Agnieszka Słota-Bohosiewicz
Akademia Sztuki Wojennej,
Wydział Zarządzania i Dowodzenia
agnes@kernel.pl
ORCID 0000-0002-6152-7995

DOI: 10.13166/JMS/111177
JOURNAL OF MODERN SCIENCE TOM 2/41/2019, S. 189–208

The impact of the Internet of Things on human security

Wpływ Internetu rzeczy na bezpieczeństwo człowieka

Abstract

The analysis of selected scientific articles about the Internet of Things leads to the conclusion that the interest of researchers is growing. The Internet of Things is a complex environment in which technical aspects meet with social and military aspects. The Internet of Things inherits and multiplies the potential vulnerability of a single device on the Internet. The effects of the Mirai botnet in the USA, the Denial of service attack on Liberia, are a picture of the possible negative impact of the Internet of Things on human security.

Streszczenie

Analiza wybranych artykułów naukowych na temat Internetu rzeczy prowadzi do wniosku, że zainteresowanie naukowców rośnie. Internet rzeczy jest złożonym środowiskiem, w którym aspekty techniczne spotykają się z aspektami społecznymi i wojskowymi. Internet przedmiotów dziedziczy i mnoży potencjalną podatność pojedynczego urządzenia w Internecie. Skutki botnetu Mirai w USA i ataku Denial of Service na Liberię obrazują możliwy negatywny wpływ Internetu przedmiotów na bezpieczeństwo ludzi.

Keywords: *Internet of Things, security, hybrid threats*

Słowa kluczowe: *Internet rzeczy, bezpieczeństwo, zagrożenia hybrydowe*

Wprowadzenie

Autorem nazwy „Internet rzeczy" (ang. Internet of Things) jest Kevin Ashton (Gabbai, 2015). Sformułowanie używane jest od 1999 r. Internet rzeczy oznacza sieć urządzeń połączonych pośrednio lub bezpośrednio do Internetu.

Badania treści artykułów w aspekcie Internetu rzeczy (Trnka, Cerny, Stickney, 2018) wskazują na rosnące naukowe zainteresowanie. Rozważania o zastosowaniu Internetu rzeczy w sferze militarnej (Bognar, 2018); Cha, S. et al., 2018) prowadzą do konstatacji o rosnącej istotności Internetu rzeczy.

Spotykane w publikacjach (HIIK, 2018) stawianie ataków w cyberprzestrzeni na poziomie destrukcyjnych ataków nawiązujących do konfliktów zbrojnych prowadzi do sformułowania pytania: w jaki sposób Internet rzeczy może wpływać na bezpieczeństwo człowieka?

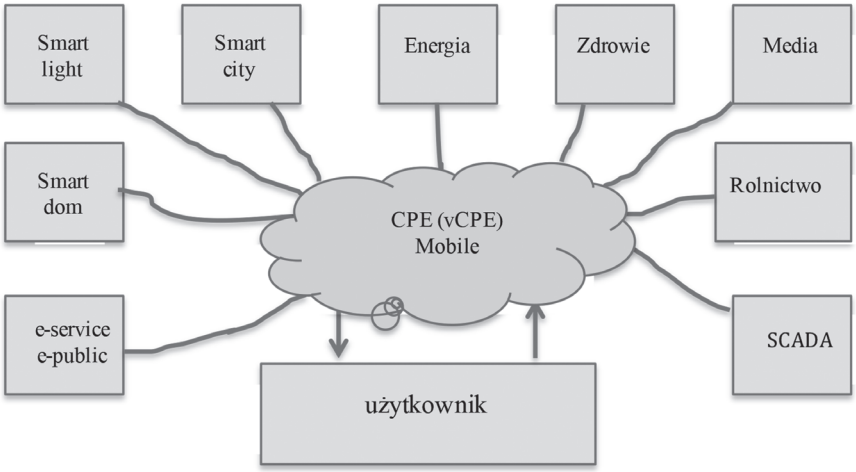
Brak zwartej naukowej publikacji na rynku polskim bezpośrednio o Internecie rzeczy oraz interdyscyplinarny i globalny charakter stosowania Internetu rzeczy w opinii autorki usprawiedliwia sięganie do źródeł poza literaturą „książkową".

Metody badawcze

W celu próby udzielenia odpowiedzi na pytanie o wpływ Internetu rzeczy na bezpieczeństwo człowieka, wybrano i przeanalizowano: publikacje zwarte, artykuły w portalu Web of Science (WoS), publikacje HIIK Barometru Konfliktów 2016 i 2017, dostępne analizy Gartnera, doniesienia prasowe oraz najlepsze praktyki zabezpieczania urządzeń (OWASP). Wykorzystano obserwację uczestniczącą – doświadczenia z pracy zawodowej. Do rozdzielenia słabych stron od zagrożeń wykorzystano technikę SWOT. W przypadku ataku na Liberię zastosowano studium przypadku.

Internet rzeczy – wielki świat korelacji

Internet rzeczy możemy zidentyfikować w usługach elektronicznych, inteligentnym domu, smart-city, nowoczesnych licznikach energii, telemedycynie, mediach, urządzeniach przemysłowych, urządzeniach latających czy rolnictwie precyzyjnym. Użytkownik łączy się Internetem rzeczy poprzez urządzenie telekomunikacyjne (CPE, ang. *Customer-premises equipment*), które także stanowi element Internetu rzeczy (rys. 1). Każdy komputer może być składnikiem Internetu rzeczy.



