KRZYSZTOF GAWKOWSKI

Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej

krzysztof.gawkowski@uth.edu.pl

Wpływ rozwoju Internetu rzeczy na bezpieczeństwo człowieka

The impact of the development of the Internet of Things on human security

STRESZCZENIE

Rewolucja cyfrowa na naszych oczach stała się faktem i od wielu dziesięcioleci nowoczesne technologie stają się katalizatorem zmian i pozwalają na jeszcze szybszy rozwój. Wszechobecny Internet spowodował przenikanie się kultur, obrzędów czy tradycji bez ograniczeń geograficznych i czasowych. Człowiek i maszyna zaczynają żyć w pewnej symbiozie, a im gęstsza jest sieć połączeń między ludźmi i urządzeniami, tym łatwiej włamać się do niej i wykraść dane. Maszyn podłączonych do sieci jest dziś zdecydowanie więcej niż ludzi, a do roku 2020 liczba urządzeń podłączonych do Internetu przekroczy 50 mld. Śmiało możemy mówić o świecie rzeczy, z których człowiek z jednej strony będzie czerpał profity, ale z drugiej musi być czuły na możliwe zagrożenia. Internet rzeczy napędza finanse oraz gospodarkę, służy poprawie opieki zdrowotnej i życia człowieka. Pozwala na lepszą komunikację, logistykę czy transport. Zbierane jednak dane pozwalają również na niekontrolowaną inwigilację, nielegalne gromadzenie informacji czy przejęcie kontroli nad prywatnością. Wraz z rozwojem Internetu rzeczy takie wyzwania stają się coraz bardziej realnymi problemami. Odpowiedzią powinno być wprowadzenie światowych regulacji prawnych, które wyprzedzą zagrożenie i zabezpieczą człowieka przed konsekwencjami, których dziś nawet sobie nie wyobrażamy.

SUMMARY

The digital revolution in front of our eyes has become a reality and for many decades modern technologies have become a catalyst for change and allow for even faster development. The ubiquitous Internet has caused the penetration of cultures, rites or traditions without geographical and temporal restrictions. Man and machine begin

to live in a certain symbiosis, and the denser the network of connections between people and devices, the easier it is to hack into it and steal data. Machines connected to the network today are definitely more than people, and by 2020 the number of devices connected to the Internet will exceed 50 billion. We can boldly speak about the world of things from which a man will profit from profits on the one hand, but on the other, be sensitive to possible threats. The Internet of Things is driving finance and the economy, it is improving human health and life. Allows for better communication, logistics or transport. However, the collected data also allow uncontrolled surveillance, illegal information gathering or taking control over privacy. As the Internet of Things develops, such challenges become more and more real problems. The answer should be the introduction of global legal regulations that will overtake the threat and protect people from the consequences that we can not even imagine today.

Słowa kluczowe: Internet rzeczy, bezpieczeństwo, rozwój, nowe technologie, cyberbezpieczeństwo.

Keywords: Internet of Things, security, development, new technologies, cybersecurity.

Wprowadzenie

Śledząc historię rozwoju technologicznego ludzkości, można śmiało postawić tezę, że wraz z rozwojem cywilizacji bezpieczeństwo przyjmowało różne formy i definicje. Odwieczny postęp technologiczny zawsze powodował, że bezpieczeństwo miało stały związek z zaspokajaniem potrzeb związanych z istnieniem, przetrwaniem czy posiadaniem (Gąska, 2011, s. 72). Człowiek, który ma poczucie braku zagrożeń, bez problemu sięga po to, co daje mu życie, obcy jest mu lęk i czuje się pewnie. W konsekwencji ma odwagę poznawać i odkrywać nowe technologie, które mogą ułatwiać bądź utrudnić jego egzystencję.

Szukając odpowiedzi o wpływ rozwoju technologicznego na bezpieczeństwo człowieka, warto podkreślić, że jest to stan, w którym każda jednostka ma poczucie stabilności, możliwość rozwoju i doskonalenia się (Babcock, 1993, s. 2053–2054). W przypadku innowatorskich technologii podmiotem bezpieczeństwa nie jest jednak tylko człowiek, lecz także całe społeczeństwa i wszelkie instytucje. Do zaspokajania potrzeby bezpieczeństwa dążą zatem wszelkie podmioty, a jego ranga i formy rozwijają się wraz z rozwojem cywilizacji. Mimo że zagrożenie jest nieodłącznym elementem, które towarzyszy bezpieczeństwu, to tylko sytuacje, w których jest ono eliminowane, dają człowiekowi komfort egzystencji i motywują do działania.

