Biuletyn Ośrodka Studiów nad Wyzwaniami Cywilizacyjnymi

CBB ASzWoj

Numer 5 | czerwiec 2017

W numerze:

- Amerykańscy badacze przeanalizowali archiwum **chińskiego aparatu propagandy internetowej** wymierzonego we własnych obywateli. Analiza daje wgląd w szczegóły jego organizacji i skalę działania.
- Wdrażany w Chinach **cyfrowy system oceny firm i obywateli** obejmie także działające w tym kraju przedsiębiorstwa zagraniczne.
- **Połączenie rzeczywistości rozszerzonej i wirtualnej** oraz technologii „**czytania myśli**" **z usługami Facebooka** daje nowe możliwości kulturowego i politycznego wpływu na społeczeństwa.
- **„Wirtualni asystenci",** coraz powszechniejsi **w urządzeniach RTV/AGD**, mogą generować **zagrożenie dla prywatności** oraz **ingerować w interakcje społeczne użytkowników**.
- **Zabawki interakcyjne** mogą pełnić **funkcje szpiegujące**. Jedna z takich zabawek została zakazana w Niemczech.
- Postęp w **technologiach nadzoru** – pojawienie się możliwości **identyfikacji twarzy na podstawie** analizy **aktywności mózgu**.
- Kanadyjski start-up zademonstrował wydajną **technologię imitowania głosu dowolnej osoby** na podstawie bardzo krótkiego nagrania jej wypowiedzi.
- Rząd USA zaakceptował procedurę analizy **aktywności w mediach społecznościowych** osób aplikujących o wizy.
- Wnioski z wyborów w USA – cyfryzacja procesu wyborczego może zwiększać ryzyko **podważania wyników wyborów**.
- W fazę testów klinicznych wejdzie w 2018 r. nowa, wywodząca się z kardiochirurgii, technologia **sterowania maszynami za pomocą mózgu**.
- Postęp w tworzeniu **hybrydy owada i maszyny** za pomocą przejęcia kontroli nad systemem nerwowym zwierzęcia.
- W **Szwecji** podjęto pierwsze próby chipowania osób, w celu ułatwienia im dostępu do różnych usług.
- **Google sprzedaje** Japończykom **wiodące w robotyce firmy**: Boston Dynamics i Schaft.
- Microsoft oficjalnie potwierdził **wyciek kodu źródłowego Windowsa 10**. Skutkiem wycieku może być wzrost podatności tego systemu na ataki hakerskie.

Redakcja biuletynu:

Zespół OSWC

Ośrodek Studiów nad Wyzwaniami Cywilizacyjnymi
Centrum Badań nad Bezpieczeństwem
Akademia Sztuki Wojennej
al. gen. A. Chruściela „Montera” 103
00-910 Warszawa

Tel.: 261-813-252
E-mail: m.gurtowski@akademia.mil.pl

Spis treści

Amerykańscy uczeni opublikowali analizę na temat zasięgu i sposobu zorganizowania chińskiej propagandy internetowej skierowanej do mieszkańców ChRL

KOMUNIKAT

27 czerwca 2017. W 2014 roku anonimowy bloger o pseudonimie Xiaolan upublicznił archiwum korespondencji elektronicznej, wysyłanej z konta Biura Propagandy Internetowej, sekcji departamentu propagandy Zhanggong, dystryktu miasta Ganzhou zlokalizowanego w chińskiej prowincji Jiangxi. Jest to unikalny materiał, który umożliwił zespołowi amerykańskich badaczy (m.in. z Harvardu i ze Stanford)[1] systematyczne oszacowanie skali i zasięgu działań tzw. partii pięćdziesięciocentowców (*50c party*, dalej 50c). W ten sposób określa się w dyskursie publicznym w USA hipotetyczną grupę „internetowych trolli" wynagradzanych przez chiński rząd w zamian za publikowanie antyamerykańskich i prochińskich postów. Samo określenie wzięło się od przekonania, że za każdy post członkowie 50c otrzymują równowartość 50 centów. Na podstawie informacji, które wyciekły, szacuje się, że grupa 50c miałaby liczyć aż 2 mln Chińczyków.