Rysunek 1.
Zakres zastosowań Internetu rzeczy

Źródło: Opracowanie własne

Przykłady nie wyczerpują katalogu możliwych usytuowań i celów stosowania urządzeń. Występująca połączoność i integracja rozwiązań elektronicznych dają efekt synergii. W opinii autorki współzależność z synergią stanowią istotę Internetu rzeczy.

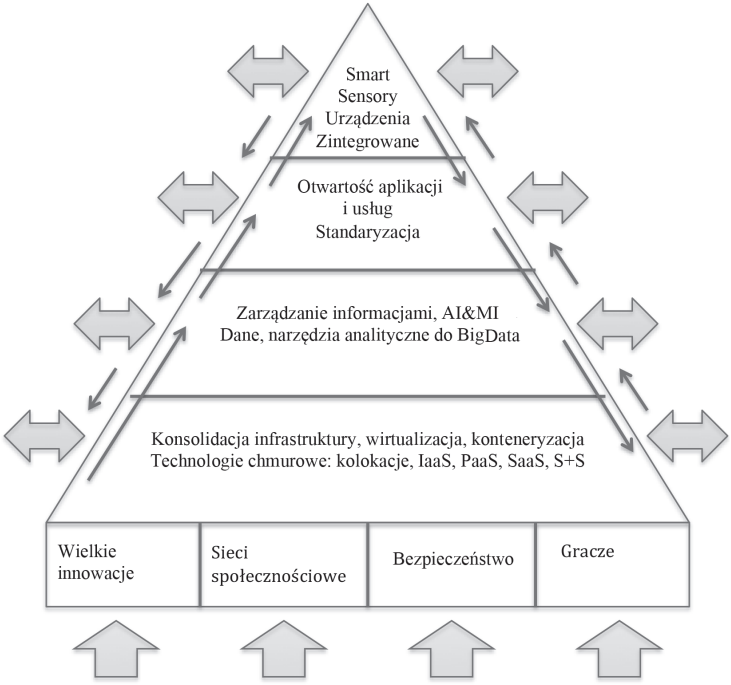
Podejmując refleksję nad wpływem urządzeń na człowieka, należy podkreślić, że fuzja świata fizycznego i świata wirtualnego (Costigan, Lindstrom, 2016) powinna zmienić podejście do zarządzania informacją. Z jednej strony indywidualizacja wykorzystywania rozwiązań elektronicznych, z drugiej strony masowe wykorzystywanie podobnych rozwiązań wymagają uwagi ze strony sektora publicznego (ustawodawcy). Ustalenie odpowiedzi na pytania dotyczące bezpieczeństwa informacji:

- w jaki sposób są gromadzone i następnie wykorzystywane dane i informacje dotyczące Internetu rzeczy,
- (czy i) jakie dane oraz informacje udostępniane są stronom trzecim,
- jak zmienia się wartość danych w połączeniu z innymi danymi,

wymaga dogłębnego zrozumienia poszczególnych składników, następnie złożonych składników, architektury i otoczenia. Agregacja danych i informacji

w Big Data: „to się dzieje" (Mayer-Schoenberger, Cukier, 2014) jest nowym podejściem do „obrazowania", tj. swoistego zdalnego monitorowania sytuacji oraz indywidualnych osób w danej przestrzeni geograficznej przez nieuprawnione podmioty.

Dogłębne zrozumienie złożoności Internetu rzeczy wymaga spojrzenia na wymiar techniczny. Rysunek 2 przedstawia piramidę – architekturę Internetu rzeczy. Należy podkreślić, że w Internecie rzeczy spotykają się wszelkie możliwe technologie, współczesne trendy rozwojowe. Z praktyki autorki w urządzeniach obecne są także „stare" błędy i „stare" rozwiązania programowe. Zaimplementowane w nowym, atrakcyjnym dla ludzkiego oka pudełku są łatwo sprzedawalne (niska cena) – wszakże celem producenta jest sprzedaż.



Rysunek 2.
Złożoność Internetu rzeczy

Źródło: Opracowanie na podstawie OWASP, Radhakrishnan 2015, własnych analiz

W opinii autorki u podstaw popularyzacji Internetu rzeczy w ujęciu społecznym jest fascynacja technicznymi innowacjami, sieciami społecznymi, potrzebą bezpieczeństwa (zgodnie z piramidą potrzeb Maslowa), a także – może niedoceniana – grupa społeczna graczy. Najniższą warstwą piramidy architektury Internetu rzeczy są usługi chmurowe, których filozofia oparta jest na elastyczności i skalowalności zasobów informatycznych, możliwości automatycznej orkiestracji narzędzi oraz przede wszystkim łatwej dostępności dla końcowego nietechnicznego klienta. Logicznie wyżej, tj. nad warstwą chmurową, znajduje się cały business intelligence posiadający narzędzia do przetwarzania danych w celu przygotowywania żądanych informacji. W następnej warstwie są szeroko pojęte aplikacje, od typowych „grubych" klientów, poprzez GUI (ang. Graphics User Interface), aż do aplikacji mobilnych. Na samym czubku piramidy jak góry lodowej znajdują się konkretne czujniki, umieszczone w danym środowisku, przetwarzające zjawiska fizyczne lub chemiczne w konkretne dane.

