane za niosące ze sobą potencjalnie niezwykle poważne skutki. Tego typu ataku się spodziewano jako następstwo ataków z 11 września 2001 r. Mimo, że nie miało to miejsca , to nie znaczy, że widmo podobnego czynu zostało zażegnane całkowicie. Inną definicją cyberterroryzmu, która została sformułowana już w 1997 r. przez M. Pollitta jest: *cyberterroryzm to przemyślany, politycznie umotywowany atak, skierowany na informacje, systemy komputerowe, programy i bazy danych, który prowadzi do zniszczenia celów niewojskowych, przeprowadzony przez grupy obce narodowościowo lub przez tajnych agentów*[171]. Czym jednak miałby się taki czyn charakteryzować? Jakie systemy bądź urządzenia mogłyby być najodpowiedniejszym celem dla terrorystów? Należy zadać sobie także pytanie – czy tego typu atak byłby celowy z punktu widzenia działania grup terrorystycznych? Czy opłacalnym byłoby zaangażowanie środków do przeprowadzenia ataku na konkretny system informatyczny, czy efekt zastraszenia ludności oraz zaznaczenia swoich politycznych przekonań zostałby w adekwatny sposób osiągnięty?

Podstawowymi cechami charakterystycznymi dla ataków przeprowadzanych przez grupy terrorystyczne są: użycie siły, polityczne motywy oraz poczucie zagrożenia wywołane w społeczeństwie[172]. Zgodnie z polskim kodeksem karnym przestępstwo o charakterze terrorystycznym charakteryzuje się tym, że musi spełniać przesłankę celowościową, to znaczy musi być popełniony w celu poważnego zastraszenia wielu osób, zmuszenia organu władzy publicznej RP lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowe. Podobne przesłanki celowościowe musi spełniać groźba popełnienia takiego czynu, aby wypełnić znamiona wspomnianego artykułu k.k.[173].

Ponadto, jak wskazuje A. Suchorzewska[174], powołując się przy tym na K. Indeckiego[175], w ustawodawstwie polskim i literaturze znaleźć można trzy główne typy

---

[170] L. Garrison, M. Grand, *Cyberterrorism: An evolving concept*, US National Infrastructure Protection Centre, 2001, za: A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Oficyna a Wolters Kluwer business, Warszawa 2010.

[171] M.M. Pollitt, *Cyberterrorism – fact or fancy?*, „Computer Fraud & Security" 1998, t. 1998(2), https://doi.org/10.1016/S1361-3723(00)87009-8.

[172] A. Suchorzewska, op. cit.

[173] Kodeks karny.

[174] A. Suchorzewska, op. cit.

definicji odnoszących się do terroryzmu. Pierwsze o charakterze jak najbardziej generalnym i abstrakcyjnym mające na celu określenie jedynie esencjonalnych cech zjawiska terroryzmu bez uszczegółowiania ich w żaden konkretny sposób i bez dokonywania dystynkcji na poszczególne formy, jakie terroryzm może przybrać. Drugi typ definicji to definicje cząstkowe, które charakteryzują się skrajnie innym podejściem niż definicje generalne. Starają się dokładnie określić cechy poszczególne rodzajów terroryzmu. Trzecim typem, a zarazem ostatnim, są definicje mieszane. Ich istota polega na tym, że koncentrują się na połączeniu obu poprzednio wymienionych definicji. Wskazują konkretne cechy wyróżniające rodzaje terroryzmu wraz z odniesieniem ich do generalnych zasad[176]. Kolejną istotną kwestią poruszaną w literaturze polskojęzycznej jest rozróżnienie dwóch pojęć, a konkretnie terroryzmu i aktu terrorystycznego. W celu scharakteryzowania tego drugiego należy wziąć pod uwagę następujące okoliczności:

- zachowanie sprawcy, czyli podjęte przez niego działania oparte są na przemocy lub groźbie jej użycia,
- motywy działania, to znaczy powody dla danego zachowania sprawcy; mogą być to motywy osobiste, ideologiczne (związane z ideologią, przynależnością do grup politycznych etc.) i strategiczne (sprawca ma inny lub dodatkowy cel oprócz jedynie wzbudzenia strachu i grozy, przykładowo jakiś cel nadrzędny pokroju obalenia lub zmiany rządu, wypuszczenia więźniów politycznych, zmiany kierunku i działania rządu etc.),
- cele i osiągnięte rezultaty, czyli zgodnie z ogólną definicją dopuszczenia się aktu lub aktów przemocy oraz wywołanie stanu terroru,
- sprawstwo, to znaczy określenie czy mamy do czynienia z samotny sprawcą, grupą osób oraz stopnia sprawstwa konkretnej osoby, jeżeli mamy do czynienia z grupą (sprawstwo, współsprawstwo, podżeganie)[177].

Terroryzm to pojęcie zdecydowanie szersze, opisujące zjawisko tworzenia się i działania grup o charakterze terrorystycznym. Znaczeniowo może zawierać w sobie także akty terrorystyczne. W tym miejscu warto również wspomnieć o definicji zdarzenia o charakterze terrorystycznym wprowadzonego przez ustawę z dnia 10 czerwca 2016 r. –

---

[175] K. Indecki, *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 1998.

[176] Ibidem.

[177] Ibidem.

Ustawa o działaniach antyterrorystycznych[178]. Jest to sytuacja, co do której istnieje podejrzenie, że powstała na skutek przestępstwa o charakterze terrorystycznym lub zagrożenie zaistnienia takowego[179]. W sensie znaczeniowym oznacza to rozszerzenie zakresu definicji kodeksowej o zagrożenie zaistnienia ujemnego społecznie zdarzenia o charakterze terrorystycznym. Jest to istotna i daleko idąca zmiana względem definicji zawartej w k.k. Można by się zastanawiać na ile jest ona zasadna. Za bezkrytycznym jej przyjęciem mógłby przemawiać obecny stan zagrożenia atakami terrorystycznymi w Europie i na świecie, a także bardziej zintensyfikowana w ostatnich latach działalność tzw. Państwa Islamskiego. Jednak zdecydowanie negatywnym wskazaniem za uznaniem tego rozszerzenia za trafne jest jego połączenie z innymi przepisami z Ustawy o działaniach antyterrorystycznych. Szczególnie wobec wątpliwości co do ich konstytucyjności podnoszonymi przez Rzecznika Praw Obywatelskich[180].

Współczesny terroryzm w nieunikniony sposób w coraz szerszym zakresie wykorzystuje do swojej działalności nowe technologie. Rozwój Internetu i mediów społecznościowych służyć może do zapewnienia ułatwionej komunikacji z aktualnymi członkami grupy lub grup terrorystycznych, koordynowania ich działań oraz rekrutacji nowych osób i szerzenia wyznawanej ideologii. Dodatkowo rozwój technologii i mediów internetowych ułatwia szerzenie propagandy i wiedzy o konkretnych grupach. W tym zakresie najłatwiej w ostatnich latach zaobserwować można nowe podejście w kwestii rekrutacji ludzi przez tzw. Państwo Islamskie. Chcąc dotrzeć szczególnie do młodych ludzi osoby rekrutujące poruszają się w środowisku doskonale znanym nastolatkom i młodzieży. Stosują także techniki i sposoby komunikacji, którymi najłatwiej do tego typu osób dotrzeć. Przykładem na to mogą być doniesienia z początku 2015 r. Wtenczas BBC donosiło, że przy użyciu *agresywnych sieciowych kampanii w mediach społecznościowych* osoby powiązane z tzw. Państwem Islamskim rekrutowały młode osoby z Wielkiej Brytanii do przyjazdu do Syrii. Opisano to na przypadku trzech nastoletnich dziewczynek w wieku między 15 a 16 rokiem życia, które dały się przekonać do wyjazdu do Syrii, aby zostać żonami dżihadystów (ang. *jihadi bride*)[181]. Zdarzenie to nie jest odosobnione,

[178] Dz.U. z 2018 r., poz. 452.

[179] Ibidem.

[180] *Rzecznik Praw Obywatelskich skarży ustawę antyterrorystyczną do Trybunału Konstytucyjnego*, https://www.rpo.gov.pl/pl/content/RPO-skarzy-ustawe-antyterrorystyczna-do-TK (dostęp 30.04.2018).

[181] D. Harvey, *How Islamic State extremists use social media to recruit*, BBC, http://www.bbc.co.uk/newsbeat/article/31574846/how-islamic-state-extremists-use-social-media-to-recruit (dostęp 30.04.2018).

w informacjach opublikowanych w sierpniu 2016 r., gdy donoszono, że serwisy takie jak Facebook czy Twitter nie są w stanie powstrzymać działalności członków organizacji terrorystycznych, a stają się niezbędnymi a zarazem doskonałymi platformami do działalności[182]. Wskazuje się, że prawidłowym sposobem postępowania w celu przeciwdziałania tej aktywności jest zwalczanie działalności przedstawicieli organizacji terrorystycznych na wymienionych wyżej serwisach internetowych przy użyciu systemów monitorujących i filtrujących treść, dostosowanych do wyszukiwania określonych treści w celu ich usunięcia. Ponadto w przypadku przywołanego już tzw. Państwa Islamskiego za kampanie propagandowe oraz medialne w Internecie na portalach społecznościowych i platformach z filmami jak YouTube, odpowiadają wręcz zorganizowane grupy przypominające agencje medialne i wytwórnie filmowe. Produkują materiały na poziomie podobnym do produkcji filmowych. W ten sposób łatwiej i szybciej docierają do ludzi w zachodniej Europie i w Stanach Zjednoczonych. Do tego typu zadań, ukierunkowanych na odbiorców na tzw. Zachodzie, zostało powołane w 2014 roku Centrum Medialne Al-Hayat (ang. *Al-Hayat Media Center*). Jego działalność skierowana jest głównie do osób niepochodzących z arabskich kręgów kulturowych, a w szczególności ludzi młodych. Wśród materiałów wyprodukowanych przez Centrum można znaleźć nagrania wideo z egzekucji, na przykład amerykańskich dziennikarzy J. Foleya i S. Sotloffa, jordańskiego pilota Muatha al-Kasaesbeha czy innych zakładników, ale także filmy zachęcające do przyjazdu odnoszące się do szeroko rozumianej popkultury. Inspirację dla twórców stanowią przykładowo gry wideo takie jak seria *Grand Theft Auto* czy *Call of Duty*, zachęcające do przyjazdu w celu przeżycia wydarzeń z ulubionej gry na żywo, w prawdziwym świecie[183]. Repertuar Centrum nie ogranicza się jedynie do scen ukazujących przemoc lub też zachęcających poprzez nią do przyjazdu na *świętą wojnę*. W produkcjach przedstawiane są także sceny ukazujące bojowników pomagających ludności cywilnej, udzielających pomocy chorym i rannym w szpitalu oraz dających dzieciom cukierki[184]. Do szerzenia propagandy dżihadyści wykorzystują bojowników zrekrutowanych spośród

---

[182] A. Griffin, *Facebook, Twitter and Google are 'the lifeblood of Daesh', according to major new report into ISIS use of social media*, Independent, 25 sierpnia 2016 r., https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-twitter-google-isis-daesh-internet-youtube-social-media-home-affairs-a7208131.html (dostęp 30.04.2018).