Amerykańscy badacze wskazują, że z analizy upublicznionego archiwum e-mailowego wyłania się obraz zdecydowanie odbiegający od niektórych rozpowszechnionych wyobrażeń na temat sposobu organizacji pracy farm trolli. Po pierwsze, trolle nie są opłacane za publikowanie postów, ale są to etatowi urzędnicy chińscy wykonujący na co dzień zwykłą pracę biurową. Zebrane materiały sugerują, że praca propagandowa jest integralną częścią ich obowiązków służbowych. Po drugie, działania propagandowe nie są prowadzone w sposób ciągły, lecz skokowo. Urzędnicy dostają dyspozycje, by publikować propagandowe posty w chińskich mediach społecznościowych bezpośrednio przed dniami wolnymi oraz rocznicami, które mogłyby zostać uznane za okazję do organizowania protestów. Urzędnicy są również oddelegowani do pracy propagandowej w sytuacji, gdy pewne niebezpieczne dla stabilności społecznej treści zaczynają się rozprzestrzeniać w mediach społecznościowych w trybie wirusowym. Po trzecie, propagandowe posty nie mają postaci entuzjastycznych głosów poparcia dla władzy, ale stanowią raczej próby przekierowania uwagi społecznej na kwestie bezpieczne i apolityczne. Archiwum zawiera informacje na temat pojedynczego dystryktu, jednak umożliwia ono oszacowanie skali propagandy internetowej w Chinach na zasadzie ekstrapolacji. I tak według szacunków badaczy chińscy urzędnicy publikują w mediach społecznościowych 448 mln komentarzy rocznie.

Komentarz: Skala chińskiej propagandy internetowej oraz sposób jej funkcjonowania sprawiają, że mamy tu do czynienia z o wiele większym potencjałem dla działań aktywnych niż w przypadku Rosji. Bariera kulturowo-językowa sprawia, że polskie media społecznościowe nie wydają się być istotnie zagrożone w chwili obecnej. Niemniej, w kontekście planów rozwojowych Chin na pewno nastąpi zwiększenie działań propagandowych w krajach Europy Środkowo-Wschodniej. **[10/8]**

[1] G. King, J. Pan, M. E. Roberts, *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument*, 9.04.2017, https://gking.harvard.edu/files/gking/files/50c.pdf [odczyt: 27.06.2017].

Chiński system cyfrowej oceny firm i obywateli wpłynie na warunki działalności polskich przedsiębiorstw w tym kraju

KOMUNIKAT

27 czerwca 2017. We wcześniejszych analizach opisywaliśmy genezę, zasady funkcjonowania i możliwe konsekwencje społeczno-polityczne testowanego obecnie systemu zintegrowanej, elektronicznej oceny obywateli Chin[2]. W dniu 24 maja br. ukazała się analiza niemieckiego ośrodka studiów chińskich Mercator Institute for China Studies (MERICS) z Berlina, w której przedstawiono konsekwencje wdrażania tego systemu dla niemieckiego biznesu[3]. Zgodnie z analizą MERICS także zagraniczni przedsiębiorcy obecni na chińskim rynku zostaną – najpóźniej w roku 2020 – objęci tym systemem. Będzie to miało bezpośrednie i znaczące konsekwencje dla warunków prowadzenia przez nich działalności gospodarczej.

Osobną uwagę warto zatem poświęcić konsekwencjom wdrożenia systemu dla polskich firm działających na rynku chińskim. Z raportu MERICS wynika, że system będzie miał silny i bezpośredni wpływ na funkcjonowanie zagranicznych przedsiębiorstw w Chinach, w szczególności w pewnych obszarach, np. e-handlu czy produkcji samochodów. Wśród kluczowych sektorów, dla których władze chińskie opracowały szczegółowe plany systemu oceny, są: budownictwo, e-handel, energetyka, hutnictwo stali, logistyka (w tym usługi kurierskie), media, produkcja żywności i leków, rolnictwo, sektor ubezpieczeniowy, transport i turystyka. Podmioty, które dostaną wysokie noty, będą mogły liczyć na zmniejszenie zakresu państwowych regulacji. Jednakże nawet relatywnie drobne naruszenia, takie jak opóźnienie w realizacji płatności, chwilowe przekroczenie limitu zużycia prądu czy nagromadzenie pewnej liczby wykroczeń drogowych, będą automatycznie (natychmiast i bez skutecznej procedury odwoławczej) skutkować obniżeniem oceny i wynikającymi z tego sankcjami.