Uzupełniając przyczyny popularyzacji Internetu rzeczy, z obserwacji autorki wynika, że wzrost liczebności urządzeń elektronicznych ma związek z:

- upowszechnianiem dostępu do Internetu,
- malejącym kosztem podłączeń,
- taniejącą technologią,
- częstym wbudowywaniem czujników i modułów komunikacyjnych,
- upowszechnianiem „gadżetów".

Do połączenia danego urządzenia są wykorzystywane protokoły komunikacyjne z wszystkich warstw ISO/OSI, zwłaszcza TCP/IP, UDP, wszelkie protokoły aplikacyjne. Ponadto feeria bezprzewodowych implementacji takich jak: Wi-Fi, NFC, RFID, Bluetooth, Z-Wave.

Dla uproszczenia i pokazania rosnącej podaży urządzeń z Internetu rzeczy można przyjąć, że technologią umożliwiającą korzystanie z cechy połączoności jest wbudowany moduł Wi-Fi. Tabela 1 przedstawia efekt sprawdzenia w wybranych sklepach internetowych liczby potencjalnych urządzeń mogących partycypować w Internecie rzeczy, w dwóch terminach.

Tabela 1.

Lp.	Sklep	urządzenia elektroniczne z modułem Wi-Fi (liczba produktów lub ofert)		
		Data sprawdzenia		wzrost lub spadek [%]
		05.08.2018	18.11.2018	
1.	Conrad.de	1 641	1 891	+ 15%
2.	Saturn.de	236	277	+ 17%
3.	Amazon.com (dział elektronika)	ok. 30 000	ok. 30 000	0%
4.	Allegro.pl	61 064	59 008	- 3%
5.	Banggood.com	2 137	2 353	+ 10%
6.	Aliexpress.com	203 291	334 436	+ 65%
7.	Newfrog.com	985	1 134	+ 15%
8.	Etsy.com	3 278	3 734	+ 14%

Źródło: Opracowanie własne

Obserwowany wzrost podaży jest związany z rosnącą popularnością na „zabawki".

Mocną stroną Internetu rzeczy jest to, że technologia zwiększa jednostkowe ludzkie możliwości. Pozytywny wpływ Internetu rzeczy na bezpieczeństwo człowieka jest niezaprzeczalny. Urządzenia mają zastosowanie w medycynie, opiece nad osobami niepełnosprawnymi i starszymi (konsultacje na odległość – przykładowo małopolski Tele-Anioł), monitoringu on-line, smart city, automatyzacji (M2M), smart meteringu i wielu innych dziedzinach.

Potrzeba standaryzacji jest realizowana przez opracowywanie dokumentów RFC (ang. Request For Comments), w których celem jest uspójnienie, ujednolicenie, uporządkowanie wiedzy o implementowaniu różnych mechanizmów charakterystycznych dla urządzeń elektronicznych Internetu rzeczy (Keränen A., Bormann C., 2016). Przykładowe dokumenty standaryzacyjne (do wyszukania przez panel https://www.rfc-editor.org/search/rfc_search.php):

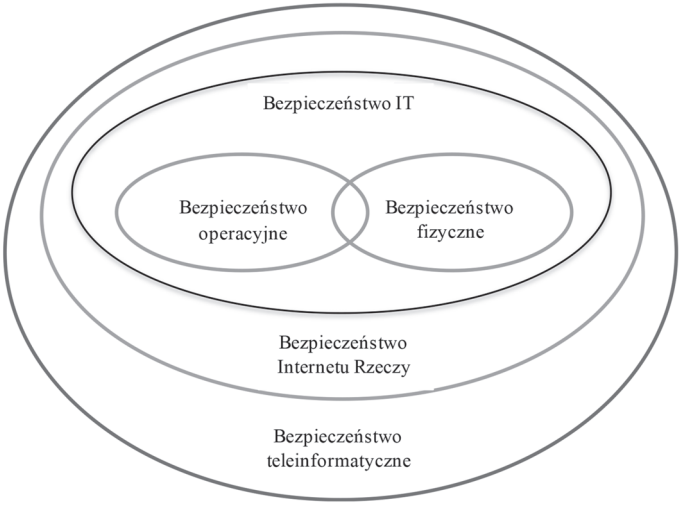
- Terminologia – RFC 7228,
- architektoniczne – RFC 7452,
- Bluetooth Low Energy – RFC 7668,
- ITU-T G.9959 (wykorzystywane w Z-Wave, RFC 7428),
- IPv6 Routing Protocol for Low-Power and Lossy Networks – RFC 6550,

- Constrained Application Protocol (CoAP)- RFC 7252,
- Rozszerzenie CoAP – RFC 7390,
- Dalszy rozwój CoAP – RFC 7641,
- Constrained RESTful Environments (CoRE link format) – RFC 6690,
- Concise Binary Object Representation (CBOR) – RFC 7049,
- Autoryzacja i uwierzytelnianie – RFC 7744,
- Specyfikacja konfiguracji IEEE 802.15.4e – RFC 7554.