Postęp technologiczny doprowadził do tego, że typologia bezpieczeństw jest coraz bardziej uzależniona nie od pojęcia zagrożenia, ale od rozwoju, a zwłaszcza rozbudowy myśli ludzkiej i rozwijających się procesów teleinformatycznych. W obecnej rzeczywistości charakter bezpieczeństwa technologicznego rozumiany jest zatem jako ochrona informacji przed niepożądanym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. Podejmowane są jednocześnie działania ochronne na szczeblu publicznym i prywatnym, które mają za zadanie takie zapewnienie poufności, integralności i dostępności, która pozwoli na niezakłócone korzystanie z dostępnej technologii (Liderman, 2012, s. 24).

Innowacyjne rozwiązania technologiczne są obecnie jednym z najważniejszych elementów wzrostu gospodarczego na całym świecie. Stanowią podstawę złożonych systemów, które napędzają finanse, opiekę zdrowotną, energetykę, logistykę czy transport. Wiele modeli biznesowych opiera się na nieprzerwanej dostępności Internetu i na sprawnym funkcjonowaniu systemów informatycznych. Przerwanie ich lub stały brak dostępu do sieci mogłoby spowodować straty rzędu setek milionów dochodów, a nawet wpływać na niezakłócone życie człowieka.

Internetowa przyszłość

W ciągu ostatnich lat Internet oraz szerzej rozumiana cyberprzestrzeń stały się niezastąpionym elementem życia człowieka i miały bardzo duży wpływ na wszystkie aspekty funkcjonowania społeczeństwa. Codzienne życie, biznes, interakcje społeczne i gospodarka uzależnione są od sprawnie funkcjonujących technologii informacyjno-komunikacyjnych. Otwarta i wolna cyberprzestrzeń usuwa bariery między obywatelami i całymi państwami. Pozwala jednocześnie na interakcję oraz wymianę informacji i pomysłów w skali światowej. Internet stanowi forum wymiany doświadczeń, promuje nowe idee oraz daje jednostkom i czasem całym społeczeństwom szansę na realizację nawet najbardziej wyszukanych idei.

Rozwój cyberprzestrzeni oprócz wielu pozytywnych aspektów niesie również zagrożenia dotychczas nieznane i nieopisane. W latach 2015–2017 na świecie, co roku pojawiało się ponad 50 tys. nowych błędów, które mogły być podstawą uznania jako hakerski atak. Średni czas niezbędny na ich usunięcie wynosił 50 dni, a łączny czas ekspozycji aplikacji zawierających luki podatne na ataki typu „zero day exploit" osiągnął blisko 300 dni. Funkcjonując na co dzień

w ramach wirtualnej rzeczywistości, nie zdajemy sobie sprawy, że codziennie atakowanych jest na świecie 500 tys. stron internetowych i generuje się ponad 30 mld e-maili o charakterze spamu. Eksperci szacują, że w ostatnich latach skradzionych mogło być łącznie prawie 500 mln tożsamości (Internet Security Threat Report, 2016).

Tylko straty finansowe, nie wspominając o problemach społecznych, związane z cyberprzestępczością, są olbrzymie. Center for Strategic and International Studies (CSIS) podaje, że każdego roku działania cyberprzestępców powodują w skali światowej straty w wysokości prawie pół biliona dolarów. W Polsce zgodnie z danymi Głównego Urzędu Statystycznego za rok 2016 ponad 80 proc. gospodarstw domowych ma dostęp do Internetu oraz posiada w domu przynajmniej jeden komputer (GUS, 2016). Z portali społecznościach korzysta 14–15 milionów Polaków, a więc ponad 50 proc. osób posiadających stały dostęp do Internetu (Digital in 2017 Global Overview). Większość z nich zapytana, czy przykłada uwagę do zachowania bezpieczeństwa związanego z użytkowaniem Internetu, odpowiada „nie" i na tle innych krajów europejskich i tak nie wypadamy wcale najgorzej.