Analitycy MERICS prognozują, iż zamiast jednolitego systemu oceny funkcjonować będzie wiele równoległych systemów branżowych. Kluczowe znaczenie ma jednak fakt, iż firmy zagraniczne będą podlegać identycznym regulacjom, co podmioty chińskie. Z jednej strony, system ma pozwolić na zmniejszenie skali korupcji i oszustw, lepszą ocenę wiarygodności partnerów biznesowych i zwiększenie przejrzystości obrotu handlowego. Mogłoby to przyczynić się do polepszenia sytuacji podmiotów zagranicznych. Z drugiej strony, autorzy analizy wskazują, iż wdrożenie systemu zrodzi m.in. ryzyko trudno uchwytnego (bo ukrytego w niejawnych algorytmach systemu oceny) faworyzowania podmiotów chińskich[4]. Powodzenie systemu mogłoby też dać

[2] Zob. Analiza pt. *Chiński system zautomatyzowanej oceny obywateli: perspektywa cyfrowego totalitaryzmu*, „Biuletyn Ośrodka Studiów nad Wyzwaniami Cywilizacyjnymi CBB ASzWoj" nr 2, marzec 2017.

[3] M. Meissner, *China's social credit system*. *A big-data enabled approach to market regulation with broad implications for doing business in China*, 24.05.2017, https://www.merics.org/fileadmin/user_upload/downloads/China-Monitor/merics_ChinaMonitor_39_englisch_Web.pdf [odczyt: 12.06.2017].

[4] M. Meissner, *China's social credit system*, s. 9.

Chinom wielką przewagę konkurencyjną na globalnym rynku, w tym zdolność do niemal natychmiastowego reagowania na nowe trendy i zjawiska. Równie wielkie jest jednak ryzyko ręcznego sterowania procesami rynkowymi za pomocą nowego narzędzia, co mogłoby m.in. prowadzić do zmuszania przez władze firm do podejmowania decyzji nieracjonalnych rynkowo[5]. Istnieje także ryzyko zmuszania firm do udostępniania gromadzonych przez siebie danych, na potrzeby ich wykorzystania do budowy systemu oceny (przed takim dylematem stoją chińskie giganty internetowe – Alibaba oraz Baidu[6]). Wreszcie, już dziś docierają sygnały o masowym fałszowaniu danych (w tym przypadku – dotyczących wielkości emisji CO^2), które są potem przedmiotem zautomatyzowanej oceny[7]. Do tego dochodzi ryzyko zhackowania całego systemu. Wszystko to sprawia, iż system oceny może negatywnie wpłynąć na stabilność warunków prowadzenia działalności gospodarczej w Chinach.

Rekomendacje: Warto rozważyć zlecenie polskim placówkom dyplomatycznym w Chinach monitoring rozwoju systemu oceny obywateli i przedsiębiorstw pod kątem potencjalnego wpływu na warunki funkcjonowania polskich firm w tym kraju. **[5/4]**

[5] Przykładem jest już obecnie prowadzona polityka, zgodnie z którą większe firmy są zobowiązane do zakupu pewnej ilości samochodów elektrycznych. Tamże, s. 9.

[6] Tamże, s. 8.

[7] Y. Suwen, Z. Tailai i L. Rongde, *Northern China Chokes on Fake Emissions Data, 06.04.2017,* http://www.caixinglobal.com/2017-04-06/101075101.html [odczyt: 27.06.2017].

Facebook pracuje nad technologią odczytywania myśli

KOMUNIKAT

9 maja 2017. W wypowiedzi z dnia 13 kwietnia br., opublikowanej na FB, szef portalu Mark Zuckerberg, ujawnił pewne istotne informacje dotyczące kierunków rozwoju firmy, w tym zwłaszcza jej jednostki badawczej znanej jako Building 8 (B8). Według deklaracji Zuckerberga, zespół ten pracuje m.in. nad rzeczywistością poszerzoną i wirtualną oraz sztuczną inteligencją, a także nad technologią odczytywania myśli (tj. wewnętrznego dialogu)[8]. Chce tego dokonać przy pomocy nieinwazyjnych sensorów, które przetwarzają dialog wewnętrzny człowieka w tekst[9]. Zespół utworzono w kwietniu 2016 roku; według oficjalnie dostępnych informacji obecnie zatrudnia on kilkudziesięciu naukowców. Na stronie zespołu można znaleźć ogłoszenia o pracę dla kolejnych 42 specjalistów (m.in. od neuroobrazowania oraz inżynierów od interfejsów mózg-komputer)[10]. Szefem zespołu jest Regina Dugan, b. dyrektor DARPA, a także – b. dyrektor Advanced Technology and Projects group w Google[11]. Zapowiedziała ona, że spodziewa się, iż w ciągu 2 lat zespołowi uda się stworzyć urządzenie (w rodzaju czepka) zdolne do zapisywania 100 „myślanych" słów na minutę.

