Piotr Słowiński

INTERNET RZECZY JAKO NOWY ASPEKT CYBERPRZESTĘPCZOŚCI – PRZEGLĄD DEFINICJI I SYSTEMATYKI

The Internet of Things as a new aspect of cybercrime – an overview of definitions and systematics

We współczesnym świecie szeroko pojęta cyberprzestrzeń coraz częściej i śmielej wkracza do codziennego życia każdego człowieka. Z cyberprzestrzenią natomiast nierozerwalnie związane jest pojęcie cyberprzestępczości. Cyberprzestępczość jest stosunkowo nowym aspektem przestępczości. Choć początków koncepcji działania współczesnych komputerów można szukać już w latach 30. XX wieku, konkretnie w pracy A. Turinga napisanej w 1936 r.[1], to dla indywidualnego odbiorcy wszechobecność komputerów i urządzeń jest zjawiskiem stosunkowo nowym. Nie zagłębiając się w historię i rozwój komputerów oraz informatyzacji, należy zaznaczyć, że postępowała ona z każdym rokiem coraz intensywniej. Jednak dopiero ostatnie lata przyniosły nieporównywalnie większy niż we wcześniejszych latach postęp w rozwoju technologicznym i liczbie urządzeń elektronicznych. Wraz ze wzrostem liczebności i typów tychże urządzeń zwiększyło się spektrum ich możliwości i wypełnianych przez nie funkcji. Między innymi rozwój telefonii komórkowej okazuje się jednym z kamieni milowych dla rozwoju technologicznego. Przy względnie niewielkiej masie i wielkości telefonów komórkowych urządzenia te są wyposażone w ogromne możliwości techniczne w postaci przykładowo mocy obliczeniowej. Rosnąca liczba aplikacji mobilnych, a także oprogramowania, tylko zwiększa spektrum możliwości urządzeń, które prawie każdy z nas miał w kieszeni. To, a także rozwój technologiczny sprzętu komputerowego oraz sieciowego w postaci sieci Internet i infrastruktury przesyłowej, stanowi podstawę dla ustawodawców, zarówno krajowych, jak i europejskich czy międzynarodowych, do stanowienia i nowelizowania prawa. Wobec ogromu zmian technologicznych i gwałtownego rozwoju nowych technologii niektóre zjawi-

[1] 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 r.].

ska pozostają nieznane lub niedostatecznie opisane w literaturze kryminalistycznej. Jedną z niezwykle gwałtownie rozwijających się koncepcji jest Internet Rzeczy.

Internet Rzeczy (ang. *Internet of Things*, w skrócie IR) w rozumieniu kryminalistycznym 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. Występuje ona w postaci jednej wielkiej sieci powiązanych wzajemnie obiektów, komunikujących się ze sobą, wymieniających i zbierających dane[2]. Należy dodać, że niezwykle istotnym elementem funkcjonowania tej koncepcji jest to, iż komunikacja, zbieranie danych i wymienianie się nimi następuje najczęściej bez wiedzy i zgody użytkownika lub po jednej uprzedniej zgodzie wyrażonej na początku używania urządzenia. Niewłaściwemu rozumieniu tej koncepcji oraz zagrożeń z niej wynikających nie sprzyja również brak jednolitego nazewnictwa w polskojęzycznych publikacjach. W literaturze polskojęzycznej używane są głównie trzy określenia: Internet rzeczy, Internet przedmiotów oraz angielska nazwa Internet of Things. O koncepcji Internetu Rzeczy wspomina również dr hab. inż. Jerzy Kosiński, wskazując na następujące zagrożenia: braki aktualizacji lub błędy w oprogramowaniu mogą zagrażać bezpośrednio użytkownikowi (życiu i zdrowiu na przykładzie inteligentnego samochodu), albo narazić byłego użytkownika inteligentnego urządzenia na utratę poufnych danych lub pozwolić na jego sprofilowanie (w razie sprzedaży inteligentnego urządzenia)[3]. Urządzenia codziennego użytku zostają wyposażone w oprogramowanie umożliwiające wysyłanie do nich wiadomości oraz uruchamianie aplikacji, czyli funkcji zarezerwowanych do tej pory dla zupełnie innego typu urządzeń, np. komputerów. Dr inż. W. Iszkowski definiuje zjawisko Internetu przedmiotów (autor używa tego określenia zamiast nazwy „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] P. Słowiński, *Nowe metody popełniania przestępstw na przykładzie rozwoju Internetu Rzeczy*, „Problemy Współczesnej Kryminalistyki" 2016, t. XX.

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

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 w pobliżu.
7. Przepisy prawne nigdy nie zabezpieczą w pełni osób i społeczeństwa przed nieuprawnionym, szkodliwym wykorzystaniem Internetu przedmiotów przeciwko nim.
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[4].

Obiekty mogące być szeroko pojętą częścią składową zjawiska Internetu Rzeczy są niezwykle różnorodne – do tego stopnia, że nie sposób je zaklasyfikować w jedną ścisłą grupę. Można je jedynie ogólnie określić jako „przedmioty codziennego użytku" bądź jeszcze bardziej ogólnie, choć konkretnie, zważywszy na ich funkcję: „przedmioty, których używamy". Ludzie nie zdają sobie sprawy, że tak naprawdę obecny kierunek rozwoju powoduje, iż w funkcję bezprzewodowego łączenia się z Internetem bywają wyposażone takie przedmioty jak lodówki, zabawki, bramy garażowe, samochody oraz wiele innych podobnych. Co ważne, obiekty te łączą się ze sobą np. przez jedno konto, uzyskują dostęp do innych urządzeń powiązanych z tym kontem lub po prostu połączonych z tym samym modemem Wi-Fi. Oprócz problemów dotyczących indywidualnych użytkowników urządzeń istnieją o wiele poważniejsze zagrożenia, o których nie sposób zapomnieć. Internet Rzeczy to nie tylko urządzenia

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

codziennego użytku wyposażone w moduły bądź komponenty umożliwiające podłączenie do Internetu, gromadzące dane i wymieniające się nimi, często bez wiedzy człowieka. To także systemy SCADA (ang. *Supervisory Control And Data Acquisition*), czyli systemy elektroniczne wykorzystywane w zarządzaniu miastem oraz infrastrukturą krytyczną. Przykładowo systemy tego typu można wykorzystać, aby kontrolować ciśnienie na zaworach w miejskim przedsiębiorstwie wodociągowym czy też monitorować przepływ prądu w miejskiej elektrowni[5].

Jak wynika z powyższej analizy, mnogość przedmiotów, urządzeń i komponentów mogących wchodzić w skład Internetu Rzeczy wymaga odpowiedniej uwagi ze strony zarówno producentów, jak i konsumentów, ale także prawników, organów ścigania i naukowców. Krótka, jednak coraz bardziej dynamiczna historia rozwoju powoduje, że należy zwrócić uwagę na możliwe niebezpieczeństwa związane ze zjawiskiem Internetu Rzeczy. Zaniedbanie tego obowiązku, jaki powstaje po stronie wymienionych powyżej podmiotów, może mieć katastrofalne skutki dla każdego z nas. Rozważania dotyczące umiejscowienia omawianego zjawiska w metodologii badań nad problematyką cyberprzestępczości należy zacząć od przytoczenia wybranych definicji cyberprzestępczości z różnych aktów prawnych i dokumentów:

1. Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.[6] wraz z Protokołem dodatkowym do Konwencji Rady Europy o cyberprzestępczości dotyczącym penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzonym w Strasbourgu w dniu 28 stycznia 2003 r.[7]
2. Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 22 maja 2007 r. – w kierunku ogólnej strategii zwalczania cyberprzestępczości[8].
3. 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[9].