Dotychczasowa rozbudowa technologii informacyjno-komunikacyjnych w dużej mierze wywodziła się od ludzi poszukujących wciąż nowych wyzwań i możliwości. Koncepcja rozwoju infrastruktury sieciowej dzięki zaangażowaniu wielu pasjonatów Internetu przyniosła olbrzymie społeczne korzyści. Wśród cyberspołeczności tworzącej środowisko przez wiele lat istniała niewielka część użytkowników, dla której wymiana e-maili, poszukiwanie treści i zdobywanie nowych kontaktów nie wystarczyło. Zaczęli korzystać z sieci jako narzędzia do zdalnego sterowania różnymi obiektami. W tamtym czasie polecenia wysłane przez Internet nie były bardzo skomplikowane. Obecnie wszystkie założenia marzycieli z przeszłości są możliwe do spełnienia, i to bez udziału człowieka. W ciągu najbliższych pięciu lat technologia informatyczna rozwinie się jeszcze bardziej, a wpłyną na to przede wszystkim rozwiązania, które dziś opisywane jako Internet rzeczy (Internet of Things – Strategic Research Roadmap, 2009, s. 8).

Symbioza człowieka i maszyny

Koncepcja Internetu rzeczy pojawiła się w Stanach Zjednoczonych pod koniec w XX wieku. Pierwszym autorem takiej teorii był Kevin Ashton, oznaczając nim tytuł swojej prezentacji dla Procter&Gamble w roku 1999 (Ashton, 2009). Autor podkreślił, że ówczesne komputery, a zatem i Internet, są niemal całkowi-

cie zależne od ludzi, którzy odpowiadają za informacje do nich wprowadzane. Opisał problemy związane z interwencją ludzką w proces wprowadzania danych do sieci, potrzebny do tego duży zakres czasowy oraz często występujące błędy. Tym samym próbował udowodnić, że ludzie nie są najlepszymi podmiotami do rejestrowania i wprowadzania danych do Internetu. Przekonywał jednocześnie słuchaczy o konieczności wyposażenia komputerów w umiejętność samodzielnego gromadzenia informacji o świecie, a w szczególności o poszczególnych produktach. Koncepcja Ashtona zakładała, że myślenie o nowoczesnych technologiach powinno się sprowadzać do umożliwienia komputerom samodzielnego przetwarzania i zbierania danych, a rozwój Internetu rzeczy nie zależy tylko od umiejętności doskonalenia świata, lecz także od naturalnego antropologicznego ograniczenia człowieka, w którym zdolny jest on utrzymywać bezpośredni kontakt z ograniczoną liczbą ludzi (Dunbar, 1998, s. 103).

Internet rzeczy w całej swojej złożoności nie jest więc czymś nowym, a początki samego istnienia Internetu były z założenia elementami, które miały łączyć rządowe i akademickie komputery w celu wymiany danych. Zmiana w rozumieniu potencjału wynikającego z masowej sieci zaszła dopiero w ciągu ostatnich lat, od kiedy istnieje możliwość przyłączania zdalnych i mobilnych urządzeń lub maszyn do sieci. W swojej złożoności Internet rzeczy składa się z sieci połączonych ze sobą komputerów, smartfonów, tabletów, pojazdów, sprzętów AGD i RTV, zabawek, narzędzi medycznych i wielu innych urządzeń wciąż komunikujących się ze sobą i wymieniających informacje. Internet rzeczy jest technologią rozszerzającą działanie Internetu i obejmującą przedmioty codziennego użytku. Symbioza między maszyną a człowiekiem stała się więc faktem i wszystkie przedmioty włączone w krwiobieg wirtualnego świata mogą być zdalnie sterowane i działać jako fizyczne punkty dostępu do usług internetowych (Mattern i Floerkemeier, 2010, s. 1).