Komentarz: Entuzjastyczne komunikaty członków zespołu oraz samego Zuckerberga, na temat spodziewanych postępów i przełomów w dziedzinie tekstowego zapisu myśli przy pomocy implantów należy traktować z ostrożnością. Na łamach „MIT Tech Review" kwestionuje się nie tyle same rewolucyjne zapowiedzi obu firm, ile przede wszystkim realistyczność podanych dat[12]. Działania – faktyczne i PR-owe – Facebooka należy postrzegać także jako posunięcia w wyścigu o tytuł największego innowatora z firmą Elona Muska Neuralink, która pracuje nad technologią o zbliżonych funkcjach[13].

---

[8] M. Zuckerberg, M.Schroepfer, 13.04.2016, https://www.facebook.com/zuck/posts/10102777889538891 [odczyt: 9.05.2017].

[9] A. Heath, *Facebook's secretive and ambitious hardware group is preparing for its debut next month*, 19.03.2017, http://businessinsider.com.pl/international/facebooks-secretive-and-ambitious-hardware-group-is-preparing-for-its-debut-next/sm72c65 [odczyt: 09.05.2017].

[10] https://www.facebook.com/careers/teams/building8/ .

[11] Warto przypomnieć, że DARPA prowadzi tego typu badnia od lat 70. XX wieku, zaś od roku 2009 realizowała projekt „Silent Talk", który miał umożliwić zdalne odczytywanie pewnego zasobu podstawowych słów używanych przez żołnierzy amerykańskich na polu walki poprzez zdalny odczyt fal elektromagnetycznych mózgu. Opis projektu: *Research, development, test and evaluation, defense-wide, Volume 1 – Defense Advanced Research Projects Agency, UNCLASSIFIED Approved for Public Release; Distribution Unlimited,* http://www.darpa.mil/attachments/(2G7)%20Global%20Nav%20-%20About%20Us%20-%20Budget%20-%20Budget%20Entries%20-%20FY2010%20(Approved).pdf s. 17.

[12] A. Regalado, *With Neuralink, Elon Musk Promises Human-to-Human Telepathy. Don't Believe It*, 22.04.2017, https://www.technologyreview.com/s/604254/with-neuralink-elon-musk-promises-human-to-human-telepathy-dont-believe-it/ [odczyt: 24.04.2017].

[13] Zob. Komunikat, *Nowa inicjatywa Elona Muska otwiera perspektywę szybkiego upowszechnienia technik wspomagania pracy mózgu*, „Biuletynu OSWC" nr 3/2017, s. 14-15.

W obu przypadkach planuje się najpierw zastosowania we wspomaganiu osób niemych oraz w terapii innych schorzeń. W dalszej kolejności należy spodziewać się zastosowań militarnych i wywiadowczych, nowych technik przesłuchań, wykrywania kłamstw (np. osób publicznych czy kandydatów na ważne stanowiska). Warto podkreślić, że zespół B8 planuje produkcję urządzeń (*hardware*), co jasno wskazuje na chęć wyjścia Facebooka poza sferę działań właściwych dla medium społecznościowego, w tym m.in. na dążenie do dywersyfikacji przychodów. Sukces zespołu B8 (oraz innych, które pracują nad zbliżonymi problemami) stworzy nowe zagrożenia dla prywatności. Jak dotąd, umysł zapewniał człowiekowi przestrzeń wolności nawet w konfrontacji z totalitarnymi reżimami. Obecnie zaczyna się debata nad prawami człowieka w erze, gdy realne staje się dosłowne „hakowanie umysłu". W ramach tej debaty proponuje się m.in. kodyfikację nowych praw człowieka, w tym „prawa do prywatności umysłu" (czyli ochrony przed wykradaniem informacji z umysłu) oraz „prawa do integralności umysłowej" (czyli ochrony przed ingerencją w umysł)[14].