[183] S. Rose, *The Isis propaganda war: a hi-tech media jihad*, „The Guardian", 7 października 2014 r., https://www.theguardian.com/world/2014/oct/07/isis-media-machine-propaganda-war (dostęp 30.04.2018).

[184] A. Imran, *Cyber-extremism: Isis and the power of social media*, „Social Science and Public Policy" 2017, t. 54(2), https://doi.org/10.1007/s12115-017-0114-0 (dostęp 30.04.2018).

obywateli Zachodu, którzy opowiadają o idylli, jaka panuje w tzw. Państwie Islamskim, o tym jakim doskonałym miejscem jest ono do życia i jak wspaniałe jest prawo szariatu, z sukcesem zastępujące pozostałe ideologie i systemy państwowe[185].

Wszystkie materiały wyprodukowane przez Al-Hayat mają spełniać przede wszystkim cele propagandowe, ale też wywołać strach. Znaczy to, że podpadają pod kategorią szeroko pojętych narzędzi do realizacji czynów o charakterze terrorystycznym. Wykorzystanie przez terrorystów środków używanych przez media zachodnie, tak dobrze znanych ludziom mieszkającym w Europie i Ameryce, pozwala na łatwiejsze dotarcie do nich i przekonanie do przekazywanego obrazu. Może się to przełożyć na wzrost liczby sympatyków i bojowników, czy to zaangażowanych w walki na Bliskim Wschodzie, czy też tych zostających w Europie lub Ameryce i gotowych do przeprowadzania zamachów.

W ostatnich latach zagrożenie czynami o charakterze terrorystycznym wzrosło, między innymi w wyniku działalności terrorystycznej tzw. samotnych wilków. W ramach programu PRIME[186] ten typ działań został zbadany biorąc pod uwagę takie czynniki jak sposób i czas potrzebny do radykalizacji terrorystów, metody w jaki sposób się dokonała, w tym między innymi zbadanie kwestii radykalizacji poprzez Internet. Kolejne kwestie wynikające poniekąd z problemu samej radykalizacji, które pozostawały w sferze zainteresowań badaczy, to motywacja ataków tzw. samotnych wilków, a także kiedy i jak pozyskują umiejętności i zdolności wykorzystywane w przygotowaniu lub przeprowadzaniu ataków. Ponadto skupiono się na analizie zarówno mediów cyfrowych i elektronicznych środków komunikacji, jak i tych analogowych jak na przykład gazety. W ramach szeroko zakrojonych badań podejmowano kwestie dotyczące działalności terrorystów, ale również te dotyczące zwalczania zagrożeń związanych *stricte* z terroryzmem tzw. samotnych wilków. W ramach ankiet zbadano wiedzę osób związanych z organami ścigania, dotyczącą najskuteczniejszych narzędzi do zapobiegania problemowi radykalizacji, a także tę dotyczącą sposobów radykalizacji potencjalnych sprawców aktów terrorystycznych. Wśród sposobów wymienionych jako najbardziej efektywne przez osoby reprezentujące europejskie i północnoamerykańskie służby wskazano: monitorowanie Internetu, środki nadzoru komunikacji elektronicznej, analizę

[185] S. Rose, op. cit.

[186] *PReventing, Interdicting and Mitigating Extremist events: Defending against lone actor extremism*; badania prowadzone w ramach programu FP7 Unii Europejskiej, w który zaangażowanych było sześć ośrodków uniwersyteckich z Wielkiej Brytanii, Polski, Holandii, Danii i Izraela. Polskim partnerem był Uniwersytet Warszawski.

kryminalną, korzystanie z informatorów, operacje policyjne polegające na infiltracji badanego środowiska oraz zakup kontrolowany. Natomiast osoby reprezentujące indyjskie służby jako najbardziej efektywne wskazali: analizę kryminalną, monitorowanie Internetu, operacje policyjne polegające na infiltracji badanego środowiska, kontrolę rynku sprzedaży przedmiotów i surowców lub świadczenia usług niezbędnych terrorystom oraz korzystanie z informatorów[187].

Z połączonych wyników obu przytoczonych wyżej ankiet wyłaniają się interesujące fakty z punktu widzenia zagrożeń wynikających z przestępczości, wykorzystującej funkcjonalności lub podatności Internetu Rzeczy. Mianowicie za najbardziej skuteczne (powyżej 90% odpowiedzi) sposoby przeciwdziałania terroryzmowi uznano monitorowanie Internetu, środki nadzoru komunikacji elektronicznej oraz analizę kryminalną. Dwie metody spośród trzech wymienionych skupiają się ściśle wokół szeroko pojętego środowiska internetowego, a również trzecia może wykorzystywać dowody oraz wnioski uzyskane w toku zabezpieczania dowodów cyfrowych lub sieciowych. Dotyczy to przykładowo lokalizacji urządzeń telefonicznych oraz elektronicznych, aktywność na różnego typu urządzeniach elektronicznych bądź elektroniczne systemy monitoringu. Analiza powyższych wyników może prowadzić do wniosku, że osoby zajmujące się ściganiem przestępstw świadome są skuteczności i efektywności wybranych aspektów nowych technologii w zapobieganiu i ściganiu przestępstw, przynajmniej do pewnego stopnia. Monitoring Internetu w sposób naturalny może być różnorodnie rozumiany oraz mieć inne konotacje znaczeniowe w zależności od kraju i specyfiki działania służb oraz organów ścigania i wymiaru sprawiedliwości. Jednak fakt, iż jest wskazywany jako istotny i skuteczny sposób pozwala na wysnucie powyższego wniosku. Świadomość znaczenia i doniosłości nowych technologii oraz wykorzystania elektronicznych środków nadzoru i obserwacji w pracy wykrywczej i śledczej ułatwia pracę badaczom z zakresu kryminalistyki. Oznacza to bowiem, że wytłumaczenie sposobu działania nowych zjawisk i koncepcji oraz ich wpływu na popełnianie i wykrywanie przestępstw będzie łatwiejsze. Jest to tym istotniejsze, że opierają się w ogromnej mierze na połączeniu wielu nowych technologii w ramach jednej koncepcji. Ostateczne wyniki badań, z uwagi na ich charakter oraz oparcie się w części o informacje niejawne, nie zostały w tym momencie opublikowane ani nie są dostępne publicznie. Jednak na podstawie ogólnie otwartych

[187] K. Gradoń, *Countering lone actor terrorism – preliminary findings of the PRIME project*, „Problemy Współczesnej Kryminalistyki" 2016, t. XX.

spotkań i dostępnych informacji już w tym momencie można określić jak wielkim niebezpieczeństwem i zagrożeniem jest wykorzystywanie nowych technologii do radykalizacji i pozyskiwania wiedzy przez terrorystów, w tym tzw. samotnych wilków oraz następnie do przygotowywania i dokonywania przez nich aktów terrorystycznych. Niewątpliwie Internet Rzeczy będzie mógł stanowić jeden z przyczółków i niezwykle skuteczne narzędzie ułatwiające, a w niektórych przypadkach takich jak ataki na infrastrukturę krytyczną, wręcz umożliwiające przeprowadzenie ataków o ogromnej skali.

7.3 Międzynarodowe prawo humanitarne – prawo konfliktów zbrojnych

Powiązania między międzynarodowym prawem humanitarnym (w skrócie MPH bądź IHL, ang. *International Humanitarian Law*), czyli prawem konfliktów zbrojnych, a Internetem Rzeczy mogą wydawać się w najlepszym wypadku nieoczywiste. Pomimo faktu, że na pierwszy rzut oka aktualnie takich związków może nie być, to nie sposób negować wpływu rozwoju nowych technologii w dziedzinie uzbrojenia. Aktualnymi trendami w tym zakresie jest odejście od *stricte* konwencjonalnego uzbrojenia armii lądowych w postaci pojazdów zmechanizowanych, czołgów etc., a rozwijanie systemów uderzenia dalekiego zasięgu takich jak drony oraz pociski rakietowe dalekiego zasięgu, a także innych zautomatyzowanych, autonomicznych oraz wymagających niewielkiego udziału człowieka. Rozwijane są systemy umożliwiające wypełnianie zadań bojowych, minimalizując przy tym potencjalne zagrożenie dla żołnierzy. Ma to na celu ochronę zdrowia i życia wyszkolonych żołnierzy, a także zminimalizowania kosztów samego szkolenia. Powoduje to tworzenie nowych, dotychczas nieistniejących, jednostek wojskowych w armii, zajmujących się obsługą dronów, pojazdów automatycznych i autonomicznych czy też tych zajmujących się *wojną w cyberprzestrzeni*. Pojęcie to może obejmować różnego typu działania – dezinformację, szerzenie propagandy, działalność wywiadowczą i kontrwywiadowczą, ale również ataki hakerskie przez specjalnie do tego wyszkolone osoby lub grupy, działające na zlecenie państw przeciwko innym krajom. Kwestia wykorzystania środków elektronicznych w walce czy też w działaniach przeciwko innym państwom nie są niczym nowym. Przykładami takich działań może być sprawa wirusa Stuxnet, który został specjalnie zaprojektowany w celu uszkodzenia irańskich

instalacji w ośrodkach wzbogacania uranu. W konsekwencji miało to doprowadzić do istotnego spowolnienia irańskiego programu nuklearnego[188]. Ponadto niewątpliwie zwracającym uwagę zdarzeniem był atak cybernetyczny na Estonię, czyli jedno z najbardziej zinformatyzowanych państw na świecie, który miał miejsce w 2007 r. Atak miał charakter ataku DDoS i spowodował wyłączenie stron internetowych większości estońskich instytucji, w tym parlamentu, ministerstw, banków, gazet oraz telewizji. Odpowiedzialnością obarczana jest Rosja, jednak brak jest ewidentnych dowodów wskazujących na ich udział w tym zdarzeniu. Z tego powodu nie do końca możliwe jest rozpatrywanie niniejszej sprawy jako przejawu agresji jednego państwa wobec drugiego. Jednym z efektów było powołanie *NATO Cooperative Cyber Defence Centre of Excellence,* w celu koordynacji opracowywania programów przeciwdziałania i zwalczania zagrożeń asymetrycznych i cyberatakami.