---

5 Więcej przykładów i historii zjawiska Internetu Rzeczy zob. P. Słowiński, *Nowe metody*…, op. cit.

6 Dz.U. z 2015 r., poz. 728.

7 Dz.U. z 2015 r., poz. 730.

8 http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267 [dostęp: 26.09. 2019 r.].

9 doc. JOIN (2013)1.

4. Definicje zebrane na stronie NATO Cooperative Cyber Defence Centre of Excellence[10].
5. Definicja Interpolu[11].

Konwencja Rady Europy o cyberprzestępczości (dalej jako „Cyberkonwencja") definiuje cyberprzestępczość przez wyróżnienie następujących rodzajów przestępstw:

- przeciwko poufności, integralności i dostępności danych i systemów informatycznych,
- komputerowe – fałszerstwa i oszustwa komputerowe,
- ze względu na charakter zawartych informacji,
- związane z naruszaniem praw autorskich i pokrewnych.

Komunikat Komisji z 22 maja 2007 r. również definiuje cyberprzestępczość w postaci wyliczenia rodzajów przestępstw i wyróżnia następujące:

- tradycyjne formy przestępstw z użyciem elektronicznych sieci informatycznych i systemów informatycznych,
- publikacja nielegalnych treści w mediach elektronicznych (np. materiałów o charakterze pedofilskim czy zawierających treści na tle nienawiści rasowej),
- przestępstwa typowe dla sieci łączności elektronicznej, tj. ataki przeciwko systemom informatycznym, ataki typu DoS (ang. *Denial of Service*) czy hakerstwo[12].

Komunikat Komisji z 7 lutego 2013 r. wskazuje strategiczne priorytety i działania Unii Europejskiej w celu zapewnienia bezpiecznego i swobodnego korzystania ze środowiska internetowego. Komunikat ten ma na celu wytyczenie długo- i krótkoterminowych kierunków działania wielu podmiotów, nie tylko instytucji UE, lecz także państw członkowskich i przedstawicieli branży, a więc podmiotów prywatnych. W tekście wymienionych jest 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,

[10] https://ccdcoe.org/cyber-definitions.html [dostęp: 03.01.2013 r.].
[11] https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime [dostęp: 26.09.2019 r.].
[12] http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267 [dostęp: 26.09. 2019 r.].

- rozbudowa zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego,
- ustanowienie spójnej międzynarodowej polityki w zakresie cyberprzestrzeni dla Unii Europejskiej i promowanie podstawowych wartości UE[13].

Dokument rozwija każdy z przedstawionych wyżej priorytetów, wskazując konkretne działania, powołane bądź planowane do powołania instytucje, przyjęte bądź planowane dokumenty, a także formułuje wnioski *de lege ferenda*. Spośród nich należy przywołać przewidziane przepisami dyrektywy powołanie w krajach członkowskich organów, których zadaniem byłoby skoordynowanie działań na obszarze jej działania w dziedzinie bezpieczeństwa sieci i informacji, opisanych w dyrektywie 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[14], nazywanej w skrócie dyrektywą NIS. Ponadto ich celem byłoby koordynowanie wdrażania postanowień dyrektywy. Dodatkowo ma być powołany organ mający pełnić funkcję punktu kontaktowego w zakresie komunikacji międzynarodowej oraz krajowego punktu kontaktowego w dziedzinie dyrektywy NIS albo można tę funkcję przypisać instytucji już istniejącej. W swoim zakresie zadań miałby on również obowiązek odgrywania roli swoistego łącznika między organami krajowymi a siecią zespołów CSIRT[15], czyli powołanymi na mocy postanowień dyrektywy sieciami współpracy[16].

Spośród definicji zebranych na stronie NATO Cooperative Cyber Defence Centre of Excellence najbardziej godna uwagi wydaje się definicja niemiecka; określa ona cyberprzestępstwa jako aktywność przestępczą, do której wykorzystuje się usługi oraz aplikacje w cyberprzestrzeni; cyberprzestrzeń może być zarówno źródłem, celem, jak i środowiskiem ataku[17]. Jest to jedna z lepiej skonstruowanych ogólnych definicji, która mogłaby funkcjonować jako sztandarowy przykład definicji przestępstw komputerowych i internetowych. W celu pełnego jej wykorzystania niezbędne jest wskazanie również definicji cyberprzestrzeni, ponieważ bez tego nie będzie możliwe pełne zrozumienie definicji cyberprzestępstwa.

---

13 doc. JOIN (2013)1.

14 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32016L1148 [dostęp: 26.09.2019 r.].

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

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

17 https://ccdcoe.org/cyber-definitions.html [dostęp: 03.01.2013 r.].

Definicja Interpolu, czyli Międzynarodowej Organizacji Policji Kryminalnej (ang. International Criminal Police Organization) charakteryzuje cyberprzestępczość, dzieląc ją na dwa rodzaje:

- zaawansowane cyberprzestępstwa (ang. *advanced cybercrime* albo *high-tech crime*) – ataki przeciwko sprzętowi oraz oprogramowaniu komputerowemu,
- cyberprzestępstwa – „tradycyjne" przestępstwa, które zyskały nowe sposoby dokonania z uwagi na rozwój technologii, w tym m.in. Internetu.

Ponadto Interpol wskazuje na takie cechy cyberprzestępczości jak wygoda i anonimowość, które zapewnia Internet, a także brak jego zarówno fizycznych, jak i wirtualnych granic. Wszystkie te czynniki sprawiają, że sprawcy mogą dopuścić się poważnych przestępstw. Ponadto zauważa się, że w przeszłości cyberprzestępstw dokonywali raczej indywidualni sprawcy. Jednak w związku ze zmianą skali cyberprzestępczości obecnie zajmują się nią grupy, nierzadko zorganizowane, nakierowane na dokonywanie konkretnych zaawansowanych cyberprzestępstw oraz tradycyjnych przestępstw, wykorzystujące przy tym zdobycze nowych technologii. Zazwyczaj same przestępstwa nie są niczym nowym, jednak zmniejsza się czas potrzebny do ich dokonania, pojawia możliwość odniesienia większego niż dotychczas zysku (z uwagi na skalę dokonywanych czynów) oraz wykorzystania ułatwień wynikających z rozwoju technologii.