M. Lakomy uważa, że „im gęstsza elektronika oraz im bardziej cyberprzestrzeń przenika realną przestrzeń, tym bardziej realne życie staje się uzależnione od właściwego funkcjonowania cyberprzestrzeni" (Lakomy, 2015).

Zagrożenia i słabe strony Internetu rzeczy

W ujęciu Gartnera (Gartner, 2016) na bezpieczeństwo Internetu rzeczy składa się bezpieczeństwo technologii informatycznych (IT), bezpieczeństwo fizyczne i bezpieczeństwo operacyjne. Zewnętrznie, na bezpieczeństwo Internetu rzeczy wpływa bezpieczeństwo teleinformatyczne (rys. 3).



Rysunek 3.
Zagrożenia Internetu rzeczy

Źródło: Opracowanie własne na podstawie Gartner, 2016

Z praktyki autorki wynika, że czynnikami wpływającymi na słabość (bezpieczeństwa) Internetu rzeczy mogą być przykładowo: oprogramowanie z błędami lub ukrytymi dodatkowymi funkcjonalnościami, nieodpowiednie mechanizmy zapewniania autoryzacji i uwierzytelniania. Ponadto za słabości odpowiada niewystarczające zaangażowanie producenta w cyklu życia danego urządzenia elektronicznego (Ross M., 2018).

Według OWASP (ang. *Open Web Application Security Project*) słabe strony korespondują z zagrożeniami, które wykorzystują faktyczne i potencjalne podatności. Możliwe są różne wektory ataków. Tabela 2 przedstawia katalog zagrożeń i słabych stron Internetu rzeczy w ujęciu OWASP.

Tabela 2.

Lp.	Zagrożenie – wektor ataku	Słabe strony – potencjalne podatności
1.	Kontrola dostępu	Domyślne zaufanie między komponentami
		Nieprawidłowe zabezpieczenia dostępu
		Nielogiczna terminacja działania
		Brak procedury dostępu
2.	Pamięć urządzenia	Niezabezpieczone loginy
		Niezabezpieczone hasła
		Dane uwierzytelniające dostawców
		Obecność kluczy
3.	Fizyczne interfejsy urządzenia	Zgranie (ekstrakcja) firmware'u
		Braki w CLI (ang. *Command Line Interface*) użytkownika
		Braki w CLI Administratora
		Przekroczenie uprawnień
		Reset umożliwiający zmiany
		Brak autoryzacji usuwania nośników

Lp.	Zagrożenie – wektor ataku	Słabe strony – potencjalne podatności
4.	Interfejs webowy użytkownika	SQL injection
		Cross-site scripting
		Cross-site Request Forgery
		Odgadywanie loginów użytkowników
		Słabe hasła
		Zablokowanie konta
		Domyślne hasła
5.	Firmware urządzenia	Hardcode'owane poświadczenia
		Ujawnianie informacji „wrażliwych", tj. o charakterze wskazówek
		Ujawnianie schowanych URL
		Obecność kluczy
		Szczegółowe wyświetlanie wersji/ostatniego update
6.	Usługi sieciowe urządzenia	Ujawnianie informacji
		Problemy z CLI użytkownika
		Problemy z CLI administratora
		Wstrzykiwanie kodu – brak sanityzacji
		Odmowa usługi
		Nieszyfrowane usługi
		Słabe szyfrowanie
		Testowe usługi (programistyczne)
		Przepełnienie bufora
		Problematyka UPnP (ang. Uniwersal Plug and Play)
		Usługi UDP

Lp.	Zagrożenie – wektor ataku	Słabe strony – potencjalne podatności
7.	Interfejs administratora	SQL Injection
		Cross-site scripting
		Cross-site request forgery
		Enumeracje loginów
		Słabe hasła
		Zablokowanie konta
		Hasła domyślne
		Niedopracowane opcje szyfrowania/zabezpieczania
		Proces rejestracji
		Niekonsekwentne uwierzytelnianie dwuskładnikowe
		Brak możliwości wyczyszczenia urządzenia
8.	Local Data Storage	Nieszyfrowane dane
		Dane zaszyfrowane przez znane klucze
		Brak kontroli integralności danych
9.	Webowy interfejs chmury	SQL injection
		Cross-site scripting
		Cross-site request forgery
		Odgadywanie loginów
		Słabe hasła
		Zablokowanie konta
		Domyślne dane uwierzytelniające
		Szyfrowanie komunikacji – problemy
		Nieodpowiedni proces odzyskiwania hasła
		Braki w uwierzytelnianiu dwuskładnikowe

Lp.	Zagrożenie – wektor ataku	Słabe strony – potencjalne podatności
10.	API (ang. *Application Programming Interface*) współpracujących firm	Nieszyfrowane dane identyfikujące osoby
		Wyciek informacji z urządzenia
		Wyciek lokalizacji urządzenia
11.	Aktualizacje	Ściąganie aktualizacji kanałem nieszyfrowanym
		Niepodpisane poprawki
		Nadpisywanie poprawek
		Brak weryfikacji aktualizacji
		Poprawka zawierająca malware
		Niepoprawny mechanizm aktualizacji
		Brak procedury/opisu aktualizacji
12.	Aplikacje mobilne	Brak zaufania (nieciągły łańcuch zaufania)
		Odgadywanie loginów
		Blokowanie konta
		Domyślne dane uwierzytelniające
		Słabe hasła
		Nieodpowiednie przechowywanie danych
		Problemy z szyfrowaniem transmisji
		Niepoprawny mechanizm odzyskiwania hasła
		Uwierzytelnianie dwuskładnikowe z brakami
13.	API dostawcy	Braki w ciągłości zaufania w aplikacji mobilnej lub w chmurze – brak blockchain
		Słabe uwierzytelnianie
		Słaba kontrola dostępu
		Ataki polegające na pomijaniu walidacji danych