Na początku rozważań można by zadać pytanie – czy atak komputerowy bądź sieciowy może być uznany za agresję i działanie niezgodne z prawem międzynarodowym, zakazane przez konwencje? Czy można by porównać tak skrajne różne na pierwszy rzut oka zjawiska jak przykładowo aneksja i atak hakerski na informatyczne systemy zarządzające infrastrukturą krytyczną? Mimo faktu, że może się to wydawać nieoczywiste z punktu widzenia tradycyjnego ujęcia tzw. praw wojny bądź reguł wojny należy stwierdzić, że we współczesnym, mocno ucyfrowionym świecie działania przeciwko systemom i urządzeniom informatycznym mogą stanowić naruszenie prawa międzynarodowego i mogą być traktowane jako agresja. Niezależnie od celu działań - zakłócenia działania, uszkodzenia, zniszczenia czy też uzyskania kontroli nad nimi. Szczególnie jeśli będą one podjęte przez osoby działające jako żołnierze lub funkcjonariusze jednego państwa przeciw drugiemu. Rozpatrywanie tej kwestii nastręcza jednak wiele problemów, które są nieuniknione. Wynika to ze specyfiki międzynarodowego prawa humanitarnego i jego regulacji, mnogości i licznych niejednoznaczności w teorii i kazuistyce regulacji prawnych dotyczących konfliktów zbrojnych, a więc jego praktycznego stosowania. Dodatkowo w tym miejscu niezbędne jest również zdefiniowanie pojęcia konfliktu zbrojnego. Oznacza przejawy walki zbrojnej między państwami nawet wówczas, kiedy wojna nie zostanie wypowiedziana, jak również

[188] M. De Falco, *Stuxnet Facts Report, a Technical and Strategic Analysis,* NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/sites/default/files/multimedia/pdf/Falco2012_StuxnetFactsReport.pdf (dostęp 30.04.2018).

takie konflikty zbrojne, w których uczestniczą strony nieuznane za podmioty prawa międzynarodowego (strony wojujące)[189].

Podstawowymi kwestiami problematycznymi, wynikającymi z przypisywania odpowiedzialności za ataki sieciowe i komputerowe na styku z ogólnymi zasadami prawa konfliktów zbrojnych, są kwestie identyfikacji poszczególnych osób i ich ról. Niejednokrotnie ich status ulega zmianom, co dotyczy także w szerszym zakresie wszelkich podejmowanych działań i ich ograniczeń w ramach *ius in bello*[190]. Odnośnie pierwszej kwestii to pierwszymi przychodzącymi na myśl problemami będzie sytuacja, gdy pojawią się trudności, co do zidentyfikowania sprawcy czynu, które jedno państwo uzna za niezgodną z prawem międzynarodowym agresję przeprowadzoną w formie ataku sieciowego bądź komputerowego. Podstawowym problemem może być dotarcie i zidentyfikowanie sprawcy w ogóle, a następnie powiązanie go z państwem-domniemanym agresorem w sposób umożliwiający udowodnienie mu tego działania oraz jego motywacji. W przypadku działań podjętych przez funkcjonariuszy lub żołnierzy jednego państwa przeciw drugiemu sprawa powinna wydawać się oczywista. Można sobie jednak wyobrazić sytuację, w której wykorzysta się osoby wynajęte do przeprowadzenia ataku, których nie da się tym mianem określić oraz trudne będzie powiązanie ich z organami państwa lub siłami zbrojnymi. Jest to najbardziej sztandarowy przykład, nie wspominając choćby o ewentualnych zmianach statusu poszczególnych osób w trakcie trwania konfliktu z osoby cywilnej na uczestnika walki zbrojnej. Problematyczność w tej kwestii jest uwarunkowana również tym, że oprócz analizy przepisów umów międzynarodowych niezbędna jest kwestia zwyczaju międzynarodowego, Jest on konstytuowany przez zgodną praktykę oraz przekonanie o jej zgodności z prawem i tego, że tworzy to prawo (*opinio iuris sive necessitatis*). Zgodna praktyka powinna być rozumiana szeroko, jako akty poszczególnych państw i akty międzynarodowe, ponadto jej zgodność opiera się na jednolitości i jej nieprzerwanym stosowaniu. *Opinio iuris sive necessitatis* jest niezbędnym elementem zwyczaju międzynarodowego, ponieważ oprócz elementu obiektywnego, jakim jest praktyka, to konieczny jest element subiektywny w postaci przeświadczenia, że tworzy ona prawo[191].

---

[189] W. Góralczyk, S. Sawicki, *Prawo międzynarodowe publiczne w zarysie,* Wolters Kluwer, Warszawa 2017.

[190] Inaczej prawo konfliktów zbrojnych bądź międzynarodowe prawo humanitarne – przyp. autor.

[191] W. Góralczyk, S. Sawicki, op. cit.

Druga kwestia dotyczy ograniczeń ustalonych w umowach międzynarodowych oraz w ramach zwyczajów międzynarodowych. W głównej mierze odnosi się do podstawowych zasad MPH takich jak zasada humanitaryzmu, rozróżniania, proporcjonalności oraz konieczności wojskowej i ograniczeń oraz zakazów z nich wynikających. Zostały one określone między innymi w konwencjach haskich i genewskich oraz innych aktach regulujących status stron i osób na terenie konfliktu zbrojnego, także dopuszczalnych środków prowadzenia działań w jego trakcie. Kwestiami problematycznymi będzie uznanie ataków sieciowych i komputerowych jako niezgodnych z prawem konfliktów zbrojnych oraz szerzej prawem międzynarodowym. Jeśli tak, to na podstawie jakich regulacji, a w przypadku ich braku jak należy je sformułować.

Kolejnymi krokami w analizie zagrożeń związanych z cyberprzestępczością wykorzystaną do prowadzenia działań w ramach konfliktu zbrojnego będzie określenie ram prowadzenia ewentualnej *wojny w cyberprzestrzeni*. Musiałaby nastąpić zgoda, co do uznania jednej lub zbliżonych znaczeniowo do siebie definicji „cyberprzestrzeni", aby była możliwość uznania działań skierowanych przeciw sieciom i urządzeniom drugiej strony konfliktu zbrojnego za działania w jego ramach. Nie jest to tak proste, jak w przypadku działań konwencjonalnych, gdyż określenie terytorium państwa nie nastręcza większych problemów. W razie wątpliwości istnieje w tym zakresie ugruntowane orzecznictwo międzynarodowe, możliwe do wykorzystania w celu ustalenia statusu danego miejsca. W tym zakresie podjęto już działania, które swój początek mają w 2013 r.[192], a ich efekt dała wydana w tym samym roku publikacja powstała z inicjatywy *NATO Cooperative Cyber Defence Centre of Excellence* w Tallinnie[193]. Opisuje ona możliwość stosowania aktualnych norm prawa międzynarodowego i aplikowania przepisów oraz zwyczajów aktualnie obowiązujących do sytuacji związanych z wykorzystaniem nowoczesnych technologii w ramach konfliktów zbrojnych.W roku 2017 wydane zostało drugie wydanie wspomnianej publikacji pod tytułem *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (w skrócie *Tallinn Manual 2.0*)[194]. Opisuje szerzej problemy identyfikowania oraz klasyfikowania operacji w cyberprzestrzeni

[192] R. Tarnogórski, *Prawo konfliktów zbrojnych a cyberprzestrzeń*, „Biuletyn Polskiego Instytutu Spraw Międzynarodowych" 2013, nr 31(1007).

[193] *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge–New York 2013, w skrócie *Tallinn Manual*, draft pierwotnej wersji dostępny jest pod adresem: http://csef.ru/media/articles/3990/3990.pdf (dostęp 30.04.2018).