Z wielu definicji cyberprzestępczości funkcjonujących w literaturze naukowej na wyróżnienie zasługuje koncepcja przedstawiona przez R. Bryanta i S. Bryant[18]. Wyróżniają oni szersze pojęcie przestępczości cyfrowej (ang. *digital crime*), do której zaliczają cyberprzestępczość oraz przestępczość komputerową. Jest to jedna z metod użytych przez autorów, druga natomiast zakłada rozróżnienie według kategorii nowości (ang. *novelty*) i charakteru cyfrowego (ang. *digitality*). Im większy każdy stopień jednej i drugiej cechy, tym łatwiej można zaklasyfikować dany czyn jako przestępstwo cyfrowe. Niewątpliwą wadą tak szerokiej definicji jest jej niedokładność i możliwość zaklasyfikowania każdego z przestępstw do kategorii przestępstw cyfrowych. Pozbawiłoby to sensu tworzenie jakiejkolwiek klasyfikacji cyberprzestępstw, przestępstw cyfrowych i komputerowych, ponieważ można zadać pytanie, czym różniłyby się one od tzw. tradycyjnych przestępstw oprócz metod wykorzystywanych do przygotowania lub dokonania przestępstwa. Sami autorzy zauważają wady takiego toku rozumowania. Do zalet tej koncepcji można zaliczyć to, że autorzy wyróżniają różne przestępstwa, które da się zaklasyfikować do kategorii prze-

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

stępstw cyfrowych lub cyberprzestępstw, często pomijane w innych publikacjach.

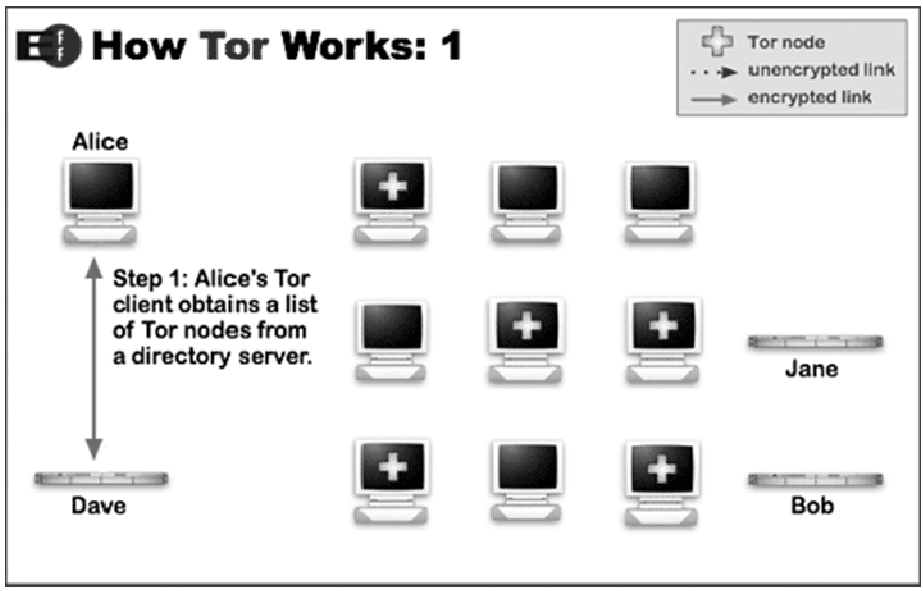
Powyżej przytoczone definicje pochodzą z dokumentów i aktów zagranicznych lub międzynarodowych, część z nich weszła już nawet do polskiego porządku prawnego, np. Konwencja Rady Europy o cyberprzestępczości. Wypada jednak również w tym miejscu przytoczyć definicję znajdującą się w polskich oficjalnych dokumentach. W dokumencie uchwalonym przez Radę Ministrów w dniu 25 czerwca 2013 r. – *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*[19], można odnaleźć definicję cyberprzestępstwa rozumianego jako czyn zabroniony popełniony 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[20] wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Dodatkowo w tym dokumencie zdefiniowana jest cyberprzestrzeń RP jako cyberprzestrzeń w obrębie terytorium państwa polskiego i poza jego terytorium, w miejscach, gdzie funkcjonują przedstawiciele RP. Definicja skonstruowana w taki rozbudowany i szeroki sposób pozwala na dostosowanie się do zagrożeń niesprecyzowanych jeszcze na etapie powstawania *Polityki Ochrony Cyberprzestrzeni RP*. Powoduje to sytuację, w której definicja nie musi być zmieniana rokrocznie z powodu jest dezaktualizacji. Sprzyja to stabilizacji i pewności prawa – zasady, która w demokratycznym państwie prawa powinna być jedną z nadrzędnych. Wątpliwości można mieć jedynie co do zasadności definiowania cyberprzestrzeni i „zamykania" jej w obrębie terytorium jednego państwa. Z jednej strony jest to jak najbardziej zasadne przy definicji cyberprzestępczości sformułowanej w powyższy sposób. Z drugiej jednak – z samej natury Internetu wynika, że jej celem jest odrzucenie granic w dotychczasowym znaczeniu, czyli jako konkretnych, materialnych i dających się ściśle określić terenów. Starając się zrozumieć intencję ustawodawcy, można przypuszczać, że najprawdopodobniej chodzi o położenie serwerów, komputerów bądź urządzeń korzystających z sieci. Należy rozważyć, czy tak ograniczony zakres przedmiotowy definicji

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

[20] System teleinformatyczny – 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 w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2016 r., poz. 1489, 1579, 1823, 1948, 1954 i 2003), czyli urządzenia telekomunikacyjnego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci (Dz.U. Nr 64, poz. 565, z późn. zm.).

nie jest zbyt wąski jak na potrzeby analizy cyberprzestępczości ogólnie, nie tylko pod kątem wykorzystania Internetu Rzeczy do popełniania przestępstw.

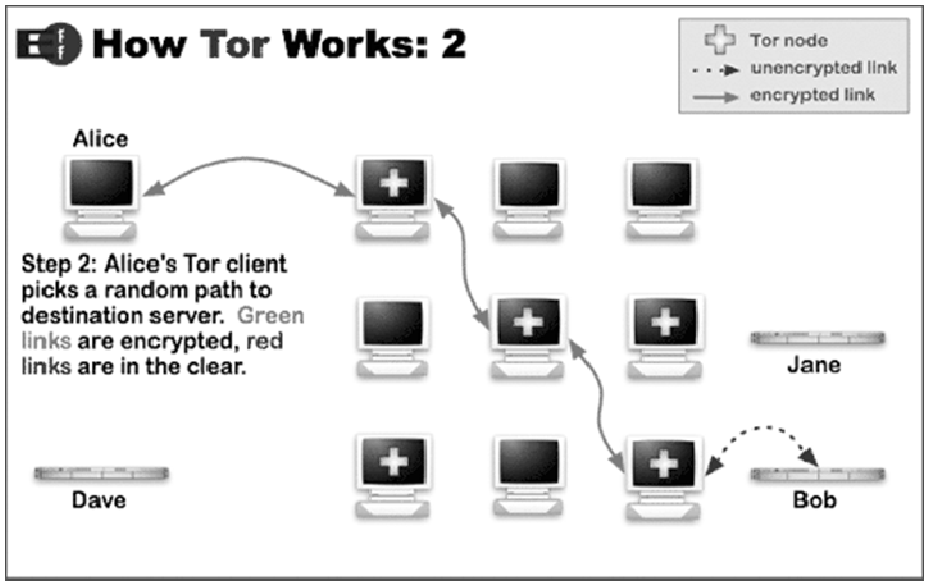
Na kanwie powyższych rozważań można zadać pytanie: co w sytuacji, gdy użytkownik korzysta z tzw. sieci cebulowej, czyli inaczej sieci TOR (ang. *The Onion Routing*)? W celu lepszego zrozumienia należy krótko opisać, na czym polega działanie sieci TOR. Jest to grupa serwerów umożliwiająca użytkownikom prawie całkowicie anonimowe przeglądanie sieci internetowej. Pierwotnie sieć została stworzona przez United States Naval Research Laboratory wraz z Marynarką Wojenną Stanów Zjednoczonych (United States Navy) jako narzędzie mające na celu zabezpieczenie komunikacji rządowej. Łączenie urządzenia użytkownika z miejscem docelowym w sieci następuje przez wysyłanie danych (informacji, maili, plików itp.) przez kilka serwerów (nazywanego przez organizację Tor Project „wirtualnymi tunelami") zamiast bezpośredniej komunikacji między wysyłającym a odbierającym[21]. TOR zapobiega namierzeniu i wyśledzeniu miejsca wysłania i przeznaczenia danego pakietu danych, na każdym etapie bowiem są one zaszyfrowane w taki sposób, że odczytanie ich będzie możliwe dopiero po przejściu przez węzeł nr 3 i z niego bezpośrednio do odbiorcy.