Rekomendacje: Należy śledzić przebieg prac badawczych nad technologią zdalnego lub inwazyjnego odczytu myśli. Należy również monitorować przebieg dyskusji i prac legislacyjnych nad prawnym uregulowaniem tych technologii, a także środkami prewencyjnymi (np. w kontekście ochrony kluczowych osób w państwie). W bliskiej przyszłości może okazać się konieczne podjęcie własnych prac legislacyjnych. **[5/12]**

[14] M. Ienca i R. Andorno, *Towards new human rights in the age of neuroscience and neurotechnology*, „Life Sciences, Society and Policy" (2017) 13:5. Autorzy proponują przyjęcie czterech nowych praw człowieka: prawo do wolności poznawczej, prawo do prywatności umysłu (ochronę przed wykradaniem informacji z umysłu), prawo do integralności umysłowej (ochronę przed ingerencją w umysł) oraz prawo do psychicznej ciągłości.

Rozszerzona rzeczywistość w mediach społecznościowych narzędziem wpływu politycznego i kulturowego

KOMUNIKAT

27 maja 2017. Mark Zuckerberg, prezes Facebooka pokazał, jak serwis społecznościowy będzie działał z wykorzystaniem technologii rozszerzonej rzeczywistości i wirtualnej rzeczywistości (VR, Virtual Reality). Pokaz miał miejsce podczas konferencji Oculus Connect dotyczącej przyszłości VR i zastosowań przygotowanych przez Oculusa, firmę, którą Facebook kupił za 2 mld dolarów w 2014 roku[15].

Wirtualna rzeczywistość jest od lat postrzegana jako jeden z ważniejszych etapów w rozwoju przemysłu rozrywkowego**.** Jednakże, jak wskazują niektóre badania, w praktyce użytkownicy dość szybko odczuwają dyskomfort i samotność wynikającą[16] ze specyfiki urządzenia, co ostatecznie prowadzi do mniejszej jego popularności, niż można by się tego spodziewać. Prezes Facebooka podczas swojej prezentacji udowadniał, że VR nie musi być już dłużej takim „izolującym doświadczeniem". Połączenie urządzeń i koncepcji VR ze światem portalu społecznościowego ma dać szansę, zdaniem Zuckerberga, na „spotykanie się" ze znajomymi, którzy znajdują się od nas fizycznie daleko. VR ma imitować wrażenie fizycznego kontaktu z żywym człowiekiem, a nie jak dotąd, tylko z jego profilem i jego „tablicą" na FB.

Propozycja i wizja Facebooka łatwo może stać się czymś, co organizuje społeczne zachowania milionów osób. I może stać się narzędziem jeszcze silniej oddziałującym na sposób życia, reakcje, emocje i wreszcie na decyzje milionów ludzi na świecie.

Jest prawdopodobne, że prócz zastosowania w sferze rozrywki, wirtualna rzeczywistość stanie się narzędziem silniejszego, bo dodatkowo bezpośrednio silnie stymulującego zmysły, wpływu kulturowego oraz politycznego. Dzięki nowemu sposobowi bodźcowania miliony osób na świecie (w tym i w Polsce) mogą stać się podatne na oferowane w nowej rzeczywistości idee i wartości. Wreszcie, rozszerzona rzeczywistość może faktycznie prowadzić do wyłączenia części osób ze swoich naturalnych wspólnot na rzecz grup wirtualnych, np. o antysystemowym charakterze. Osoby te mogą dokonać samo-wykluczenia ze swoich politycznych przynależności i ich norm oraz wartości, ale jednocześnie stać się jeszcze bardziej podatne na sygnały płynące z grup wirtualnych.

Wnioski:

1. Rozwój VR w połączeniu z portalami społecznościowymi stanowi nowe wyzwanie dla tego wymiaru polityki, który polega na wywieraniu wpływu na duże zbiorowości.

[15] A. Perry, *Zobacz, jak będzie wyglądał Facebook w wirtualnej rzeczywistości*, 7.10.2016, http://businessinsider.com.pl/technologie/nowe-technologie/facebook-w-wirtualnej-rzeczywistosci-oculus-connect-3/cb49rtj [odczyt: 29.05.2017].

[16] A. Hines, *Virtual retail-ity The strange, lonely world of virtual shopping in China*, 11.11.2016, https://news.vice.com/story/alibaba-vr-shopping-buy-singles-day [odczyt: 29.05.2017]; S. Ranger*, VR is spectacular but lonely: Here's how it needs to change to succeed*, 21.03.2017, http://www.zdnet.com/article/vr-is-spectacular-but-lonely-heres-how-it-needs-to-change-to-succeed/ [odczyt: 29.05.2017].