[194] https://ccdcoe.org/research/tallinn-manual/ (dostęp 30.04.2018).

podejmowanych w czasach pokoju i wskazuje sposób interpretacji przepisów w takim przypadku. Ponadto rozszerzono katalog zasad, określanych w systemie *common law* jako *black letter rule* lub *black letter laws*, z 95 do 154. Są to zasady oraz reguły ugruntowane, powszechnie znane i funkcjonujące w systemie prawnym, które nie podlegają kwestionowaniu przez większość lub zostały przyjęte jako tzw. „żelazne" zasady[195]. *Tallinn Manual 2.0* określa między innymi takie kwestie jak odniesienie zasad prawa międzynarodowego do cyberprzestrzeni np. suwerenność państw w wymiarze wewnętrznym, zewnętrznym oraz sytuacje naruszające wraz z konsekwencjami takiego zachowania. Ponadto, wskazuje granice jurysdykcji państw w przypadku operacji w cyberprzestrzeni, zarówno w charakterze ofiary jak i atakującego. Rozległym i ważnym rozdziałem w *Tallinn Manual 2.0* jest ten dotyczący odpowiedzialności za naruszenia zasad prawa międzynarodowego w cyberprzestrzeni wraz ze środkami, które państwa mogą podejmować w celu przeciwdziałania naruszeniom suwerenności. Autorzy dokonują także ważnej analizy operacji w cyberprzestrzeni, które *per se* nie są regulowane przez prawo międzynarodowe jak np. dokonywanie aktów cyberszpiegostwa w czasach pokoju oraz tzw. ugrupowania nieposiadające statusu państwowego (ang. *Non-State actors*). Pozostałe aspekty publikacji wskazują także sytuacje i granice użycia siły oraz podejmowania działań obronnych przez państwa, także tzw. wspólnej lub kolektywnej obrony. Nie brakuje także odniesień do innych aspektów międzynarodowego prawa takich jak prawo morskie, międzynarodowe prawo humanitarne (prawo konfliktów zbrojnych), kwestie neutralności i okupacji oraz specjalnego statusu niektórych osób i miejsc. Jak wskazują sami autorzy oraz co wynika z treści dokumentu, *Tallinn Manual 2.0* to rozbudowany komentarz pozwalający na wyjaśnienie wielu kwestii problematycznych lub dyskusyjnych powstających między państwami w wyniku ich suwerennej działalności lub obecności w cyberprzestrzeni. Umożliwia państwom odniesienie się do konkretnych zasad w sytuacji, gdy powstaje między nimi spór lub pojawia się sytuacja konfliktowa, co grozi dalszą eskalacją. Nierzadko wspomniane wyżej 154 zasady wynikające z ugruntowanego orzecznictwa międzynarodowego, co nadaje mu dodatkowego znaczenia w stosunkach między państwami i innymi podmiotami prawa międzynarodowego. Można zdecydowanie liczyć na rozbudowę tego typu dokumentów, a także być może na przekucie tego rodzaju eksperckich publikacji na rzeczywiste regulacje międzynarodowe uznawane na forum

[195] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge–New York 2017.

światowym. Polepszyłoby to poziom światowego bezpieczeństwa, a co najmniej pozwoliłoby na rozstrzygnięcie wielu problematycznych prawnie kwestii. Istnieje także szansa, że w kolejnych edycjach uwzględnione zostaną zagrożenia wynikające z rozwoju Internetu Rzeczy.

Problematyka związków prawa konfliktów zbrojnych z rozwojem techniki, a w konsekwencji wykorzystania jej w konfliktach zbrojnych jest szeroka i nie do końca opracowana. Należy jednak z optymizmem patrzeć na podejmowane skuteczne i wartościowe, z punktu widzenia nauki i praktyki, próby opracowania tejże kwestii. W kontekście związków międzynarodowego prawa humanitarnego i konkretnego aspektu nowoczesnych technologii, jakim jest Internet Rzeczy należy zwrócić uwagę, że takich badań nie ma aktualnie prowadzonych. Ciężko determinować i przesądzać o tym, czy będą podejmowane w najbliższej przyszłości, biorąc pod uwagę stopień zaawansowania badań naukowych w odniesieniu do prawa karnego i kryminalistyki. Należy jednak wysuwać postulat zbadania tychże związków w momencie, w którym określone zostaną ogólne ramy „wojny w cyberprzestrzeni" i jej miejsca w systematyce prawa konfliktów zbrojnych oraz szerzej międzynarodowego prawa publicznego. W tym aspekcie godną odnotowania jest publikacja autorstwa H. H. Dinniss pod tytułem *Cyber warfare and the laws of war* podejmująca tematykę „wojny w cyberprzestrzeni" w kontekście i w odniesieniu do prawa międzynarodowego. Obejmuje analizę różnych źródeł prawa międzynarodowego ze szczególnym uwzględnieniem tych dotyczących prawa konfliktów zbrojnych, co pozwala na dokładną i dogłębną analizę oraz syntezę tematu. W konsekwencji stanowi punkt wyjścia dla dalszych badań z punktu widzenia bardziej ogólnego bądź szczegółowych metod i technik stosowanych w ramach potencjalnych i już istniejących konfliktów zbrojnych, w których stosuje się szeroko pojęte metody prowadzenia działań w cyberprzestrzeni[196].

7.4 Działalność inspirowana lub sponsorowana przez inne państwa

[196] H.H. Dinniss, *Cyber Warfare and the Laws of War*, Cambridge University Press, New York 2012.

Funkcjonalnie oraz pod względem prawnym, a konkretnie mechanizmów i przepisów, które należałoby stosować w razie zaistnienia takiej sytuacji, ten aspekt jest związany z prawem konfliktów zbrojnych. Działania inspirowane lub sponsorowane przez państwa i skierowane przeciwko innym podmiotom prawa międzynarodowego wymagają oceny pod kątem zasad prawa międzynarodowego, w tym prawa konfliktów zbrojnych także. W ostatnich latach zaobserwować można zdecydowany wzrost działalności skierowanej przeciwko bezpieczeństwu sieci, systemów i urządzeń komputerowych lub cyfrowych. Po czasie nierzadko okazuje się, że za tymi najbardziej dotkliwymi najprawdopodobniej stoją zorganizowane grupy działające w ramach lub pozostające w ścisłym związku z państwowymi organizacjami wywiadowczymi. Mogą to być zależności finansowe, materiałowe, ideologiczne, polityczne, wojskowe lub inne. Niezależnie od podłoża związków, należy stwierdzić, że niosą one ze sobą implikacje niezbędne do rozpatrzenia w związku z kryminalistyczną analizą Internetu Rzeczy.

Działalność inspirowana lub sponsorowana przez państwa skierowana przeciwko innym państwom lub podmiotom prawa międzynarodowego bywa określana mianem działalności typu APT lub działalności APT. Jest to skrót od angielskiego rozwinięcia „*Advanced Persistent Threat*" i w samej nazwie zawiera definicję. Grupy APT, czyli prowadzące działalność typu APT, są sponsorowane lub inspirowane przez państwo. Podejmują działalność nieodbiegającą od szeroko rozumianej cyberprzestępczości, czy też incydentów naruszenia bezpieczeństwa komputerowego. Dokonują aktów cyberszpiegostwa, kradną informacje lub tajemnice państwowe, zakłócają pracę lub niszczą systemy informatyczne lub sieci. Cechami charakterystycznymi ich działań są trzy filary:

- **Zaawansowanie** (ang. *advancement* lub *advanced*) oznacza korzystanie z dopracowanych i zaawansowanych kodów lub oprogramowania, nierzadko stworzonego przez grupę lub w autorski sposób zmodyfikowanego na konkretne jej potrzeby. W wielu przypadkach, co wynika ze specyfiki działania grup, wykorzystywane przez nie arsenał jest przygotowywany każdorazowo pod konkretny cel lub ofiarę.
- **Długotrwałość** lub **trwałość** (ang. *persistence* lub *persistent*) przebywania w systemach lub sieciach ofiary, lub możliwość uzyskania dostępu do nich w dowolnym momencie, choćby poprzez zastosowanie oprogramowania typu backdoor. Długotrwałość przebywania w sieciach lub urządzeniach

przez sprawcę najczęściej bywa mierzona w miesiącach, aniżeli w dniach. Zablokowanie jednej z metod uzyskania dostępu lub kontroli nad urządzeniem ofiary niekoniecznie oznacza usunięcie intruzów z systemu.

- **Stwarzanie zagrożenia** (ang. *threat*) realnego i groźnego dla ofiary, zapewniającego lub wysoce uprawdopodobniającego odniesienie sukcesu przez atakującego. Połączone jest to z aspektem zaawansowania, gdyż tworzenie kontentych i przeznaczonych do specyficznego sposobu działania arsenału przekłada się na większe zagrożenie dla ofiary.[197]

Mimo, że niektórzy wskazują, że działalności typu APT nie należy utożsamiać jedynie z inspiracją lub sponsorowaniem przez państwo, to na ten moment jest to dominujący typ aktywności. Istotne jest jednak, aby brać pod uwagę możliwość zmiany tego trendu w przyszłości i nie zamykać tego pojęcia na tylko jeden, ściśle określony typ.

Działalność typu APT obserwowana jest już od kilku lat i z każdym rokiem zyskuje tak na dotkliwości, znaczeniu jak i intensywności. W raporcie dotyczącym aktywności za pierwszy kwartał 2020 r. wskazuje się na zaangażowanie grup rosyjsko- i chińskojęzycznych. Szczególnie w opisywanym czasie miało miały miejsce wyraźnie określone działania atrybuujące niektóre kampanie lub ataki przedstawicielom Rosji[198], Korei Północnej[199] oraz organizacji Hamas[200]. Ponadto, dla większości grup głównym motywem do działania są aspekty i relacje geopolityczne, dopiero w dalszej kolejności można zauważyć grupy operujące w celu odniesienia zysku finansowego. Działalność APT jest najbardziej aktywna w regionie Azji Południowo-Wschodniej, choćby podejmowanej przez znaną grupę Lazarus (najpewniej związaną z Koreą Północną). W kwestii *modus operandi* grupy dalej wykorzystują ogólnie znane podatności oprogramowania, coraz chętniej korzystają także z wariantów szkodliwego oprogramowania przeznaczonego na

---

197 https://web.archive.org/web/20180508161501/https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (dostęp 31.10.2020).

198 https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks (dostęp 31.10.2020).

199 https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack (dostęp 31.10.2020).

200 https://www.timesofisrael.com/idf-hamas-hacked-soldiers-phones-by-posing-as-pretty-girls/ (dostęp: 31.10.2020).

urządzenia mobilne, a także w swoich działaniach wykorzystują motywy związane z szalejącą pandemią COVID-19.[201] Na całym świecie funkcjonuje wiele różnorodnych grupy typu APT. Jedne koncentrują się na działalności ukierunkowanej na zdobywanie funduszy, z kolei inne podejmują działania o charakterze wywiadowczym lub sabotaże wszelkiego rodzaju. Różnorodność podejmowanych czynności oraz wykorzystywanego arsenału powoduje, ze stanowią i stanowić będą w przyszłości niewątpliwie coraz większe i poważniejsze zagrożenie.