Trudno oszacować, kiedy człowiek przekroczył linię demarkacyjną wzajemnej symbiozy z maszyną, ale warto przypomnieć, że w roku 2000 na świecie żyło ponad 6 mld ludzi i tylko 500 mln urządzeń było podłączonych do sieci internetowej. Na przełomie lat 2008 i 2009 liczba urządzeń podłączonych do Internetu po raz pierwszy przekroczyła liczbę mieszkańców ziemi, a w roku 2010 znaczny przyrost użytkowanych smartfonów i tabletów spowodował, że liczba urządzeń podłączonych do sieci wyniosła ok. 12,5 mld. Średnio przypadało więc 1,84 takiego urządzenia na mieszkańca globu, a liczba ludności sięgała 6,8 mld

(Evans, 2011, s. 2). Obecnie szacuje się, że liczba urządzeń podłączonych do globalnej sieci przekracza 25 mld, a do roku 2020 takich urządzeń ma być ponad 50 mld (Vermesan, Friess, Guillemin, Gusmeroli, Sundmaeker, Bassi, Jubert, Mazura, Harrison, Eisenhauer, Doody, 2011, s. 11). Nietrudno policzyć, że średnio ponad sześć urządzeń podłączonych do Internetu będzie przypadało na każdego człowieka, a szacunki te nie uwzględniają gwałtownego postępu i rozwoju kolejnych innowacyjnych technologii.

Prosta analiza powyższych danych wskazuje, że potencjał Internetu rzeczy cały czas rośnie. Dobrze wykorzystany może w znacznym stopniu poprawić sposób życia, uczenia się, pracy czy zabawy. Umożliwi lokalizowanie zagubionych lub skradzionych przedmiotów, zrewolucjonizuje łańcuch dostaw i logistyki oraz ograniczy koszty życia. Równocześnie otaczające nas rzeczy będą zawierały różne informacje, więc i zagrożenia wykorzystania ich niezgodne z przeznaczeniem staną się dużo większe niż obecnie. W celu przygotowania odpowiedniego procesu ochronnego w zakresie bezpieczeństwa Internetu rzeczy warto zastanowić się nad przyjęciem ram międzynarodowej polityki bezpieczeństwa. Takie wytyczne wskazujące rodzaje naruszeń, zawierające scenariusze, które ukazują metody postępowania w sytuacjach kryzysowych oraz prezentujące działania, jakie należy podejmować na przyszłość, byłyby wartością, która w dużym stopniu ograniczałaby ryzyko wystąpienia problemów.

Rozwój technologiczny pędzi jednak nieubłaganie i już dziś urządzenia mogą oddziaływać na siebie często bez udziału człowieka. Koncepcja takiej komunikacji szerzej opisywana jest jako technologia M2M (Machine to Machine) i pozwala na wzajemne przekazywanie zbieranych danych m.in. między komputerami, czujnikami, wbudowanymi procesorami czy urządzeniami mobilnymi (Raymond James & Associates, 2014, s. 3). Struktury Internetu rzeczy i komunikacji M2M są bardzo podobne. Termin Machine to Machine jest skierowany dla bardziej przemysłowych zastosowań, w których ludzie są angażowani w niewielkim zakresie, natomiast szersze pojęcie Internetu rzeczy jest skierowane dla zastosowań konsumenckich. Internet rzeczy będzie stwarzać jednak liczne szanse oraz zagrożenia również i w biznesie. Beneficjentami takiego procesu komunikacji będą m.in. producenci półprzewodników, twórcy zapewniający oprogramowanie infrastruktury, firmy konsultingowe i operatorzy telekomunikacyjni (Vermesan, Friess, Guillemin, Gusmeroli, Sundmaeker, Bassi, Jubert, Mazura, Harrison, Eisenhauer, Doody, 2011, s. 11).

Warto podkreślić, że koncepcja Internetu rzeczy i komunikacja M2M odwołują się do idei, w której rzeczy, szczególnie te codziennego użytku, są odczytywalne, rozpoznawalne, możliwe do zlokalizowania, adresowalne i sterowalne za pomocą Internetu. W dużym skrócie są one zatem w dużej mierze samodzielne, a rozwój komunikacji związanej z Internetem rzeczy będzie napędzany przez praktycznie powszechną dostępność sieci bezprzewodowych i zredukowane koszty komunikacji. Przewiduje się także, że Internet rzeczy będzie częściowo korzystać z rozwiniętej już na potrzeby komunikacji M2M infrastruktury i z dostępnej globalnie sieci łączności (Viswanathan, Lenney, Woysch, 2012, s. 323–324).