Ośrodki kreujące politykę w wielu krajach w zasadzie całkiem niedawno zdobyły kompetencje w zakresie mediów społecznościowych, tymczasem nowa technologia wymaga rozbudowy wiedzy i narzędzi dostosowanych do rozszerzonej rzeczywistości.

2. Rozszerzona rzeczywistość może kierować komunikację w zakresie polityki w stronę jeszcze większej emocjonalności, osłabiając starą, ale jeszcze niekiedy aktualną ideę działań politycznych opartych o siłę racjonalnej argumentacji.

Rekomendacja. Zjawisko powinno być pilnie monitorowane w zakresie możliwości oferowanych klientom, tak aby instytucje państwa były gotowe do użycia (ewentualnie blokowania) nowych kanałów komunikacji, zanim zostaną one przejęte np. przez grupy antysystemowe. **[6/3]**

Inteligentne głośniki Amazon Echo – wizja urządzenia podsłuchowego w każdym pomieszczeniu

ANALIZA

22 maja 2017. Firma Amazon wprowadziła na rynek nowy model wirtualnego asystenta Echo Show. Perspektywa szybkiego upowszechnienia urządzeń tego typu stwarza nowe zagrożenia dla prywatności, a także – co mniej oczywiste i rzadziej wskazywane – ingerencji w interakcje społeczne użytkowników.

Od kilku lat szereg firm rozwija technologie tzw. wirtualnych asystentów w postaci oprogramowania instalowanego na komputerach osobistych lub smartfonach. Apple proponuje Siri, Microsoft – Cortanę zaś Google – Google Now, a następnie (od listopada 2016) Google Home. Począwszy od roku 2016 kilka firm wprowadziło na rynek fizyczne urządzenia przypominające głośniki, wyposażone w funkcje asystentów.

Najnowszy model Amazon Echo Show posiada także kamerę i wyświetlacz LCD. Urządzenie potrafi m.in. czytać audiobooki, opowiadać bajki i żarty, obsługiwać kalendarz (zapisywać terminy i przypominać o spotkaniach), prowadzić listę zakupów oraz dokonywać zakupów online. Posiada też funkcje wyszukiwarki internetowej, kontroli oświetlenia w pomieszczeniu, odtwarzania muzyki; pełna lista „umiejętności" urządzenia („skills") liczy ok. 7000 pozycji[17]. Amazon wynajął satyryków z portalu The Onion oraz twórców filmów ze studia Pixar, aby opracowali dla asystenta „osobowość". Asystentka Alexa (posługująca się głosem żeńskim) potrafi zmieniać ton głosu. Ma to umożliwiać nawiązywanie przez użytkowników psychicznych relacji z urządzeniem, a docelowo przywiązywać emocjonalnie do produktu. W oficjalnej reklamie produktu asystentkę określana się mianem członka rodziny[18].

Komentarz: Rozwój Internetu Rzeczy daje firmom zajmującym się gromadzeniem i przetwarzaniem *Big Data* nowe możliwości pozyskiwania danych. Amazon sugeruje umieszczenie Echo w każdym domu, a nawet w każdym pomieszczeniu. Oznaczałoby to pokrycie budynku szczelną siecią czujników, które potencjalnie umożliwią podsłuchiwanie użytkowników.

Urządzenie znajduje się domyślnie w trybie czuwania i jest aktywowane komendą głosową (np. „Alexa!"). Rozpoczyna wówczas rejestrowanie i rozpoznawanie dźwięków; wszelkie zapytania są rejestrowane na koncie użytkownika i zapisywane w chmurze. Teoretycznie mikrofon można wyłączyć. Komentatorzy wskazują jednak na ryzyko złamania zabezpieczeń i zdalnego aktywowania funkcji nagrywania, tak jak jest to możliwe w przypadku niektórych telewizorów marki Samsung. Nie można też wykluczyć, że urządzenie błędnie zinterpretuje jakieś słowo jako komendę aktywizującą i rozpocznie nagrywanie bez wiedzy użytkownika. Czyni to z urządzenia potencjalnie ważne źródło danych wywiadowczych. Obecnie toczy się sprawa, w której amerykańska policja wystąpiła do Amazona o udostępnienie nagrań i danych

[17] *The 2017 Voice Report*, VoiceLab, https://s3-us-west-1.amazonaws.com/voicelabs/report/vl-voice-report-exec-summary_final.pdf, s. 8 [odczyt: 22.05.2017].