Lp.	Zagrożenie – wektor ataku	Słabe strony – potencjalne podatności
14.	Komunikacja w ekosystemie	Braki w kontroli poprawności „łańcuchów" zależności
		Szeroka dostępność komponentów (brak ograniczania geolokalizacji)
		Zdalnie wykonywane polecenia (komendy)
		Braki terminacji – wylogowania/wyrejestrowania
		Niebezpieczne wymuszanie aktualizacji
15.	Ruch sieciowy	Sieć lokalna – podsłuch
		Sieć lokalna na styku z Internetem
		Niestandardowe – inne podatności

Źródło: Opracowanie własne, na podstawie informacji w portalu OWASP

Przedstawione w tabeli słabe strony mają związek ze „sklepową" jakością dyktowaną przez detaliczny rynek nietechnicznych klientów: po włączeniu zasilania urządzenie ma „działać" (jako UPnP).

Badacze (De Donno, et al. 2018) podkreślają, że bezpieczeństwo Internetu rzeczy zostało źle zaprojektowane. M. Marczyk pisze, że „we współczesnej organizacji jednym z najważniejszych zagrożeń bezpieczeństwa jest możliwość niekontrolowanego dostępu i ujawnienia informacji stanowiącej tajemnicę, najczęściej dotyczy to informacji przetwarzanej w systemach i sieciach teleinformatycznych (sieci komputerowe)" (Marczyk, 2015).

Z obserwacji autorki wynika, że klient często nie ma świadomości technicznej, jak również sprzedawca nie ma obowiązku szkolenia z podstaw bezpieczeństwa Internetu rzeczy. Tymczasem brak konieczności lub wymuszania konieczności posiadania wiedzy przez klienta o podstawowych zabezpieczeniach na wejściu generuje ryzyko:

- fałszywego poczucia bezpieczeństwa,
- umożliwienia szpiegostwa,
- wykradania danych,
- przejmowania uprawnień.

Każdy czas ma swoje wojny i swoje ograniczenia (Clausewitz, 2017). Internet rzeczy ma związek z zagrożeniami opisywanymi jako hybrydowe (Mahlyanov, 2018). Ponadto może mieć wpływ na działania militarne, może być także wykorzystywany do celów militarnych (Bognar, 2018). Wyzwaniem może być metodyka obiektywnej oceny bezpieczeństwa rozwiązań elektronicznych do zastosowań militarnych (Cha, S. et al., 2018).

Jak skuteczne może być zmasowane niezgodne z przeznaczeniem, funkcjonowanie Internetu rzeczy, zostało opisane w artykule naukowym (De Donno, et al. 2018). W październiku 2016 roku botnet Mirai składający się głównie z przejętych kamer CCTV (Waqas, 2016) i głównie w USA sparaliżował firmę DNS Dyn, powodując wyłączenie wielu stron postawionych na infrastrukturze na terenie USA. Co ciekawe, przed wyborami prezydenckimi. Efekt zmasowania zrobił swoje, natężenie ruchu przekroczyło ponad 500 Gbps (Goldman, 2016; Krebs, 2016), wysycając łącza lub wyczerpując zasoby obliczeniowe. Uzyskany efekt ataku DoS (ang. Denial of Service), czyli odmowa usługi, w opinii autorki, jest zawsze skutecznym narzędziem nacisku. Konsekwencją ataku jest utrata przychodów firm komercyjnych oferujących lub funkcjonujących w oparciu na usługi internetowe dla zwykłych obywateli, innych firm lub dla administracji publicznej (efekt: „Internet nie działa"). Atak DoS uniemożliwia także prowadzenie monitorowania działań biznesowych na krótki czas, co jest istotne, gdy monitoring dotyczy przepływu pieniędzy lub towarów o szczególnym charakterze, jak na przykład diamenty z regionów objętych konfliktami. Zatem atak DoS jest bardzo dobrym narzędziem nieletalnym (uwaga na urządzenia medyczne udostępnione nieświadomie przez Wi-Fi lub tradycyjnie przekierowanie do Internetu – zdarzają się błędy administratorom lub… „ułatwienia" dla lekarzy).

Poniżej przykład fragmentu zapytania, które zostało wysłane do prywatnego webserwera autorki w czasie aktywności botnetu Mirai. Celem zapytania było rozpoznanie i potencjalne przejęcie w celu dołączenia do botnetu (być może Mirai). IP źródłowe zostało celowo zanonimizowane.