W literaturze wskazuje się na zagrożenia wynikające z możliwości zastosowania podatności urządzeń Internetu Rzeczy przez grupy typu APT[202]. Wskazuje się wręcz, że w niektórych przypadkach takie zdarzenie miało już miejsce[203]. Opisywanym w literaturze przypadkom brakuje jednak, na ten moment, skali i dotkliwości porównywalnej do ataku na serwery Dyn z 2016 r. Pod kątem kryminalistycznej analizy możliwości Internetu Rzeczy niezwykle interesującym i znaczącym atakiem był ten skierowany na sieć energetyczną, w tym urządzenia typu SCADA, na Ukrainie. Zdarzenie miało miejsce w grudniu 2015 roku, a sprawcy wykorzystali między innymi szkodliwe oprogramowanie BlackEnergy[204]. Niewątpliwie spodziewać się można i należy oczekiwać wykorzystania funkcjonalności lub podatności Internetu Rzeczy do przeprowadzenia ataków przez grupy APT. Jest to metoda umożliwiająca na zwiększenie skali oraz dotkliwości ataku. O ile w tym drugim aspekcie jest to pożądana cecha incydentów wywoływanych prze grupy, o tyle zwiększenie skali może być aspektem deprymującym do korzystania dla sprawców. Jak to zostało wskazane wyżej, grupy APT obierają na cel konkretne ofiary. Z tego powodu raczej ograniczają skalę efektów swojego działania, chyba że jej rozszerzenie ma na celu obfuskację działań i utrudnienie pracy organom ścigania i służbom bezpieczeństwa.

Działalność typu APT jest zjawiskiem niezwykle groźnym i nie do końca rozpoznanym. W szczególności z punktu widzenia możliwości wykorzystania Internetu

---

[201] https://securelist.com/apt-trends-report-q1-2020/96826/ (dostęp 31.10.2020).

[202] X. Cheng, J. Zhang, B. Chen, *Cyber situation comprehension for IoT systems based on APT alerts and logs correlation*, „Sensors" 2019, t. 19(18), doi:10.3390/s19184045.

[203] P.J. Taylor, T. Dargahi, A. Dehghantanha, *Analysis of APT actors targeting IoT and big data systems: Shell_Crew, NetTraveler, ProjectSauron, CopyKittens, Volatile Cedar and Transparent Tribe as a case study*, w: A. Dehghantanha, K.K. Choo (red.), *Handbook of Big Data and IoT Security*, Springer, New York 2019, https://doi.org/10.1007/978-3-030-10543-3_11.

[204] https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01 (dostęp 3.02.2020).

Rzeczy w jej ramach. Niezależenie czy będzie to aktywność podejmowana przez grupy inspirowane przez państwa lub zorganizowane organizmy przestępcze, należy rozumieć i dostrzegać powagę zagrożenia. Zaniedbanie w tej kwestii może mieć katastrofalne skutki. Dotyczy to zarówno indywidualnego, jak i kolektywnego bezpieczeństwa, tak w wymiarze ogólnokrajowym, jak i międzynarodowym.

Rozdział 8. Wnioski i postulaty

Przedstawienie ogólnego stanu aktualnej wiedzy o zjawisku Internetu Rzeczy wobec kryminalistyki oraz w szerszym zakresie prawa karnego ze szczególnym uwzględnieniem aspektów teoretycznych oraz praktycznych w możliwie jak największym wymiarze jest niezwykle wartościowym z punktu widzenia nauk penalnych, w tym także kryminalistycznych. Pozwala na wskazanie najbardziej palących i nie do końca rozpoznanych jeszcze aspektów nowych metod popełniania i zapobiegania przestępczości. Przyjęte na wstępie założenia dotyczyły określenia ram, w granicach których rozważania byłyby podejmowane. Na podstawie wstępnie przyjętych ram oraz założeń, odnosząc się jednocześnie do wiedzy z zakresu nauk prawnych oraz informatycznych, możliwe było udzielenie odpowiedzi na podstawowe pytania powstające w wyniku rozważań odnośnie Internetu Rzeczy i związków tego zjawiska z kryminalistyką. W szczególności dotyczyły potencjału wykorzystania podatności lub funkcjonalności tego zjawiska do popełniania przestępstw. Niezbędnym było także omówienie podstaw technicznych w celu łatwiejszego zrozumienia sposobu i zasad działania tej koncepcji wraz z odniesieniem tego do funkcjonujących w doktrynie i praktyce kwestii zabezpieczania dowodów cyfrowych oraz sieciowych. Na podstawie przytoczonych w tym opracowaniu argumentów, przykładów i aspektów można z prawdopodobieństwem graniczącym z pewnością stwierdzić, że Internet Rzeczy nie jest dostatecznie opisany pod kątem kryminalistycznym, a także prawnym. Ma to w konsekwencji wpływ na potencjalne zagrożenia dla bezpieczeństwa państwa, jak i jego obywateli i mieszkańców. Potencjalnie zwiększa to ryzyka stania się przez nich ofiarami przestępstwa, a w razie jego zaistnienia nie daje gwarancji złapania przez organy ścigania sprawcy odpowiedzialnego za czyn. Składające się na to braki można rozpatrywać w dwóch sferach: **prawnej** oraz **kryminalistycznej**.

8.1 Sfera prawna

W kwestii wniosków i postulatów odnoszących się do aspektów prawnych Internetu Rzeczy i możliwości wykorzystania jego funkcjonalności lub podatności do popełniania przestępstw to część była przedstawiana w poszczególnych rozdziałach, ponieważ dotyczyła konkretnych przykładów i sytuacji. Z tego powodu zasadnym było

omówienie obok wspomnianych obserwacji. W ramach podsumowania należy zwrócić raczej uwagę na bardziej ogólne rekomendacje. Zwięzła synteza aktualnych przepisów dotyczących postepowania dowodowego pozwala na sformułowanie wniosków odnośnie tego aspektu postępowania karnego. Szczególnie w odniesieniu do kwestii dowodów cyfrowych i sieciowych, a więc ich specyfiki w stosunku do innego typu dowodów. Dotyczy to głównie ich gromadzenia i zabezpieczania na poczet postępowania przygotowawczego oraz sądowego, w sposób zapewniający ich poufność, integralność oraz autentyczność. W ten sposób nie powinno być wątpliwości, co do ich wartości dowodowej. Wnioski płynące z tej analizy pozwalają stwierdzić, że w obecnym stanie prawnym byłyby ogromne problemy w zakresie odpowiedniej interpretacji dowodów sieciowych. To one mają największe znaczenie odnośnie cyberprzestępczości związanej z rozwojem Internetu Rzeczy.

Na uwagę ponadto zasługuje ustawa o krajowym systemie cyberbezpieczeństwa[205] mający implementować założenia dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[206] do polskiego porządku prawnego. Nakłada ona konkretne obowiązki na podmioty: operatorów usług kluczowych oraz dostawców usług cyfrowych, wskazanych przez uprawnione do tego organy. Ponadto tworzy kręgosłup systemu zarządzania i monitorowania zagrożeń dla cyberbezpieczeństwa państwa w formie zespołów reagowania na incydenty bezpieczeństwa komputerowego. Wprowadza procedury dotyczące obsługi incydentów, współdziałania podmiotów i koordynacji całości tychże procesów. Na pełną ocenę w warstwie językowej oraz spodziewanej funkcjonalnej naturalnie trzeba będzie jeszcze poczekać do ostatecznego ukształtowania się treści projektu ustawy oraz finalnej wersji, która wejdzie w życie po jej uchwaleniu i opublikowaniu. Na podsumowanie i ocenę realizacji zadań oraz obowiązków z niej wynikających pod kątem *stricte* funkcjonalnym i z punktu widzenia bezpieczeństwa państwa poczekać trzeba będzie jeszcze dłużej.

Na gruncie przepisów UKSC w kontekście niebezpieczeństw wynikających z przestępczości wykorzystującej funkcjonalności lub podatności Internetu Rzeczy należy zwrócić uwagę na potencjalne problemy w sferze funkcjonalnej oraz w kwestii efektywności działań. Rzeczona ustawa wprowadza, jak to zostało wspomniane, podział

[205] T.j. Dz. U. z 2020 r., poz. 1369.
[206] Dz. Urz. UE L 194.

kompetencji w zakresie reagowania na incydenty bezpieczeństwa komputerowego pomiędzy trzy zespoły. Ich poszczególne zakresy odpowiedzialności są rozdzielone, więc w warstwie kompetencyjnej nie należy się spodziewać problemów. Przyjęto podejście zdekoncentrowane i podział kompetencji oraz zadań w warstwie operacyjno-technicznej pomiędzy trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego, czyli tak zwane CSIRTy: CSIRT, GOV, CSIRT NASK i CSIRT MON[207]. Zespoły te zajmują się koordynacją obsługi incydentów na poziomie krajowym i mają równorzędny status.