Rozbudowa możliwości wykorzystania Internetu rzeczy wydają się praktycznie nieograniczone. Innowacyjne rozwiązania służyć będą na pewno podniesieniu jakości życia ludności, mogą dać impuls dla powstawania nowych przedsiębiorstw, a także na szybszy rozwój wielu istniejących. Potencjał Internetu rzeczy może służyć w kreacji nowych produktów i wpływać na doskonalenie jakości usług. Pamiętając, że siłą napędową łączenia przedmiotów w sieci jest chęć wygenerowania dodatkowych zysków, powstawać będą zapewne też nowe rynki zbytu. Korzyści osiągną także konsumenci, bo dzięki możliwość sprawdzania przez nich istotnych parametrów w czasie rzeczywistym (m.in.: ceny, jakości, specyfikacji technicznej) dotyczących oferowanych przez przedsiębiorców produktów i usług, wzmacniała się będzie wzajemna konkurencja.

Sektor, w którym wykorzystanie Internetu rzeczy już dziś daje realną poprawę bezpieczeństwa człowieka, jest branża zdrowotna. Obecnie jest już możliwe zamontowanie w domu czujników, monitorujących codzienne życie, a dzięki zastosowaniu technologii bezprzewodowego systemu monitorowania zdrowia pacjenta możliwe staje się jego wstępne, zdalne diagnozowanie nawet w domu. Coraz częściej zbierane są też dane medyczne przez czujniki znajdujące się np. w zegarku, przyklejane do powierzchni ciała lub wszczepiony chip. Zastosowanie bezprzewodowego, zdalnego systemu monitorowania parametrów życiowych pacjenta, z wykorzystaniem medycznego sprzętu pomiarowego i transmisji danych daje szanse na przekazania zebranych danych lekarzowi w czasie rzeczywistym i bardzo szybką reakcję zwrotną (Baig i GholamHosseini, 2013, s. 2429). Rewolucjonizuje się również sieć telefonii mobilnej, a konsumenci posługujący się smartfonami, otrzymują interesujące ich informacje na temat wybranych produktów czy usług. Narzędzia Internetu rzeczy wykorzystywa-

ne są już także w nieruchomościach poprzez zdalny odczyt liczników energii elektrycznej czy wody oraz opracowaniu i wdrożeniu koncepcji inteligentnych miast (Gawkowski, 2017, s. 218–219).

Wnioski

Rozwój Internetu rzeczy, jak widać, otwiera wiele możliwości, pozytywnie wpływających na ludzkie życie, pamiętać jednak należy, że tak zaawansowana technologia może być niebezpieczna. Podłączone do Internetu maszyny są zdolne do tworzenia ponad 2,5 tryliona bajtów dziennie. Chcąc w sposób policzalny określić, jaka jest to wielkość, warto wspomnieć, że 90 proc. danych na świecie zostało stworzonych w ciągu ostatnich dwóch lat. Największym wyzwaniem Internetu rzeczy nie będzie zatem przechowywanie tych wszystkich danych, tylko sposób na ich przetwarzanie i generowanie wniosków. Wielkie zbiory danych, czyli big data, wymagają zastosowania wyjątkowych technologii, aby efektywnie przetwarzać duże ilości danych i realizować to akceptowalnym czasie. Ważne jest, aby postęp, już dziś ciężko policzalnych, zastosowań Internetu rzeczy szedł w parze z zaufaniem oraz z zapewnieniem obywatelom gwarancji dotyczących niewykorzystywania przez niepowołane osoby, informacji generowanych w sieci.

Największą rolę w budowaniu wzajemnego zaufania obywatela do Internetu mają jednak struktury państwa i każda osoba korzystająca z zasobów w cyberprzestrzeni musi być świadoma zagrożeń, jakie mogą ją spotkać lub sama może je stworzyć, gdy w nieodpowiedzialny sposób będzie z nich korzystała. Zachowanie w sieci indywidualnej jednostki ma wpływ na bezpieczeństwo pozostałych użytkowników i bez zaufania obywateli do budowanego systemu, nie jest możliwa wzajemna spójna kooperacja. Działania na rzecz bezpieczeństwa Internetu muszą mieć zatem charakter kompleksowy, obejmujący zarówno elementy infrastruktury teleinformatycznej, procedury niezbędne do sprawnego funkcjonowania systemu, jak i zasady dla użytkowników korzystających z tych zasobów. Tylko takie państwa, które nie będą bały się tematu Internetu rzeczy i skrupulatnie podejdą do zapewnienia jego bezpieczeństwa, otworzą nowy horyzont rozwoju technologicznego.