ABCD.EFGH.IJK.LMN - - [27/Oct/2016:05:33:05 +0200] "GET **/.git/**HEAD HTTP/1.1" 404 994 "-" "Mozilla/5.0

ABCD.EFGH.IJK.LMN - - [27/Oct/2016:05:33:05 +0200] "GET /**HNAP1** HTTP/1.1" 404 994 „-" „Mozilla/5.0

Wyżej wskazane dwa zapytania mają bezpośredni związek z poszukiwaniami słabych/niedokonfigurowanych usług, dalszej inwestygacji i przejęcia kontroli w celu zasilenia botnetu. W przypadku webserwera autorki komunikat 404 zakończył „rekrutację" w sposób bezowocny.

Oczywiście Internet jest regularnie przeszukiwany w poszukiwaniu **słabych haseł** – domyślnie ustawianych przez producenta (tak było w przypadku kamer CCTV w botnecie Mirai), host autorki również jest regularnie „szturmowany", poniżej dowód (z zanonimizowaną adresacją):

```
[agnes@agnes ~]$ sudo su -
[sudo] password for agnes:
Last login: Thu Feb 16 21:42:58 CET 2017 on pts/0
Last failed login: Sun Feb 19 01:17:42 CET 2017 from AAA.BBB.CCC.DDD on ssh:notty
There were 46298 failed login attempts since the last successful login.
[root@agnes ~]# date
Sun Feb 19 01:17:59 CET 2017
```

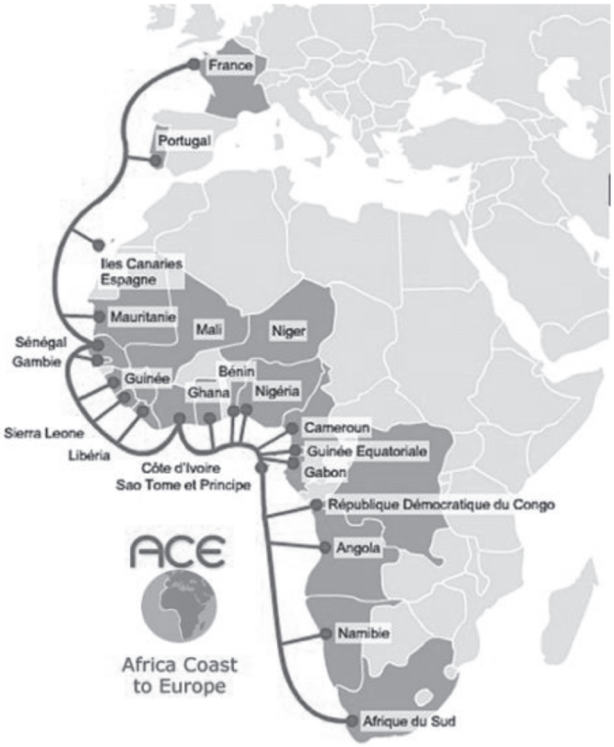
Ze względu na fakt, iż logowanie bezpośrednio na roota jest zakazane w odpowiednim pliku konfiguracyjnym, „gość" dobija się bezskutecznie. Niemniej na uwagę zasługuje liczba prób wejścia: 46298. Tak wytrwały może być tylko automat – inne urządzenie z Internetu rzeczy.

DoS na Liberię

W 4 kwartale 2016 r. efekt skali przejętych urządzeń w ramach Internetu rzeczy został wykorzystany poza USA także przeciwko państwu w Afryce: Liberii (Krebs, 2016; Neal, 2016). Od 2003 r. do 20 marca 2018 r. trwała Misja Organizacji Narodów Zjednoczonych w Liberii (UNMIL). Państwo to, podobnie jak sąsiednie Sierra Leone, ma złożoną sytuację państwową.

Autorka przeanalizowała w pierwszym kwartale 2017 r. publicznie dostępne informacje o wybranych aspektach cyberprzestrzeni Liberii. Obok możliwości korzystania z komunikacji satelitarnej od 2011 r. razem z 23 krajami afrykańskimi Liberia podłączona jest do światowego Internetu przez podmorski kabel o przepustowości 5,12 Tb (rys. 4). Kabel jest fizycznym po-

jedynczym punktem awarii dostępu do Internetu. Według danych z początku 2017 r. Liberia posiadała przyznanych w sumie 22576 numerów IPv4, zatem technicznie jest dobrym „poligonem"? Analiza prawdopodobnej lokalizacji stron czterech usługodawców telekomunikacyjnych Novafone, Lonestar Cell, Cellcom, Libtelco wskazywała, że serwisy informacyjne umieszczone są poza granicami Liberii: przykładowo w Libanie lub Izraelu.



Rysunek 4.
Internet na zachodnim wybrzeżu Afryki

Źródło: TLCAfrika 2011

W pierwszym kwartale 2017 r. oraz czwartym kwartale 2018 r. autorka przeanalizowała prawdopodobną lokalizację wybranych stron www liberyjskich państwowych urzędów i instytucji rządowych. Dostrzegalna jest zmiana usytuowania niektórych portali (tabela 3).

Tabela 3.