UKSC nie jest jednak dokumentem idealnym i wymagać będzie zmian w przyszłości. Niektóre przepisy oraz nakładane obowiązki mogą nie wytrzymać tak zwanej próby czasu lub mogą nie być możliwe do praktycznego wdrożenia. Jednak już w warstwie tekstowej można dostrzec pewne elementy, które mogłyby ulec poprawie już w tym momencie. Szczególnie rzucające się w oczy są aspekty lingwistyczne, zarówno w tłumaczeniu tytułu dokumentu, który jest implementowany przez UKSC oraz w treści samej ustawy. Jak zauważa się w doktrynie oryginalny zapis „*information systems*" został przetłumaczony na język polski jako „systemy informatyczny", zamiast istniejącego w polskim języku prawnym pojęcia „systemy informacyjne". To drugie określenie jest szersze znaczeniowo aniżeli pierwsze, co powoduje, że powstaje wątpliwość co do zasadności takiego, a nie innego tłumaczenia[208]. Podobne, wobec braku innego bardziej adekwatnego określenia, rozbieżności w przekładzie dostrzec można w tłumaczeniach na inne języki. W ich przypadku również, tak jak w polskim tłumaczeniu, wymienne są słowa „informacja" i „informatyka"[209]. W kwestii warstwy językowej samej ustawy należy się zastanowić nad zasadnością mieszania nazewnictwa polskiego i angielskiego, jak na przykład ma to miejsce w przypadku Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego. Wobec nich użyto skrót z języka angielskiego: CSIRT. Podkreślić należy, że oba pojęcia, zarówno długie (po polsku), jak i krótkie (po angielsku) występują w ustawie. Jest to pewna niekonsekwencja, choć na pewno nie w stopniu uniemożliwiającym lub wpływającym na stosowanie przepisów w praktyce. W tym wymiarze należy też wspomnieć, że skoro już przyjęta została koncepcja stosowania angielskojęzycznego skrótu, to powinno się stosować dany język konsekwentnie. Natomiast na gruncie przepisów UKSC łączy się angielski skrót CSIRT z polskimi

[207] K. Prusak-Górniak, K. Silicki, *Art. 26,* w: G. Szpor, A. Gryszczyńska, K. Czaplicki (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz,* Wolters Kluwer, Warszawa 2019.
[208] G. Szpor, *Wprowadzenie,* w: G. Szpor, A. Gryszczyńska, K. Czaplicki (red.), op. cit.
[209] Por. ibidem, przypis nr 12.

skrótami jak NASK (Naukowa Akademicka Sieć Komputerowa) czy MON (Ministerstwo Obrony Narodowej). Wskazane rozbieżności nie wpływają w sposób znaczący na praktyczne stosowanie ustawy, jednak mogą wpływać na odbiór tekstu.

Niewątpliwie wartym odnotowania aspektem problematycznym pozostającym na styku prawa karnego i innych gałęzi prawa jest problematyka związaną z danymi osobowymi. W tym w szczególności z obecnie implementowanym i wdrażanym Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, czyli tzw. ogólne rozporządzenie o ochronie danych, RODO (ang. *General Data Protection Regulation,* GDPR). Stale poszerzana ochrona danych osobowych i prawa do prywatności niesie ze sobą kolejne wyzwania dla badaczy i producentów urządzeń wykorzystujących funkcjonalności zjawiska Internetu Rzeczy. Implikuje to nie tylko poszerzanie horyzontów w kwestii zabezpieczeń systemów informatycznych przed atakiem, wtargnięciem, zmienianiem lub zakłócaniem działania, ale także dbałość o uniemożliwianie dostępu do informacji noszących cechy danych osobowych. Należy zwrócić uwagę na bezpieczeństwo systemów i sieci przetwarzających tego rodzaju informacje i podjęcie starań mających na celu zapewnienie przestrzegania zasad ścisłego bezpieczeństwa. Przykładowo poprzez niepodłączanie zbędnych urządzeń (z punktu widzenia prawidłowego funkcjonowania systemów i sieci) mających jednocześnie funkcjonalności komunikacji bezprzewodowej z innymi urządzeniami. Im mniej urządzeń połączonych dodatkowo, a niepotrzebnych z punktu widzenia prawidłowości funkcjonowania, tym mniejsza szansa na wykorzystanie podatności, ponieważ każde dodatkowe urządzenie dodaje potencjalnie kolejne wady i niedostatki w kwestii zabezpieczeń.

W odniesieniu do przestępczości wykorzystującej funkcjonalności lub podatności Internetu Rzeczy występują i będą dalej występować problemy natury prawnej na styku cyberbezpieczeństwa, prawa ochrony danych osobowych i bezpieczeństwa informacji oraz prawa karnego i kryminalistyki. Wraz z implementacją coraz większej liczby systemów informatycznych i informacyjnych do codziennego funkcjonowania, choćby administracji państwowej lub służby zdrowia, należy się spodziewać pogłębienia interdyscyplinarnych problemów. Wyzwaniem dla organów ścigania, wymiaru sprawiedliwości oraz państwowych, w tym władzy ustawodawczej i wykonawczej, będzie adekwatne

reagowanie na występujące nowe problemy wynikające z rozwoju nowych technik oraz technologii informatycznych.

8.2 Sfera kryminalistyczna

Pod względem kryminalistycznym brak jest naukowych badań oraz publikacji naukowych dotyczących zagadnień zwalczania cyberprzestępczości, analizowania dowodów pozostawianych w wyniku wykorzystania Internetu Rzeczy do popełniania przestępstw. Brak jest także wniosków i kierunków zwiększania bezpieczeństwa sieci i systemów informatycznych w związku z tym konkretnie zagrożeniem. Można to zaobserwować w wymiarze tak krajowym, jak i międzynarodowym. Obecne przepisy nie pozwalają na efektywne przeciwdziałanie i zapobieganie pełnemu spektrum zagrożeń wynikających z rozwoju Internetu Rzeczy. Robią to jedynie w sposób ograniczony i nierzadko na zasadzie analogicznego stosowania przepisów lub procedur. Walorem jest fakt, że w sferze prawnej pojawia się coraz więcej aktów i dokumentów dotyczących kwestii zabezpieczeń urządzeń i systemów informatycznych. Należy się spodziewać, że przełoży się to na większą świadomość społeczeństwa oraz organów ścigania i wymiaru sprawiedliwości. Być może będzie to stanowić przyczynek do stopniowego wprowadzania bardziej kompleksowych regulacji umożliwiających efektywne ściganie i zapobieganie cyberprzestępczości związanej z rozwojem Internetu Rzeczy.

Ponadto, podstawowym problemem jest także brak świadomości możliwych zagrożeń. Z tego niestety wynika także brak wiedzy do szukania i zabezpieczenia odpowiednich śladów. Powoduje to, że możliwe są błędy w prowadzonych postępowaniach, w których dużą bądź znaczącą rolę odgrywać będą dowody cyfrowe lub sieciowe, co przełoży się na ich wynik. Celem powinno być zapobieganie występowaniu sytuacji, w których w wyniku błędów lub braku wiedzy pojawiają się błędy w postępowaniu mające lub chociażby mogące mieć na wpływ na jego wynik.

W kwestii technicznego zabezpieczenia śladów cyfrowych należy stwierdzić, że obecnie funkcjonują odpowiednie procedury, zapewniające wiarygodność zabezpieczanego materiału i jego późniejszego wykorzystania przez organy śledcze i wymiaru sprawiedliwości. Ewentualnym problemem w przypadku dowodów sieciowych jest ich ulotność oraz odpowiednia analiza ich znaczenia. W tej kwestii niewątpliwie

istotnym jest aspekt wyszkolenia specjalistów od zabezpieczania materiału dowodowego. W przypadku urządzeń i przedmiotów wchodzących w skład Internetu Rzeczy problematyczną kwestią jest w jaki sposób w ogóle je zabezpieczyć. Budowa oraz sposób działania, a w szczególności liczby dokonywanych procesów, w mniejszym lub większym stopniu odbiegają od tych komputerowych. Należy jednak stwierdzić, że nawet jeśli tylko w minimalnym stopniu, to funkcjonują w społeczeństwie osoby dysponujące wiedzą adekwatną do wiernego i wiarygodnego zabezpieczenia dowodów cyfrowych oraz także dowodów sieciowych. Wadą może być niewystarczająca liczba takich osób, dysponujących wiedzą umożliwiającą identyfikację problemów związanych z rozwojem nowych technologii w kontekście zwalczania przestępczości. Odpowiednia praca nad tym w postaci regularnych badań stanu wiedzy, naukowych badań poświęconych cyberprzestępczości i jej nowym aspektom jest w stanie osiągnąć pozytywne rezultaty w postaci bardziej efektywnego prowadzenia działań na miejscu zdarzenia. Podobnie szkolenia prowadzone dla techników kryminalistyki oraz wszystkich funkcjonariuszy Policji przez specjalistów i osoby dysponujące wiedzą specjalistyczną wpłyną pozytywnie na stopień bezpieczeństwa sieci i systemów informatycznych, a także efektywności działań prowadzonych w postępowaniu przygotowawczym. W kwestii zabezpieczeń technicznych pozytywną informacją są o opracowywanym reaktywnym środku reagowania na zagrożenia związane z nieprawidłowym zabezpieczeniem urządzeń i przedmiotów podłączonych do Internetu. Badacze A. Cui i J. Pantoga zajęli się opracowywaniem zautomatyzowanej strategii identyfikowania problemów i braków w zabezpieczeniach. Mimo faktu, iż dotyczy to raczej problemów już znanych, ale jeszcze nieodkrytych w różnego typu urządzeniach, to należy przyjąć tego typu badania z optymizmem i nadzieją, że z biegiem czasu wprowadzone będą jeszcze bardziej zaawansowane rozwiązania umożliwiające zwalczanie błędów zanim zostaną odkryte i wykorzystane[210].

8.3 Uwagi końcowe

Tematyka możliwości wykorzystania funkcjonalności lub podatności Internetu Rzeczy do popełniania przestępstw jest niewątpliwie kwestią nową i nie do końca zbadaną.

[210] L.H. Newman, *A new way to track down bugs could help save IoT*, WIRED, https://www.wired.com/story/a-new-way-to-track-down-bugs-could-help-save-iot/ (dostęp 10.01.2018).

Świadczy o tym szczątkowa wręcz liczba dostępnych opracowań naukowych w języku angielskim. Braki w rozpoznaniu potencjału Internetu Rzeczy w sferze kryminalistycznej oraz w sferze prawnej, ze szczególnym uwzględnieniem prawa karnego, jako ściśle i nierozerwalnie związanego z kryminalistyką, są przez to uwypuklone. Rozważania poruszone mają na celu zasygnalizowanie jak istotnym w przyszłości problemem może być przestępczość wykorzystująca koncepcję Internetu Rzeczy do swoich korzyści. Zaletą wszystkich powyższych rozważań jest uniwersalność wniosków z nich płynących, możliwych jednocześnie do wykorzystania przez teoretyków, jak i praktyków w wielu gałęziach nauk prawnych. Kontekst bezpieczeństwa urządzeń, sieci i systemów informatycznych oraz sieciowych jest wspólny dla Internetu Rzeczy, niezależnie od gałęzi prawa w ramach której zjawisko to jest wykorzystywane lub analizowane. Wnioski płynące z przedstawionych studiów przypadków, a także rekomendacje i teorie zaprezentowane w pracy pozwolą na sformułowanie tez mogących mieć wpływ na całokształt regulacji prawnych, nie tylko w warstwie prawa karnego.