Ryc. 1. Schemat dzialania sieci TOR, cz. 1.

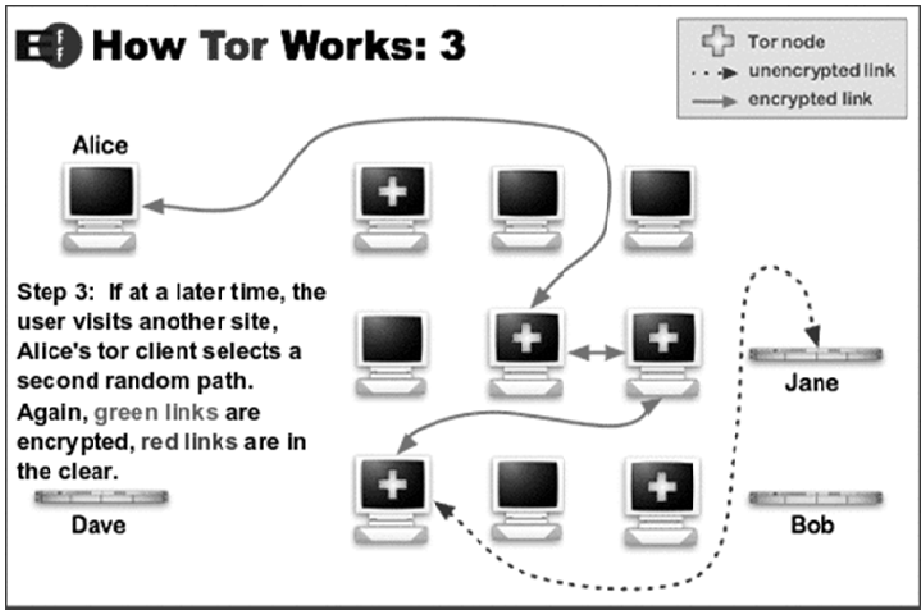
Źródło: https://www.torproject.org/about/overview.html.en#overview [dostęp: 26.09.2019 r.].

[21] https://www.torproject.org/about/overview.html.en#overview [dostęp: 26.09.2019 r.].



Ryc. 2. Schemat dzialania sieci TOR, cz. 2.

Źródło: https://www.torproject.org/about/overview.html.en#overview [dostęp: 26.09.2019 r.].



Ryc. 3. Schemat dzialania sieci TOR, cz. 3.

Źródło: https://www.torproject.org/about/overview.html.en#overview [dostęp: 26.09.2019 r.].

Sieć TOR pozwala na ukrycie tożsamości, ponieważ nie ujawnia, z jakiego miejsca na świecie dana osoba łączy się z konkretną stroną. Może to być wykorzystane chociażby przez sprawców do popełnienia przestępstwa za pośrednictwem koncepcji Internetu Rzeczy – w ich mniemaniu zapewni bowiem większą anonimowość, czyli utrudni pracę organom ścigania. Nie oznacza to jednak, że jest to narzędzie idealne i zapewniające oczekiwaną przez przestępców bezkarność. Sieć TOR nie gwarantuje zachowania pełni anonimowości w przypadku, gdy wysyłane informacje albo strona, którą odwiedzimy, pozwoli na ustalenie tożsamości użytkownika. Przykładowo w niczym nie pomoże korzystanie z przeglądarki TOR, gdy zalogujemy się na swoje konto mailowe czy bankowe i będziemy wykonywali wszystkie te czynności, które wykonujemy w normalnej przeglądarce. Wnikliwy obserwator będzie wtedy w stanie powiązać tożsamość użytkownika TOR z naszą. To samo tyczy się plików – pliki naszego autorstwa lub zawierające treści wyraźnie wskazujące na nas, jedynie wysłane za pośrednictwem sieci TOR, z pewnością nakierują na nas jako użytkownika. Dodatkowo wykorzystywanie tego samego konta mailowego lub nazwy użytkownika, zarówno w życiu prywatnym, jak i w czasie działalności o charakterze przestępczym, również powoduje, że sprawca może zostać w łatwy sposób zidentyfikowany przez organy ścigania.

Na marginesie rozważań o anonimowości w sieci i jej związku z cyberprzestępczością należy podkreślić, że korzystanie z sieci TOR nie może stawiać osoby w kręgu podejrzeń o działalność niezgodną bądź na granicy prawa. W artykułach prasowych często pojawia się teza, że korzystanie z tego typu programów bądź podobnych, które mają za zadanie zwiększyć anonimowość użytkowników w sieci, automatycznie oznacza, że ta osoba ma do ukrycia coś niezgodnego z prawem, tak jak przedstawia to J. Chmielecka już w tytule artykułu opublikowanego w „Dużym Formacie”[22]. Kompletnie niewłaściwe i nieuprawnione jest twierdzenie, że sieć TOR ma na celu maskowanie działalności przestępczej. W obiegu publicznym funkcjonuje błędne przeświadczenie, że osoby chcące zachować anonimowość w sieci to tylko i wyłącznie przestępcy i terroryści. Należy w tym miejscu wyjaśnić podstawowe różnice między tą częścią Internetu, z której wszyscy korzystamy na co dzień, a Deep Web i Dark Web, inaczej zwanym Darknet, bo każda z nich oznacza co innego.

Najprościej będzie opisać każde z tych pojęć na obrazowym przykładzie, funkcjonującym dosyć powszechnie w publicznym obiegu. Wyobraźmy sobie, że Internet jest górą lodową. Jej część znajduje się ponad powierzchnią wody, natomiast, jak wiadomo powszechnie, jest to tylko jej niewielki fragment.