Lp.	Nazwa internetowa – czego dotyczy	Lokalizacja 1q 2017	Lokalizacja 4q 2018
1.	http://emansion.gov.lr – The Executive Mansion	Chicago (USA)	Ontario (Canada)
2.	http://www.moci.gov.lr – The Ministry of Commerce and Industry	Chicago (USA)	Ontario (Canada)
3.	http://www.mot.gov.lr – The Ministry of Transport	Chicago (USA)	Ontario (Canada)
4.	http://mod.gov.lr – Ministery of Defence	Chicago (USA)	Ontario (Canada)
5.	http://www.nsa.gov.lr/ – National Security Agency	Chicago (USA)	Ontario (Canada)
6.	http://www.accessbank.com.lr/ – Access Bank	Chicago (USA)	Ontario (Canada)
7.	https://cbl.org.lr – Central Bank of Liberia	Kolokacja Hetzner w Niemczech	Kolokacja Hetzner w Niemczech
8.	http://www.mofa.gov.lr/public2/index.php – MSZ	Kolokacja Hetnzner Niemczech	Ontario (Canada)
9.	http://www.mopt.gov.lr – The Ministry of Posts and Telecommunications	Kolokacja Hetzner w Niemczech	Kolokacja Hetzner w Niemczech
10.	http://www.moj.gov.lr – Ministry of Justice	Hosting w Pittsford w stanie Nowy York (USA)	Hosting w adresacji holenderskiej przez amerykańską firmę.
11.	http://moe.gov.lr – Ministry of Education	USA	Califormia (USA)

Źródło: Opracowanie własne

Usytuowanie stron rządowych poza państwem wiąże się z tym, że znaczna część infrastruktury została zniszczona lub zrabowana w czasie dwóch wojen domowych (1989–1996 i 1999–2003).

Nasuwa się wniosek, że atakiem DoS nie wyrządzono żadnej krzywdy administracji państwowej Liberii, zatem nie mamy tutaj sklonowania sytuacji z Estonii (maj 2007 r.). Atak nie był także wymierzony przeciwko operatorom telekomunikacyjnym. Zatem komu atak pomógł albo zaszkodził?

Barometry HIIK o konfliktach w cyberprzestrzeni

W Barometrze Konfliktów wydawanym przez Instytut Konfliktów Międzynarodowych w Heidelbergu za rok 2017 (HIIK, 2017) napisano, że „Internet stał się integralną częścią codziennego życia. Od sprawdzenia prognozy pogody po uruchomienie sieci energetycznej prawie wszystko w nowoczesnym społeczeństwie wydaje się opierać na funkcjonującej technologii informacyjnej i komunikacyjnej." HIIK zwraca uwagę, że „cyberprzestrzeń oferuje unikalne funkcje, które sprawiają, że jest szczególnie atrakcyjną domeną dla atakujących". Wymieniono trzy cechy: problem z atrybucją, nieistotność odległości geograficznej oraz stosunkowo niskie koszty. „Jeśli urządzenie jest podłączone do Internetu, może zostać zaatakowane z dowolnego miejsca w sieci. To umożliwia atakującym celować w obiekty, których fizycznie nie będą w stanie osiągnąć (…) możliwość uderzenia w dowolne miejsce w podłączonym świecie sprawia, że cyberprzestrzeń jest unikalną domeną" (HIIK, 2017).

Barometry Konfliktów za 2016 r. (HIIK, 2016) oraz za 2017 r. nie wspominają o ataku DoS na Liberię. W raporcie za 2017 r. zwrócono uwagę na domniemanie próby rosyjskiego wpływania na wybory prezydenckie w USA poprzez cyberprzestrzeń.

Raport za 2017 r. zaakcentował zdarzenie z 27 czerwca 2017 r. na Ukrainie spowodowane rozprzestrzenianiem się złośliwego oprogramowania NotPetya, za czym stała Rosja (Gov.UK, 2018; Whitehouse.gov, 2018). Złośliwe oprogramowanie rozprzestrzeniało się nie poprzez podatne kamery CCTV (jak przy Mirai), lecz przez komputery z podatnym oprogramowaniem.

W opinii autorki ucieczka Snowdena, schronienie w Rosji mogły przyczynić się do wzrostu odwagi Rosji w działaniach w cyberprzestrzeni.

Wnioski

Internet rzeczy wpływa na bezpieczeństwo człowieka w sposób pozytywny albo negatywny. Wpływ pozytywny polega głównie na przesuwaniu granic ludzkich możliwości, co dotyczy zwłaszcza niepełnosprawnych lub ludzi starszych. Wpływ negatywny polega na trudnych do przewidzenia skutkach awarii technicznych oraz niewłaściwym wykorzystaniu urządzeń w sposób

jednostkowy lub zmasowany. U źródeł słabych stron jest suma małej świadomości użytkowników, zaniedbań i zaniechań producentów.

Zagęszczające się środowisko Internetu rzeczy wymaga poprawiania świadomości użytkowników w aspektach technicznych posiadanych urządzeń elektronicznych.

Niniejsza wypowiedź nie narusza ekonomicznych lub wizerunkowych interesów żadnej marki. Wypowiedź nie dewaluuje żadnego urządzenia Internetu rzeczy z nazwy lub nazwiska twórcy lub producenta. Przywołane odniesienia mają na celu zobrazowanie i przybliżenie praktycznej problematyki wpływania sztucznego środowiska Internetu rzeczy na bezpieczeństwo człowieka, wobec braku teorii zagadnienia.

Literatura

Publikacje zwarte:

Clausewitz, C. (2017). *Vom Kriege. Vollständige Ausgabe*. Hamburg: Nikol Verlag. ISBN 9783868200010.