[18] Amazon, *Introducing the all-new Echo Dot,* 16.09.2016, https://www.youtube.com/watch?v=hPXS7rC1PWo [odczyt: 22.05.2017].

z głośników w sprawie o morderstwo z roku 2015[19]. Amazon początkowo odmówił, niedawno jednak dane udostępnił[20]. Wyrok sądu jeszcze nie zapadł, nie wiemy więc, czy i w jakim zakresie sąd wykorzysta dane z Echo.

Zestaw głośników kosztuje ok. 180 dolarów. Otwiera to perspektywę jego szybkiego upowszechnienia. Urządzenie nie jest bezpośrednio dostępne w Polsce, ale należy się spodziewać, że wkrótce to się zmieni. Prognozuje się, iż w 2017 roku przynajmniej 60,5 mln Amerykanów (czyli ponad 20% populacji) użyje jakiegoś aktywowanego głosem urządzenia (poza smartfonami) przynajmniej raz w miesiącu[21]. Według niektórych ocen, aktualnie w USA w użyciu jest od 7 do 11 mln takich urządzeń[22]. Przewiduje się, że liczba ta w najbliższym czasie będzie dynamicznie wzrastać, zaś obsługa głosowa stanie się dominującym sposobem interakcji człowieka z urządzeniami różnego typu[23].

Aktualnie, 70% rynku wirtualnych asystentów kontroluje Amazon[24]. Firma ta kieruje się strategią marketingową, polegającą na początkowym ograniczaniu możliwości zakupu jedynie do wybranych („zaproszonych") osób. Ma to pomóc zwiększyć postrzeganą atrakcyjność produktu. Ceny urządzeń mogą wkrótce znacząco spaść, gdyż szykuje się wojna pomiędzy Amazon, Apple, Google i Microsoft o to, kto przejmie kontrolę nad naszą „kuchnią, łazienką i sypialnią"[25].

W Polsce przeważa pozytywna recepcja urządzenia. Głosy krytyczne koncentrują się raczej na niedoskonałościach technicznych, np. nieznajomości języka polskiego (na razie komendy trzeba wypowiadać po angielsku)[26], braku precyzji wyszukiwania, czy

---

[19] B. Heater, *After pushing back, Amazon hands over Echo data in Arkansas murder case*, 7.03.2017, https://techcrunch.com/2017/03/07/amazon-echo-murder/ [odczyt: 22.05.2017].

[20] L. Brandom, *How much can police find out from a murderer's Echo*? 06.01.2017, https://www.theverge.com/2017/1/6/14189384/amazon-echo-murder-evidence-surveillance-data [odczyt: 22.05.2017].

[21] Tamże.

[22] *Amazon has sold more than 11 million Echo devices, Morgan Stanley says*, http://www.seattletimes.com/business/amazon/amazon-has-sold-more-than-11-million-echo-devices-morgan-stanley-says/ [odczyt: 22.05.2017].

[23]A. Marchick, *The 2017 Voice Report by VoiceLabs*, 15.01.2017, http://voicelabs.co/2017/01/15/the-2017-voice-report/ [odczyt: 15.05.2017].

[24] S. Perez, *Amazon to control 70 percent of the voice-controlled speaker market this year*, 2017.05.08, https://techcrunch.com/2017/05/08/amazon-to-control-70-percent-of-the-voice-controlled-speaker-market-this-year/ [odczyt: 22.05.2017]. Na drugim miejscu plasuje się Google Home, z udziałem w amerykańskim rynku szacowanym na ok 24%. Warto podkreślić, że konsument, który zakupi jedno urządzenie interaktywne w rodzaju Amazon Echo, z dużym prawdopodobieństwem także inne urządzenia z dziedziny IoT wybierze u tego samego producenta. Natura tego rynku sprzyjać będzie koncentracji i monopolizacji. Zob. tamże.

[25] Voicelabs, *The 2017 Voice Report*, 2017, https://s3-us-west-1.amazonaws.com/voicelabs/report/vl-voice-report-exec-summary_final.pdf, s. 5, [odczyt: 15.05.2017].

[26] *Amazon Echo: Jak rozmawiać z Alexą*, „Komputer Świat" 3/2017, 25.02.2017, http://www.komputerswiat.pl/artykuly/redakcyjne/2017/02/amazon-echo-jak-rozmawiac-z-

– w przypadku polskich internautów – nieznajomości polskiego kontekstu (np. brak precyzji w podawaniu pogody dla polskich miejscowości)[27]. Pomija się na ogół lub zbywa kwestie zagrożenia dla prywatności.