[22] J. Chmielecka, *Po ciemnej stronie internetu*, „Duży Format”, http://wyborcza.pl/duzyformat/1,127290,13318724,Po_ciemnej_stronie_internetu.html [dostęp: 30.01.2013 r.].

Reszta góry jest ukryta pod powierzchnią wody i z daleka nie jest widoczna jej całkowita wielkość i skala. Część widoczna, czyli tzw. sieć zindeksowana (ang. Surface Web), to ta, w której porusza się największa liczba użytkowników; jej nazwa wiąże się z ogólnym dostępem do niej i z faktem, że strony w niej się znajdujące są indeksowane przez wyszukiwarki sieciowe takie jak Google czy Bing. Można w niej znaleźć ogólnodostępne i najpopularniejsze strony internetowe, takie jak Google, Yahoo, YouTube, Wikipedia, Facebook, Twitter oraz inne, wszelkiej maści serwisy informacyjne oraz tematyczne. Jej wielkość szacuje się na niecałe 10% całej sieci. Kolejną częścią metaforycznej góry lodowej jest sieć ukryta, czyli Deep Web. W przeciwieństwie do sieci zindeksowanej obejmuje ona strony niezindeksowane, czyli takie, na które nie można wejść, używając wyszukiwarki sieciowej, ponieważ ich zawartość została zakodowana w tym celu[23]. Obejmuje ona strony umyślnie lub nieumyślnie ukryte, niewidoczne albo w inny sposób zablokowane przed wyszukiwarkami, a także zastrzeżone dla twórcy i użytkowników ze specjalnymi uprawnieniami[24]. 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 to największa część Internetu i stanowi nawet 90% całej sieci[25]. Ostatnią częścią jest Darknet, czyli Dark Web, najmniejsza pod względem liczby stron. Wbrew pozorom nie jest ona niewidoczna dla użytkowników, a dotarcie do stron w Darknecie nie wymaga magicznych zdolności, 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, ale jedynie na ustaleniu położenia serwera, na którym działa[26]. Najczęściej funkcjonują one za pomocą sieci TOR albo I2P, czyli oprogramowania podobnego w swoim działaniu do TOR. Konsekwencją takiego stanu rzeczy jest to, że na stronę operującą w sieci TOR może wejść tylko użytkownik przeglądarki działającej w tej samej sieci. 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. Najszerszą sferą działalności był handel narkotykami i bronią oraz witryny służące do prania brudnych pieniędzy; z tego głównie znane były Silk Road (dwukrotnie likwidowane) oraz Al-

[23] https://www.pcmag.com/encyclopedia/term/41069/deep-web [dostęp: 26.09.2019 r.].
[24] https://www.techopedia.com/definition/15653/deep-web [dostęp: 26.09.2019 r.].
[25] A. Greenberg, *Hacker lexicon: What is the Dark Web?*, WIRED.com, https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ [dostęp: 19.11.2014 r.].
[26] Ibidem.

phaBay, to drugie ze względu na swoją renomę po zamknięciu Silk Road i stabilność serwerów. Silk Road 2 zostało ostatecznie zlikwidowane w listopadzie 2014 roku w ramach operacji „Onymous", przeprowadzonej wspólnie przez Europol, FBI oraz Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych (ang. Department of Homeland Security)[27]. AlphaBay z kolei przestał nagle działać 5 lipca 2017 r., serwery zostały zarekwirowane w Kanadzie przez Kanadyjską Królewską Policję Konną (ang. Royal Canadian Mounted Police) na prośbę FBI oraz przez odpowiednie organy w takich krajach jak Litwa, Wielka Brytania, Tajlandia i Francja, a w tym samym czasie w Bangkoku zatrzymano właściciela serwisu A. Cazesa, obywatela Kanady, który 12 lipca odebrał sobie życie w tajskim więzieniu w oczekiwaniu na ekstradycję do USA[28]. „The Guardian" w artykule cytuje p.o. dyrektora FBI w owym czasie, A. McCabe'a, który stwierdził, że AlphaBay był dziesięć razy większy niż zamknięty w 2013 r. Silk Road, wyraził przy tym obawę, że pomimo zlikwidowania jednej strony w jej miejsce powstanie kolejna, tak jak w miejsce Silk Road powstał AlphaBay i inne strony[29]. 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 znacznie większą skalę, pokazuje, że największym wyzwaniem nie jest jedynie zamykanie tego typu serwisów, ale również zapobieganie powstawaniu nowych, co może wydawać się nierealne, albo monitorowanie tych nowo powstających. Podobna zresztą refleksja odnosi się również do Darknetu, Deep Web oraz sieci TOR – nie należy ich utożsamiać jedynie z przestępczą działalnością w cyberprzestrzeni. Mimo faktu, iż mogą one być narzędziem przestępców, w tym wykorzystujących koncepcję Internetu Rzeczy do celów przestępczych, są czymś o wiele istotniejszym. Są narzędziami, które mogą posłużyć do wielu działań, zarówno legalnych, jak i nielegalnych. Ich funkcjonalność i działanie umożliwiają wielu osobom dostęp do sieci z miejsc, gdzie jest on ograniczony, np. z uwagi na system polityczny, co 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 na jakąkolwiek, na-

[27] 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: 07.11.2014 r.].

[28] S. Gibbs, L. Beckett, *Dark web marketplaces AlphaBay and Hansa shut down*, „The Guardian", https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down [dostęp: 20.07.2017 r.].

[29] Ibidem.

wet szczątkową anonimizację swoich działań[30]. Przykładowo użytkowanie sieci TOR do komunikacji między innymi w opisanych wyżej warunkach rekomendują takie organizacje jak Reporterzy bez Granic i Human Rights Watch[31].

Biorąc pod uwagę temat niniejszego artykułu i dotychczas poruszone w nim zagadnienia, należałoby się zastanowić, w jakim celu powstała konstrukcja „cyberprzestępstwa". Czy, jak twierdzi J. Kosiński: „»Cyber« jest idealnym prefiksem [w słowie cyberprzestępstwo – przyp. autora] – 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"[32]. Nie sposób się nie zgodzić z opinią, że przedrostek „cyber-" jest w takim wypadku nadużywany, co powoduje pewien chaos terminologiczny, a także zupełnie niepotrzebne uogólnienie. Wprowadza się nowe pojęcie zbiorcze dla kategorii, które swoją definicję już mają, i w dodatku zakorzenioną od jakiegoś czasu w badaniach naukowych i doktrynie. Ujednoliceniu terminologii powinno towarzyszyć doprecyzowanie definicji „cyberprzestępstwa" w stopniu wyższym niż jedynie „wrzucenie" do jednego wspólnego kotła różnych definicji odnoszących się do przestępstw komputerowych i sieciowych. Uwzględniając powyższe, należy się zastanowić, w jakim celu używamy definicji „cyberprzestępstwa". Czy dlatego, że jest nam wygodniej i łatwiej nazwać pewną grupę zjawisk zbiorczo, nie zagłębiając się w ich istotę? Czy dlatego, że dążymy do ujednolicenia terminologicznego w kwestii przestępstw doby komputerów, Internetu i nowych technologii w sposób rozumny i odpowiedzialny, uwzględniając niuanse każdego z możliwych przestępstw oraz ich zróżnicowanych postaci i sposobów ich popełniania? Prawdą jest jednak, że w obecnie powstającej literaturze, a także w aktach prawnych, dominującym pojęciem staje się określenie przestępstw komputerowych i internetowych mianem „cyberprzestępstw". Z jednej strony należy stwierdzić, że rzeczywiście przedrostek „cyber-„ jest nadużywany. Z drugiej 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

[30] 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", https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents [dostęp: 05.06.2014 r.].