Hoeren T., Kolany-Raiser B. (2017). *Big Data in Context Legal, Social and Technological Insights*, Springer (Kindle Edition). ISBN 9783319624617.

Lakomy, M. (2015). *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice: Wydawnictwo Uniwersytet Śląski. ISBN 9788380123571.

Marczyk, M. (2015). *Zagrożenia cyberterrorystyczne obszaru militarnego państwa – wybrane aspekty*. Warszawa: Akademia Obrony Narodowej. ISBN 9788375235067.

Mayer-Schoenberger V., Cukier K., (tł. Głatki M.), (2014). *Big Data, Rewolucja, która zmieni nasze myślenie, pracę i życie*, Warszawa: MT Biznes sp. z o.o. ISBN 9788377465158.

Artykuły

Bognar, E.K. (2018). *Possibilities and security challenges of using IoT for military purposes*. Hadmérnök. sze2018, Vol. 13 Issue 3, p378-390. 13p, Pozyskano (30.11.2018) z http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=132742661&lang=pl&site=ehost-live.

Cha, S. et al. (2018). *Security Evaluation Framework for Military IoT Devices*. Security & Communication Networks, [s. l.], p. 1–12, Pozyskano (30.11.2018) z http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=130502959&lang=pl&site=ehost-live.

Costigan, S.S., Lindstrom, G. (2016). *Policy and the Internet of Things*. Connections (18121098), [s. l.], v. 15, n. 2, p. 9–18, 2016. Pozyskano (30.11.2018) z http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=127235318&lang=pl&site=ehost-live.

De Donno, M. et al. (2018). *DDoS-Capable IoT Malwares: Comparative Analysis and Mirai Investigation*. Security & Communication Networks, [s. l.], p. 1–30, 2018. Pozyskano (30.11.2018) z http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=128054114&lang=pl&site=ehost-live.

Mahlyanov, D. (2018). *Internet of Things – a New Attack Vector for Hybrid Threats*. Information & Security, [s. l.], v. 39, n. 2, p. 175–182, 2018. Pozyskano (02.12.2018) z http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=133174967&lang=pl&site=ehost-live.

Trnka, M., Cerny, T., Stickney, N. (2018). *Survey of Authentication and Authorization for the Internet of Things*. Security & Communication Networks. 6/12/2018, s. 1–17, Pozyskano (29.11.2018) z http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=130114078&lang=pl&site=ehost-live.

Źródła internetowe

Gabbai A. *Kevin Ashton Describes "the Internet of Things"* http://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/ (dostęp: 02.12.2018).

Gartner, *Control Your IoT Destiny,* z http://www.gartner.com/technology/research/internet-of-things/ (dostęp: 02.12.2018).

Goldman J. *Massive DDoS Attacks Disable Internet Access Throughout Liberia,* http://www.esecurityplanet.com/network-security/massive-ddos-attacks-disable-internet-access-throughout-liberia.html .(dostęp: 02.12.2018)

Gov.UK. *Foreign Office Minister condemns Russia for NotPetya attacks,* https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks (dostęp: 02.12.2018).

HIIK 2017. *Conflict Barometer 2017*, https://hiik.de/2018/02/28/conflict-barometer--2017/?lang=en (dostęp: 02.12.2018).

HIIK 2016. *Conflict Barometer 2016*, https://hiik.de/konfliktbarometer/bisherige--ausgaben/ (dostęp: 02.12.2018).

Keränen A., Bormann C. *Internet of Things: Standards and Guidance from the IETF,* https://www.ietfjournal.org/internet-of-things-standards-and-guidance-from-the-ietf/ (dostęp: 02.12.2018).

Krebs B. *Did the Mirai Botnet Really Take Liberia Offline?*, https://krebsonsecurity.com/2016/11/did-the-mirai-botnet-really-take-liberia-offline/ (dostęp: 02.12.2018).

Neal D. *DDoS attack takes out Liberia web access. Mirai continues to cause havoc,* https://www.v3.co.uk/v3-uk/news/2476487/ddos-attack-takes-out-liberia-web-access (dostęp: 02.12.2018).

OWASP. *OWASP Internet of Things Project,* https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project (dostęp: 02.12.2018).

Radhakrishnan R., *IoT: Enterprises and Architecture*, z http://www.slideshare.net/Nibodha/enterprise-architecture-and-iot (dostęp: 02.12.2018).

Ross M. *Kommentar zur IoT-Sicherheit: Europas Verordnung ist zahnlos*, https://www.heise.de/newsticker/meldung/Kommentar-zur-IoT-Sicherheit-Europas-Verordnung-ist-zahnlos-4208938.html (dostęp: 02.12.2018).

TLCAfrika. *CCL Announces the Landing of Liberia's First Fiber Optic Cable System (ACE)*, z http://www.tlcafrica.com/technology_ccl_announces_ace_landing_in_liberia_nov_1_2011 (dostęp: 02.12.2018).

United Nations. *Closure of UNMIL.* Pozyskano (02.12.2018) z https://unmil.unmissions.org

Waqas. *$55 surveillance camera hacked by Mirai botnet within 98 seconds,* https://www.hackread.com/mirai-botnet-hacks-surveillance-camera-in-98-secs/ (dostęp: 02.12.2018)

Whitehouse.gov. *Statement from the Press Secretary*, https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/ (dostęp: 02.12.2018)