Przedstawione poglądy, choć o nasuwającej się raczej negatywnej konotacji przywodzące na myśl kasandryczne wizje rozwoju cyberprzestępczości, mają na celu przede wszystkim jedno. Wskazują na zagrożenia wynikające z rozwoju Internetu Rzeczy w celu budowania świadomości jak najszerszego grona teoretyków i praktyków nauk prawnych, w tym organów ścigania i wymiaru sprawiedliwości, a także szerzej – społeczeństwa. Zaprezentowane informacje nie powinny wywoływać jedynie złych skojarzeń lub spowodować ograniczenia rozwoju tej koncepcji. Wręcz przeciwnie - kwestie bezpieczeństwa i wskazywania błędów oraz luk powinny stymulować dalszy rozwój nowoczesnych technologii, wzbogacony jedynie o dbałość w zapewnieniu bezpieczeństwa użytkownikom nowych urządzeń. Zwracanie uwagi na zagwarantowanie adekwatnego poziomu zabezpieczeń w warstwie technicznej, jak i programistycznej powinny być wspólnym celem tak producentów, organów władzy, jak i badaczy oraz naukowców. Współpraca, między innymi polegająca na wskazywaniu błędów, braków w regulacjach prawnych i procedurach, a także zabezpieczeń technicznym, jest niezwykle istotnym elementem i powinna być pogłębiana, kiedy i jak tylko się da. Jednak najważniejszym wnioskiem powinno być stwierdzenie, że choć rozwój nowych technologii jest nieunikniony i potrzebny, to nie należy zapominać o tak podstawowych kwestiach jak zapewnienie bezpieczeństwa bez naruszania i wkraczania w sferę praw oraz wolności jednostki. W dobie dynamicznego rozwoju techniki, Internetu i komunikacji

bezprzewodowej dbałość o prawa i wolności leżą po stornie każdego z nas, niezależnie od roli w społeczeństwie. Sprzyjać temu zdecydowanie będzie większa świadomość społeczna odnośnie zagrożeń, a także potencjalnych rozwiązań w razie wystąpienia problemu oraz efektywność pracy organów władzy publicznej, ścigania i wymiaru sprawiedliwości w neutralizacji niebezpieczeństw.

Bibliografia

Literatura

Abomhara M., Køien G.M., *Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks*, „Journal of Cyber Security and Mobility" 2015, t. 4(1).

Adams R.B., *The Advanced Data Acquisition Model (ADAM): a Process Model for Digital Forensic Practice*, Murdoch University 2012.

Adamski A., *Europejskie standardy prawnokarnej ochrony sieci i informacji oraz ich implementacja do ustawodawstwa polskiego,* w: G. Szpor, A. Gryszczyńska (red.), *Internet. Strategie bezpieczeństwa*, C.H. Beck, Warszawa 2017.

Adamski A., *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000.

Agarwal A., Gupta M., Gupta S., Gupta S.C., *Systematic digital forensic investigation model*, „International Journal of Computer Science and Security" 2011, t. 5(1).

Ashton K., *That 'Internet of Things' thing*, „RFID Journal", 22.09.2009.

Atlam H.F., Wills G.B., Alenezi A., Alassafi M.O., *Blockchain with Internet of Things: Benefits, challenges, and future directions*, „International Journal of Intelligent Systems and Applications" 2018, t. 10, nr 6.

Ayala L., *Cybersecurity Lexicon*, Apress, New York 2016.

Ball J., *Guardian launches SecureDrop system for whistleblowers to share files*, „The Guardian", 05.06.2014.

Beardsley T., Stanislav M., *Hacking IoT: a Case Study on Baby Monitor Exposures and Vulnerabilities*, Rapid7, 2015.

Blythe J.M., Sombatruang N., Johnson S.D., *What security features and crime prevention advice is communicated in consumer IoT device manuals and support pages?*, „Journal of Cybersecurity" 2019, t. 5(1), https://doi.org/10.1093/cybsec/tyz005.

Bonderud D., *Leaked Mirai Malware Boosts IoT Insecurity Threat Level*, Security Intelligence, 04.10.2016, https://securityintelligence.com/news/leaked-mirai-malware-boosts-iot-insecurity-threat-level/ (dostęp 01.10.2019).

Brachman A., *Internet przedmiotów – Raport*, Obserwatorium ICT, Technopark Gliwice 2013.

Bryant R., Bryant S., *Policing Digital Crime*, Ashgate, Farnham 2014.

Casey E., *Trust in digital evidence*, „Digital Investigation" 2019, t. 31, https://doi.org/10.1016/j.fsidi.2019.200898.

Cheng X., Zhang J., Chen B., *Cyber situation comprehension for IoT Systems based on APT alerts and logs correlation*, „Sensors" 2019, t. 19(18), doi:10.3390/s19184045.

Czarnecka M., *Inteligentne opomiarowanie energii elektrycznej a prawa konsumentów*, w: G. Szpor (red.), *Internet Rzeczy. Bezpieczeństwo w Smart city*, C.H. Beck, Warszawa 2015.

De Falco M., *Stuxnet Facts Report, a Technical and Strategic Analysis*, NATO Cooperative Cyber Defence Centre of Excellence, 2012.

Digital Forensic Research Workshop, *Road Map for Digital Forensic Research*, New York 2001.

Dinniss H.H., *Cyber Warfare and the Laws of War*, Cambridge University Press, New York 2012.

Eichstaedt K., *Art. 218(b)*, w: D. Świecki (red.), *Kodeks postępowania karnego. Tom I. Komentarz aktualizowany*, LEX/el. 2018.

Gardocka T., *Zasady postępowania dowodowego w polskim procesie karnym*, w: T. Gardocka, D. Jagiełło (red. nauk.), *Zagadnienie dowodowe w procesie karnym*, C.H. Beck, Warszawa 2017.

Garrison L., Grand M., *Cyberterrorism: An evolving concept*, US National Infrastructure Protection Centre 2001.

Gibbs S., Beckett L., *Dark web marketplaces AlphaBay and Hansa shut down*, „The Guardian", 20.07.2017.

Goodin D., *First known hacker-caused power outage signals troubling escalation*, Ars Technica, 04.01.2016.

Goodin D., *Smart TV hack embeds attack code into broadcast signal – no access required*, Ars Technica, 31.03.2017.

Góralczyk W., Sawicki S., *Prawo międzynarodowe publiczne w zarysie*, Wolters Kluwer, Warszawa 2017.

Górnisiewicz M., Obczyński R., Pstruś M., *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa związane z bankowością elektroniczną*, Komisja Nadzoru Finansowego, Warszawa 2014.

Gradoń K., *Countering lone actor terrorism – preliminary findings of the PRIME project*, „Problemy Współczesnej Kryminalistyki" 2016, t. XX.

Greenberg A., *Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains*, WIRED, 07.11.2014.

Greenberg A., *Hacker Lexicon: What is the Dark Web?*, WIRED, 19.11.2014.

Greenberg A., *Hackers cut a Corvette's brakes via a common car gadget*, WIRED, 11.08.2015.

Greenberg A., *Hackers remotely kill a jeep on the highway – with me in it*, WIRED, 21.07.2015.

Griffin A., *Facebook, Twitter and Google are 'the lifeblood of Daesh', according to major new report into ISIS use of social media*, „Independent", 25.08.2016.

Gruza E., Goc M., Moszczyński J., *Kryminalistyka – czyli rzecz o metodach śledczych*, Oficyna Wydawnicza Łośgraf, Warszawa 2011.

Guidelines on Digital Forensic Procedures for OLAF Staff, 15.02.2016.

Hambridge S., Lunde A., *DON'T SPEW. A Set of Guidelines for Mass Unsolicited Mailings and Postings*, The Internet Society, 1999.

Hanausek T., *Kryminalistyka: zarys wykładu*, Oficyna a Wolters Kluwer business, Warszawa 2009.

Harvey D., *How Islamic State extremists use social media to recruit*, BBC, 23.02.2015.

Higginbotham S., *The elephant in the room for IoT security*, Stacey on IoT Blog, 18.04.2017.

Hilton S., *Dyn Analysis Summary Of Friday October 21 Attack*, Dyn, 2016.

Horoszowski P., *Kryminalistyka*, Państwowe Wydawnictwo Naukowe, Warszawa 1958.

Horoszowski P., *Nazwa i pojęcie „dowodu" w teorii i praktyce prawa sądowego*, „Państwo i Prawo" 1956, nr 10.

Imran A., *Cyber-extremism: Isis and the power of social media*, „Social Science and Public Policy" 2017, t. 54(2).

Indecki K., *Prawo karne wobec terroryzmu i aktu terrorystycznego*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 1998.

Internet Security Threat Report, Volume 24, Broadcom, luty 2019.

Iszkowski W., *Internet of Things. Systemy wbudowane*, w: G. Szpor (red.), *Internet Rzeczy. Bezpieczeństwo w Smart city*, C.H. Beck, Warszawa 2015.

Karasek P., *Dowód cyfrowy – aspekty kryminalistyczne*, praca mgr niepublikowana, obroniona na Uniwersytecie Warszawskim, Warszawa 2014.

Kasprzak W., *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Difin, Warszawa 2015.

Kebande V.R., Ray I., *A generic digital forensic investigation framework for Internet of Things (IoT)*, Proceedings of 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016.

Kohn M., Eloff J.H.P., Olivier M.S., *Framework for a digital forensic investigation*, Information and Computer Security Architectures Research Group (ICSA), Department of Computer Science, University of Pretoria, 01.2006.

Kosiński J., *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015.

Krasniqi X., Hajrizi E., *Use of IoT Technology to drive the automotive industry from connected to full autonomous vehicles*, „IFAC-PapersOnLine" 2016, t. 49(29).

Lach A., *Art. 269(a)*, w: V. Konarska-Wrzosek (red.), *Kodeks karny. Komentarz*, Wolters Kluwer, Warszawa 2016.