[31] https://www.torproject.org/about/torusers.html.en [dostęp: 26.09.2019 r.].

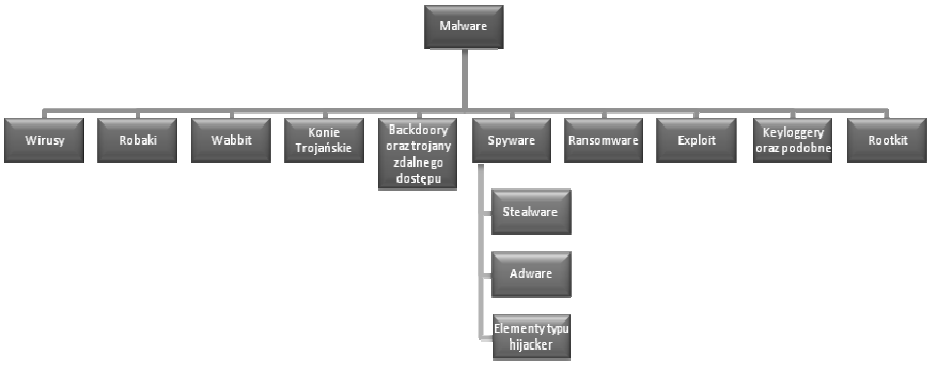
[32] J. Kosiński, *Paradygmaty*…, op. cit.

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 najbardziej efektywnym sposobem 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 nad związkami przestępczości z rozwojem nowych technologii i ich użyciem do popełniania przestępstw.

Powyższa wstępna analiza dotycząca zakresu definicji cyberprzestępczości umożliwia omówienie miejsca Internetu Rzeczy w tejże metodologii. Nie był on do tej pory umiejscowiony w konkretnym jej miejscu. Naturalnie jest to spowodowane tym, że konkretne badania pod tym kątem nie były prowadzone lub są nieznane. Ze względu na charakter przestępstw zaliczanych do kategorii cyberprzestępstw można wywnioskować, że w związku z obecną skalą i dotkliwością cyberprzestępczości oraz rozwojem Internetu Rzeczy należy się spodziewać pogłębienia problemów z bezpieczeństwem. 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. Jest to niezbędne zarówno dla zapobiegania, jak i lepszego zwalczania przestępczości tradycyjnej oraz cyberprzestępczości, jakkolwiek ją zdefiniujemy. Wymienione wyżej zagrożenia nie są jedynymi, które można wykorzystać w połączeniu z koncepcją Internetu Rzeczy. Wyróżnić można również takie niebezpieczeństwa jak: oprogramowanie typu *malware*, spam, botnet, phishing, ataki typu DoS i DDoS oraz oszustwa komputerowe.

Malware to określenie powstałe z połączenia angielskich słów *malicious* i *software*, tzn. szkodliwe oprogramowanie. 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[33]. Podziału oprogramowania typu *malware* można dokonać z uwagi na to, do jakiego typu działania można je wykorzystać i do czego jest ono przeznaczone.

[33] Ibidem.



Ryc. 4. Schemat podziału oprogramowania typu *malware*.

Źródło: opracowanie własne.

Wskazany powyżej podział w sposób wystarczający ukazuje, jak wielkie spektrum możliwości ma do wykorzystania przestępca chcący dokonać cyberprzestępstwa. Z uwagi na charakter popełnianego czynu może podjąć wiele działań, z których zarówno każde z osobna, jak i kilka połączonych ze sobą może mieć dotkliwe skutki nie tylko dla indywidualnego użytkownika, lecz także dla większej grupy. Kolejnymi zagrożeniami istotnymi z punktu widzenia możliwych skutków oraz ich znaczenia i możliwości wykorzystania w ramach koncepcji Internetu Rzeczy są:

- spam – pojęcie to odnosi się do maili czy innego typu wiadomości, których nadawca nie chciał otrzymać, nie oczekiwał ich lub nie zamawiał, najczęściej w ogromnej liczbie, co ma na celu spowolnienie pracy systemu informatycznego, urządzenia lub sieci internetowej[34]; do tej kategorii zagrożeń można zaliczyć również inne zjawiska[35], takie jak:
  - spam nigeryjski (inaczej: przekręt nigeryjski, oszustwo 419)[36],
  - fałszywe reklamy (ang. *false advertising*) – ukrywające pewne warunki sprzedaży lub reklamujące fałszywe bądź podrobione produkty,
  - spam na portalach społecznościowych, np. na Facebooku[37],
  - Pay Per Click – zysk dla właściciela danej reklamy nalicza się po kliknięciu przez użytkownika w daną reklamę, ponadto można przy okazji

[34] S. Hambridge, A. Lunde, *Don't Spew. A Set of Guidelines for Mass Unsolicited Mailings and Postings*, https://www.ietf.org/rfc/rfc2635.txt [dostęp: 26.09.2019 r.].
[35] J. Kosiński, *Paradygmaty*…, op. cit.
[36] Więcej informacji: http://419scam.org [dostęp: 14.01.2014 r.].
[37] *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: 2012 r.].

infekować urządzenia programami typu exploit (np. exploit kit *Magnitude*), czyli rodzaj oprogramowania typu *malware*,

- botnet – grupa komputerów zainfekowanych oprogramowaniem typu *malware*, kontrolowanych przez cyberprzestępców w sposób zdalny[38]; można je wykorzystywać do ataków typu DoS lub DDoS,
- phishing – metoda ataku polegająca na wysyłaniu ofierze maili zainfekowanych złośliwym oprogramowaniem umożliwiających uzyskanie informacji z urządzenia użytkownika, np. danych do logowania do konta bankowego; maile mają naśladować te pochodzące z zaufanego i znanego źródła, takiego jak np. bank lub operator sieci komórkowej[39],
- DoS i DDoS – z ang. *Denial of Service* i *Distributed Denial of Service*, atak polegający na tym, że atakujący chce uniemożliwić innym użytkownikom dostęp do informacji lub usług takich jak poczta elektroniczna, witryny internetowe itp.[40], atak typu *Distributed Denial of Service* polega na wykorzystaniu wielu komputerów lub urządzeń, w tym tego należącego do użytkownika,
- oszustwa komputerowe – wszelkie próby wpływania na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub ich zmienianie bez upoważnienia w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody[41].