Bibliografia

Ashton K. (2009). *That 'Internet of Things' Thing. In the real world, things matter more than ideas*. RFID Journal.

Babcock P. (1993). *Webster's Third New International Dictionary of the English Language*, Könemann: Published by Merriam-Webster.

Baig M.M., GholamHosseini H. (2013). *Wireless remote patient monitoring in older adults, Engineering in Medicine and Biology Society (EMBC)*. Osaka, Japan: 35th Annual International Conference of the IEEE.

Brodie B. (1995). *Strategy as a Science*, "World Politics" 1, 949, s. 477.

Levy M.A., *Is the Environment a nationalSecurity Issue?*, International Security.

Cygan T. (2016). *Podręcznik Administratora Bezpieczeństwa Informacji*. Wrocław: Presscom.

Dunbar R. (1998). *Grooming, gossip, and the evolution of language*. Cambridge, MA: Harvard University Press.

Evans D. (2011). *The Internet of Things – How the Next Evolution of the Internet Is Changing Everything*. CISCO Internet Business Solutions Group (IBSG). White Paper.

Gawkowski K. (2017). *Administracja samorządowa w teorii i praktyce*. Toruń: Wydawnictwo Adam Marszałek.

Gąska M. (2011). *Problematyka bezpieczeństwa społeczności lokalnych*, [w:] *Zarządzanie bezpieczeństwem na poziomie lokalnym*, Zamość: WSH-E.

Goban-Klas T. (1999). *Społeczeństwo informacyjne i jego teoretycy*, [w:] *W drodze do społeczeństwa informacyjnego,* red. J. Lubacz. Warszawa: Instytut Problemów Współczesnej Cywilizacji.

Karimi K., Atkinson G. (2013). *What the Internet of Things (IoT) Needs to Become a Reality*, FreeScale and ARM, Austin, USA: White Paper.

Koziej S. (2016). *Transsektorowy charakter cyberbezpieczeństwa. Strategiczne wyzwania dla Polski i NATO.* Warszawa: IBK.

Liderman K. (2012). *Bezpieczeństwo informacyjne*. Warszawa: Wydawnictwo Naukowe PWN.

Mattern F., Floerkemeier C. (2010). *From the Internet of Computers to the Internet of Things*. Zurich.

Wiśniewski B., Zalewski S., Podleś D., Kozłowska K. (2004). *Bezpieczeństwo wewnętrzne Rzeczypospolitej Polskiej*. Warszawa: Akademia Obrony Narodowej.

Smith I.G. (2012). *The Internet of Things 2012*. Halifax: New Horizons IERC.

Vermesan O., Friess P., Guillemin P., Gusmeroli S., Sundmaeker H., Bassi A., Jubert I.S., Mazura M., Harrison M., Eisenhauer M., Doody P. (2011). *Internet of Things Strategic Research Roadmap*. Berlin: IERC Cluster SRA.

Viswanathan H., Lenney M., Woysch G. (2012). *IoT – Going horizontal to win in verticals!*, [w:] *'The Internet of Things – Where it is going?' A Global Overview*, [w:] I.G. Smith (ed.), *The Internet of Things 2012 New Horizons*. Oslo, Norway: IERC.

Raporty i analizy

Internet Security Threat Report. (2016). Mountain View, USA: Symantec.

Internet of Things – Strategic Research Roadmap. (2014). Oslo, Norway: IERC.

Raymond James & Associates, The Internet of Things – A Study in Hyde. (2014). St. Petersburg, USA: Reality, Disruption, and Growth.

Społeczeństwo informacyjne w Polsce w 2016 r. (opracowanie sygnalne). (2016). Warszawa: Główny Urząd Statystyczny.

Źródła internetowe

Digital in 2017 Global Overview, We Are Social and Hootsite, Pozyskano (28.11.2017). https://www.slideshare.net/wearesocialsg/digital-in-2017-global-overview?ref=http://wearesocial.com/uk/blog/2017/01/digital-in-2017-global-overview

Ericsson Mobility Report on the pulse of the networked society 2016 (dostęp: 28 listopada 2017 r.). https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf (dostęp: 27 listopada 2017 r.).

https://www.csis.org/analysis Pozyskano (dostęp: 27 listopada 2017 r.).

https://www.iotsecurityfoundation.org (dostęp: 27listopada 2017 r.).