Lach A., *Dowody elektroniczne w postępowaniu karnym*, Towarzystwo Naukowe Organizacji i Kierownictwa, Toruń 2004.

Lomas N., *Dyn DNS DDoS likely the work of script kiddies, says Flashpoint*, Techcrunch, 26.10.2016.

Lone A.H., Mir R.N., *Forensic-chain: Ethereum blockchain based digital forensics*, „Scientific and Practical Cyber Security Journal" 2017, t. 1–2.

Longman Dictionary of Contemporary English, Pearson.

Measuring the Information Society Report 2015, International Telecommunication Union, 2015.

Mukasey M.B., Sedgwick J.L., Hagy D.W., *Electronic Crime Scene Investigation: A Guide for First Responders*, U.S. Department of Justice, Office of Justice Programs, Washington 2008.

National Institute of Justice, *Results from Tools and Technology Working Group*, Governors Summit on Cybercrime and Cyberterrorism, Princeton 2002.

Newman L.H., *A new way to track down bugs could help save IoT*, WIRED, 18.01.2018.

Olbrycht J., *Idea smart city*, w: G. Szpor (red.), *Internet Rzeczy. Bezpieczeństwo w Smart city*, C.H. Beck, Warszawa 2015.

Oriwoh E., Jazani D., Epiphaniou G., Sant P., *Internet of Things forensics: Challenges and approaches*, The 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013.

Polityuk P., *Ukraine to probe suspected Russian cyber attack on grid*, Reuters, 31.12.2015.

Pollitt M.M., *Cyberterrorism – fact or fancy?*, „Computer Fraud & Security" 1998, t. 1998(2).

Raport Internet Rzeczy w Polsce, IAB Polska, 2015.

Reith M., Carr C., Gunsch G., *An examination of digital forensic models*, „International Journal of Digital Evidence" 2002, t. 1(3).

Rose S., *The Isis propaganda war: A hi-tech media jihad*, „The Guardian", 07.10.2014.

Sandberg-Diment E., *The executive computer*, „The New York Times", 8.12.1985.

Security Flaws in Universal Plug and Play, Rapid 7 White Paper, 01.2013.

Silicki K., *Co wynika z dyrektywy NIS?*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna 2016*, Wyższa Szkoła Policji w Szczytnie, Szczytno 2017.

Skorupka J., *Sprawiedliwość proceduralna jako cel procesu karnego*, w: J. Skorupka (red.), *Rzetelny proces karny. Księga jubileuszowa Profesor Zofii Świdy*, Wolters Kluwer, Warszawa 2009.

Słowiński P., *Nowe metody popełniania przestępstw na przykładzie rozwoju Internetu Rzeczy*, „Problemy Współczesnej Kryminalistyki" 2016, t. XX.

Stavroulakis P., Stamp M., *Handbook of Information and Communication Security*, Heidelberg–New York, Springer 2010.

Stefański R.A., Zabłocki S., *Art. 218(b)*, w: R.A. Stefański, S. Zabłocki, *Kodeks postępowania karnego. Tom II. Komentarz do art. 167–296*, Wolters Kluwer Polska, Warszawa 2018.

Stoyanova M., Nikoloudakis Y., Panagiotakis S., Pallis E., Markakis E.K., *A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues*, „IEEE Communications Surveys & Tutorials" 2020, t. 22, nr 2.

Tarnogórski R., *Prawo konfliktów zbrojnych a cyberprzestrzeń*, „Biuletyn Polskiego Instytutu Spraw Międzynarodowych" 2013, nr 31(1007).

Skowron A., *Rzetelny proces karny w ujęciu Karty Praw Podstawowych Unii Europejskiej oraz Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, „Prokuratura i Prawo" 2017, nr 11.

Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Oficyna a Wolters Kluwer business, Warszawa 2010.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, Cambridge–New York 2017.

Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, Cambridge–New York 2013.

Taylor P.J., Dargahi T., Dehghantanha A., *Analysis of APT actors targeting IoT and big data systems: Shell_Crew, NetTraveler, ProjectSauron, CopyKittens, Volatile Cedar and Transparent Tribe as a case study*, w: A. Dehghantanha, K.K. Choo (red.), *Handbook of Big Data and IoT Security*, Springer, New York 2019, https://doi.org/10.1007/978-3-030-10543-3_11.

Turing A.M., *On computable numbers, with an application to the Entscheidungsproblem*, „Proceedings of the London Mathematical Society" 1937.

US Food and Drug Administration, *FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework*, 2014.

Waltoś S., Hofmański P., *Proces karny. Zarys systemu*, Wolters Kluwer, Warszawa 2016.

Wang K., Du M., Sun Y., Vinel A., Zhang Y., *Attack detection and distributed forensics in machine-to-machine networks*, „IEEE Network" 2016, t. 30(6).

Williams J., *ACPO Good Practice Guide for Digital Evidence*, Association of Chief Police Officers, marzec 2012.

Woodward A., Williams P., *Cybersecurity vulnerabilities in medical devices: A complex environment and multifaceted problem*, „Medical Devices: Evidence and Research" 2015, t. 8.

Zawoad S., Dutta A.K., Hasan R., *SecLaaS: Secure logging-as-a-service for cloud forensics*, Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, 2013.

Zawoad S., Hasan R., *FAIoT: Towards building a forensics aware eco system for the Internet of Things*, Proceedings of The 12th IEEE International Conference on Services Computing (SCC 2015), 2015.

Zetter K., *An unprecedented look at Stuxnet, the world's first digital weapon*, WIRED, 03.11.2014.

Zetter K., *Hacker can send fatal dose to hospital drug pumps*, WIRED, 08.06.2015.

Zillner T., *ZigBee Exploited, The good, the bad and the ugly*, Cognosec 2015.

Źródła prawa

Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194).

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 24.04.2011 r. „Inteligentne sieci energetyczne: od innowacji do wdrożenia", COM/2011/0202 wersja ostateczna.

Komunikat Komisji Europa 2020. Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu, COM/2010/2020 końcowy.

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa 2013.

Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych (Dz. U. Nr 100, poz. 1023).

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2020 r., poz. 1369).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz. U. z 2019 r., poz. 796).

Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2016 r., poz. 1489, 1579, 1823, 1948, 1954 i 2003).

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2020 r., poz. 346 z późn. zm.).

Ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. Nr 69, poz. 626).

Ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344).

Ustawa z dnia 4 września 2008 r. o zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. Nr 171, poz. 1056).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j. Dz. U. z 2020 r., poz. 1444).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz. U. z 2020 r., poz. 30 z późn. zm.).

Źródła internetowe

http://419scam.org

http://download.nai.com/Products/mcafee-avert/whitepapers/akapoor_rootkits1.pdf

http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267

http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267

http://www.um.warszawa.pl/aktualnosci/rozwi-zania-smart-city-musz-zintegrowane

https://ccdcoe.org/cyber-definitions.html

https://ccdcoe.org/research/tallinn-manual/

https://cyberpolicy.nask.pl/cp/inicjatywy/unia-europejska/csirt-network/71,Siec-CSIRT-CSIRT-network.html

https://en.wikipedia.org/wiki/Backdoor_(computing)

https://en.wikipedia.org/wiki/Bluetoot

https://en.wikipedia.org/wiki/Computer_virus

https://en.wikipedia.org/wiki/Computer_worm

https://en.wikipedia.org/wiki/Electronic_control_unit

https://en.wikipedia.org/wiki/Fork_bomb

https://en.wikipedia.org/wiki/Remote_desktop_software

https://en.wikipedia.org/wiki/SOAP

https://en.wikipedia.org/wiki/Trojan_horse_(computing)

https://en.wikipedia.org/wiki/Universal_Plug_and_Play

https://en.wikipedia.org/wiki/Wi-Fi

https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016L1148

https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf

https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/

https://krebsonsecurity.com/2018/09/alleged-satori-iot-botnet-operator-sought-media-spotlight-got-indicted/

https://krebsonsecurity.com/2018/09/mirai-botnet-authors-avoid-jail-time/

https://krebsonsecurity.com/2019/09/satori-iot-botnet-operator-pleads-guilty/

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

https://pl.wikipedia.org/wiki/Script_kiddie

https://plblog.kaspersky.com/botnet/6302/

https://plblog.kaspersky.com/co-to-sa-exploity-i-dlaczego-sa-zle/3409/

https://pomoc.nazwa.pl/baza-wiedzy/produkty-i-uslugi/domeny/o-domenach-bardziej-technicznie/co-to-jest-dns/

https://securelist.com/apt-trends-report-q1-2020/96826/

https://sjp.pwn.pl/sjp/informatyka;2561527.html

https://usa.kaspersky.com/resource-center/threats/ransomware.

https://web.archive.org/web/20180508161501/https://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf

https://www.adaware.com/knowledge-database/spyware-glossary#Adware

https://www.avast.com/c-browser-hijacker.

https://www.computerhope.com/jargon/e/ecu.htm

https://www.cyber.nj.gov/threat-center/threat-profiles/botnet-variants/satori

https://www.economist.com/science-and-technology/2016/10/08/the-internet-of-stings

https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/410117/Internet_of_things_-_FINAL.pdf

https://www.ic3.gov/media/2015/150910.aspx

https://www.ic3.gov/Media/Y2016/PSA160317

https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

https://www.justice.gov/opa/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases-involving

https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack

https://www.pcmag.com/encyclopedia/term/41069/deep-web

https://www.pentestpartners.com/security-blog/hacking-defcon-23s-iot-village-samsung-fridge/

https://www.rpo.gov.pl/pl/content/RPO-skarzy-ustawe-antyterrorystyczna-do-TK

https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/scams-spam-to-avoid-facebook-12-en.pdf

https://www.techopedia.com/definition/15653/deep-web

https://www.timesofisrael.com/idf-hamas-hacked-soldiers-phones-by-posing-as-pretty-girls/

https://www.torproject.org/about/overview.html.en#overview

https://www.torproject.org/about/torusers.html.en

https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

https://www.us-cert.gov/ncas/tips/ST04-015