Wymieniony powyżej katalog zagrożeń nie jest zamknięty czy enumeratywny. Nie sposób wymienić w tym miejscu wszystkich zagrożeń, a także nie byłoby to celowe. Do omówienia zjawiska wystarcza wskazanie tych kilku. Powyższe zagrożenia można zaobserwować od dawna, jednak wykorzystanie ich w połączeniu z urządzeniami mogącymi być częścią Internetu Rzeczy stworzy zupełnie nowe niebezpieczeństwa. Najlepszym dowodem na to będzie atak typu *Distributed Denial of Service*. Do przeprowadzenia największego do tej pory ataku posłużono się wieloma urządzeniami, które wchodzą w skład koncepcji Internetu Rzeczy. Mowa w tym miejscu o *Dyn cyber attack*. Rozpoczął się on 21 października 2016 r. i obejmował wiele ataków typu DDoS. Celem sprawców były serwery dostawcy usług typu DNS[42] – spółki Dyn, działającej

[38] D. Fischer, *Co to jest botnet?*, Oficjalny Blog Kaspersky Lab, https://plblog.kaspersky.com/botnet/6302/ [dostęp: 27.02.2017 r.].

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

[40] https://www.us-cert.gov/ncas/tips/ST04-015 [dostęp: 04.11.2009 r.].

[41] Zob. art. 287 k.k.

[42] *Domain Name System* – system serwerów przechowujących dane na temat adresów domen; dzięki ich istnieniu użytkownicy mogą posługiwać się adresami stron www w postaci tek-

głównie na terenie Ameryki Północnej, z której usług korzystają największe internetowe serwisy informacyjne, rozrywkowe i usługowe. Do przeprowadzenia ataku wykorzystano dziesiątki milionów adresów IP, z czego dużą liczbę stanowiły sprzęty mające połączenie z Internetem, takie jak drukarki, kamery IP, elektroniczne nianie oraz urządzenia wykorzystywane w domach do łączenia sieci lokalnej z Internetem, na przykład modemy czy routery. Wszystkie te urządzenia z uwagi na możliwość łączenia się przez nie z Internetem mogą być częścią zjawiska Internetu Rzeczy. Wykorzystanie ich do ataku typu DDoS było możliwe w wyniku zakażenia ich oprogramowaniem typu *malware* (w tym przypadku pod nazwą Mirai). Szkodliwe oprogramowanie Mirai zamieniało je w „urządzenia-zombie", czyli elementy sieci typu botnet[43], wykorzystywane do przeprowadzania ataków typu DDoS. Mechanizm jest prosty i opiera się na wysyłaniu takiej liczby „żądań" dostępu do witryny sieci internetowej, że doprowadza to do przeciążenia serwera i uniemożliwia dostęp do niej zwykłym użytkownikom. Cechą wyróżniającą atak z października 2016 r. była użyta metoda, czyli wykorzystanie nie komputerów, ale urządzeń i przedmiotów połączonych z Internetem innych niż komputery, a także skala tego ataku, co pośrednio wynika z zastosowanej metody. Według krótkiej analizy opublikowanej na stronie spółki Dyn sprawcy byli w stanie zaobserwować połączenia pochodzące z milionów adresów IP, brak jest jednak możliwości oszacowania dokładnej liczby adresów pochodzących z zainfekowanych urządzeń. Według niektórych twierdzeń ilość przesyłanych danych była w granicach 1,2 Tbps (ang. *Terabit per second*, terabit na sekundę), jednak brak ostatecznego potwierdzenia tej kwestii. Nawet bez ostatecznego potwierdzenia dokładnych danych można uznać, że pod względem skali i dotkliwości był to jeden z najbardziej groźnych ataków, a dodatkowo niepokoi metoda jego przeprowadzenia[44]. W celu łatwiejszego wyobrażenia, czym atak DDoS jest i czym był w tym konkretnym przypadku, można użyć porównania z centrum handlowym.

stowej zamiast adresów IP, DNS dokonuje „tłumaczenia" wpisanego adresu w formie tekstu na odpowiadający mu adres IP i na odwrót, za: https://pomoc.nazwa.pl/baza-wiedzy/produkty-i-uslugi/domeny/o-domenach-bardziej-technicznie/co-to-jest-dns/ [dostęp: 01.06.2018 r.].

[43] „Botnet to grupa zhakowanych komputerów, które są kontrolowane w sposób zdalny. Autorem botnetu może być jedna lub kilka osób; infekują one 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 się składać z setek lub tysięcy zainfekowanych maszyn, a większe – nawet z milionów" (za: D. Fischer, *Co to jest botnet?*, Blog Kaspersky Lab, https://plblog.kaspersky.com/botnet/6302/ [dostęp: 27.02.2017 r.]); obecnie na kanwie rozważań dotyczących Internetu Rzeczy, czyli także tematyki tej pracy, można mówić o grupie zhakowanych urządzeń, a nie tylko grupie zhakowanych komputerów.

[44] 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: 26.10.2016 r.].

Centrum handlowe będzie serwerem, a poszczególne sklepy w nim się znajdujące – witrynami internetowymi. Zazwyczaj atak tego typu skierowany jest przeciwko jednej konkretnej stronie, w przypadku niniejszej analogii – jednemu sklepowi w centrum handlowym. W efekcie ataku zwykli klienci nie mogą do niego wejść i skorzystać z jego oferty. Specyfika ataku z października 2016 r. polegała na tym, że zdecydowano się nie na blokowanie każdego ze sklepów oddzielnie, co w oczywisty sposób byłoby czaso- i pracochłonne, ale przeprowadzono atak na całe centrum handlowe, czyli serwer. Przez zablokowanie możliwości wejścia klientów do centrum handlowego pojedynczym atakiem o ogromnej skali uniemożliwiono dostęp do wszystkich sklepów naraz. Tak opisana metafora pozwoli na obrazowe przedstawienie, czym był w istocie *Dyn cyber attack*, oraz ukazanie jego istoty w kontekście ataków typu DDoS i możliwości wykorzystania w tym celu nowych koncepcji i zjawisk.

Z punktu widzenia możliwości wykorzystania Internetu Rzeczy do dokonywania ataków komputerowych i sieciowych atak opisany wyżej ma charakter przełomowy. Był pierwszym dokonanym z wykorzystaniem urządzeń i produktów z dostępem do Internetu innych niż komputery. Należy podkreślić w tym miejscu, że w kontekście tematu niniejszej pracy nie sposób przecenić wartości doświadczeń i wniosków, które powinno się wyciągnąć, analizując jego przebieg i efekty. Wykazało to wprost, jak groźne mogą być urządzenia wchodzące w skład Internetu Rzeczy w kontekście przeprowadzenia szeroko zakrojonego ataku sieciowego, którego skutki mogą być trudne do przewidzenia. Departament Bezpieczeństwa Krajowego Stanów Zjednoczonych wszczął śledztwo, ale według źródeł w Białym Domu do dzisiaj brak jest jednak efektów jego ewentualnych działań. Do przeprowadzenia ataku przyznały się grupy takie jak Anonymous oraz New World Hackers, lecz brak potwierdzenia również tych doniesień, a według spółki Flashpoint zajmującej się bezpieczeństwem został on dokonany przez tzw. *script kiddies*[45], którzy wykorzystali kod oprogramowania Mirai udostępniony publicznie w tym samym miesiącu, w którym nastąpił atak[46]. Do dzisiaj nie udało się ustalić sprawcy ataku, dlatego aktualnie można się poruszać jedynie w sferze domysłów. Można próbować wysnuwać wnioski co do tożsamości sprawcy lub sprawców na podstawie znanych ogólnie faktów. Z uwagi na zastosowany typ ataku oraz fakt, iż kod złośliwego

[45] *Script kiddie* – żargonowe określenie niedoświadczonego hakera bądź crackera, który używa aplikacji i programów nienapisanych przez siebie, lecz wytworzonych przez innych, bez dogłębnej znajomości ich działania, za: https://pl.wikipedia.org/wiki/Script_kiddie [dostęp: 1.06.2018 r.].

[46] 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: 26.10.2016 r.].

oprogramowania Mirai był jawny i każdy użytkownik sieci mógł mieć do niego dostęp, można domniemywać, że osoba lub osoby dokonujące ataku nie musiały koniecznie posiadać wąskiej specjalistycznej wiedzy z zakresu programowania, choć niezbędna była wiedza podstawowa. Z uwagi na powyższe ogólnie można przychylić się do wniosków niektórych osób, że bardziej prawdopodobne jest sprawstwo *script kiddies* aniżeli tak dobrze zorganizowanych grup hakerskich jak Anonymous. Mimo faktu, iż sprawcy samego ataku nie zostali ustaleni, w grudniu 2017 r. amerykański Departament Sprawiedliwości wystosował komunikat o przyznaniu się trzech nastolatków do stworzenia dwóch sieci botnet opartych na urządzeniach mogących wchodzić w skład koncepcji Internetu Rzeczy. Mieli oni wykorzystać do tego *malware* Mirai, czyli ten sam, który został użyty do ataku na serwery firmy Dyn[47].

Najistotniejszym faktem wynikającym z *Dyn cyber attack* jest to, że po raz pierwszy zastosowano urządzenia mające dostęp do Internetu, a co więcej, wykorzystano je w ogromnej, właściwie wiodącej roli. Ukazuje to niemały potencjał Internetu Rzeczy w kontekście popełniania przestępstw. Ujawniło również, jak problematyczne może być ustalenie chociażby sprawcy lub dokładnego miejsca, z którego rozpoczęto przygotowywanie bądź dokonywanie czynu. Zwraca uwagę, jak niski był poziom zabezpieczeń tychże urządzeń, co umożliwiło dokonanie ataku na tak wielką liczbę różnego typu urządzeń, pochodzących od różnych producentów. Może to świadczyć o wspólnych wadach i brakach w zabezpieczeniach, niezależnie od producenta, a więc wspólnych dla zjawiska Internetu Rzeczy.

Podsumowując rozważania dotyczące umiejscowienia omawianego zjawiska w metodologii badań nad problematyką cyberprzestępczości, należy stwierdzić, że jest to koncepcja umożliwiająca połączenie wielu dotychczas istniejących możliwości popełniania tego typu przestępstw. Środowisko to może stanowić jedną wielofunkcyjną platformę służącą zarówno do popełniania przestępstw, jak i zapobiegania im. Z tego powodu niezbędne jest przeprowadzanie pogłębionych badań kryminalistycznych i prawnokarnych. Pozwoli to na dostosowanie obecnego stanu wiedzy kryminalistycznej do nowych wyzwań, jakie niesie ze sobą rozwój nowych technologii i ich wykorzystanie przez przestępców.

[47] Department of Justice, U.S. Attorney's Office, District of New Jersey, Justice Department Announces Charges And Guilty Pleas In Three Computer Crime Cases Involving Significant Cyber Attacks, Department of Justice 2017, https://www.justice.gov/usao-nj/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases [dostęp: 8.12.2018 r.].

Streszczenie

Artykuł ma na celu przedstawienie różnych i funkcjonujących obecnie definicji Internetu Rzeczy w odniesieniu do mnogich definicji cyberprzestępczości oraz umieszczenie Internetu Rzeczy i możliwych zagrożeń dla bezpieczeństwa wynikających z rozwoju tego zjawiska w systematyce i metodologii badań szeroko rozumianej cyberprzestępczości. Dodatkowo w artykule wskazane i omówione zostały potencjalne metody techniczne i narzędzia popełniania przestępstw z wykorzystaniem zjawiska Internetu Rzeczy.

Słowa kluczowe: Internet Rzeczy, cyberprzestępczość, cyberbezpieczeństwo, kryminalistyka

Summary

The aim of this article is to relate Internet of Things with cybercrimes and its various definitions, currently circulating in scientific and professional disputes. Due to the rapid development of Internet of Things, possible dangers associated with the phenomenon need to be positioned in reference with extensive amount of definitions of cybercrimes. Additionally, these dangers need to be put within cybersecurity's and legal research methodology and systematics. Moreover, this article covers potential methods and tools to commit crimes with the use of Internet of Things phenomenon.

Keywords: Internet of Things, cybercrime, cybersecurity, criminalistics

Bibliografia

Literatura

Ball J., *Guardian launches SecureDrop system for whistleblowers to share files*, „The Guardian", https://www.theguardian.com/technology/2014/jun/05/guardian-launches-securedrop-whistleblowers-documents.

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

Chmielecka J., *Po ciemnej stronie internetu*, „Duży Format", http://wyborcza.pl/duzyformat/1,127290,13318724,Po_ciemnej_stronie_internetu.html.

Gibbs S., Beckett L., *Dark web marketplaces AlphaBay and Hansa shut down*, „The Guardian", https://www.theguardian.com/technology/2017/jul/20/dark-web-marketplaces-alphabay-hansa-shut-down.

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

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

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

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*, Springer, Heidelberg–New York 2010.

Turing A.M., *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.

Źródła

Department of Justice, U.S. Attorney's Office, District of New Jersey, Justice Department Announces Charges And Guilty Pleas In Three Computer Crime Cases Involving Significant Cyber Attacks, Department of Justice 2017, https://www.justice.gov/usao-nj/pr/justice-department-announces-charges-and-guilty-pleas-three-computer-crime-cases.

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

Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 22 maja 2007 r. – w kierunku ogólnej strategii zwalczania cyberprzestępczości.

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.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r.

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

Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczącym penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasbourgu w dniu 28 stycznia 2003 r.

Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2016 r. poz. 1489, 1579, 1823, 1948, 1954 i 2003), Dz. U. Nr 64, poz. 565, z późn. zm.)

Internet

Fischer D., *Co to jest botnet?*, Oficjalny Blog Kaspersky Lab, https://plblog.kaspersky.com/botnet/6302/.

Greenberg A., *Global Web crackdown arrests 17, seizes hundreds of Dark Net domains*, WIRED.com, https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/.

Greenberg A., *Hacker lexicon: What is the Dark Web?*, WIRED.com, https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.

Hambridge S., Lunde A., *Don't Sew. A Set of Guidelines for Mass Unsolicited Mailings and Postings*, https://www.ietf.org/rfc/rfc2635.txt.

Hilton S., *Dyn analysis summary of Friday October 21 Attack*, Dyn 2016, https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

Lomas N., *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.

Symantec, 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.