Inne źródło zagrożeń ma charakter bardziej ulotny i mniej bezpośredni, ale jednocześnie znacznie bardziej fundamentalny niż samo ryzyko bycia podsłuchanym. Dziennikarze testujący urządzenie relacjonują przypadki „ingerencji" urządzenia w normalne interakcje mieszkańców domu[28]. Ingerencje te na ogół wynikają z niewłaściwego zrozumienia komend głosowych, ale obrazują potencjalne zagrożenia ze strony bardziej zaawansowanych modeli w przyszłości. Mogą one – „samodzielnie" lub sterowane z zewnątrz – wpływać na przebieg interakcji domowników (lub innych grup ludzkich), np. wywołując lub łagodząc spory, kształtując poglądy lub przekonując użytkowników do „własnych" racji. Jeśli te doniesienia się potwierdzą, inteligentne głośniki mogą stać się kolejnym sieciowym (po mediach społecznościowych), ważnym kanałem wpływu społecznego. Firmy produkujące urządzenia oraz inne podmioty, które posiądą zdolność do wpływania na sposób funkcjonowania tego typu asystentów (np. służby specjalne lub hakerzy), mogą zyskać potężne narzędzie do realizacji swoich interesów.

Rekomendacje: Należy rozważyć wprowadzenie zakazu wykorzystywania interaktywnych głośników w instytucjach publicznych oraz monitorować przypadki złamania zabezpieczeń tych urządzeń przez hakerów, a także przypadki wykorzystania ich w działaniach wywiadowczych lub podobnych. Należy wspierać oddolne inicjatywy, które podkreślają znaczenie prywatności i edukują w zakresie środków jej ochrony. **[5/10]**

---

alexa.aspx [odczyt: 22.05.2017]. Redakcja czasopisma zauważa także, że „w regularnych testach Komputer Świata postępy [urządzenia] były zauważalne w cyklu tygodniowym".

[27] M. Połowianuk, *Oto dwa nowe urządzenia Amazon Echo. Jeśli myślisz, że to tylko głośniki, jesteś w błędzie*, http://www.spidersweb.pl/2016/03/amazon-echo-dot-tap.html [odczyt: 22.05.2017].

[28] R. Carroll, *Goodbye privacy, hello 'Alexa': Amazon Echo, the home robot who hears it all*, 21.11.2015, https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud [odczyt: 22.05.2017].

Zabawki podłączone do Internetu umożliwiają manipulację dzieckiem

ANALIZA

13 czerwca 2017. Rosnąca liczba zabawek wyposażona jest w możliwość łączenia się z Internetem i przekazywania danych (np. zarejestrowanego głosu dziecka) na serwery producenta[29]. Choć już w przeszłości europejskie i amerykańskie urzędy ochrony praw konsumentów wskazywały na potencjalne zagrożenia z tym związane, w ostatnim czasie serwery, na których przechowywane są zbierane przez zabawki dane, faktycznie padły ofiarą ataków hakerskich. W lutym br. jedna z takich zabawek została zakazana w Niemczech jako urządzenie szpiegujące.

Komentarz: Gdy w 2015 roku ofiarą ataku hakerów padła firma VTech (znany producent „edukacyjnych" smartfonów i tabletów dla dzieci), dysponowała ona danymi 5 milionów rodziców oraz zdjęciami i treścią z czatów 200 tys. dzieci[30]. Dane te umożliwiały identyfikację i lokalizację geograficzną tych dzieci. Okazało się, że dane były przechowywane na serwerze, który był publicznie dostępny bez żadnej weryfikacji użytkownika[31]. Choć o wydarzeniu tym było głośno, zaś firma obiecała podwyższenie standardów bezpieczeństwa, podobne sytuacje odnotowano także w przypadku szeregu innych zabawek podłączonych do sieci (np. lalki „Hello Barbie")[32]. VTech natomiast wprowadził nowe zasady użytkowania, które całą odpowiedzialność za losy nagrań i skutki ewentualnych ataków hakerskich przerzuciły na rodziców; w efekcie pojawiły się nawoływania do bojkotu firmy[33]. W lutym br. okazało się, że w Internecie dostępna była niezabezpieczona żadnym hasłem baza 2,2 mln nagrań głosów dzieci i rodziców – użytkowników zabawki firmy SpiralToys, właściciela marki CloudPets[34]. Mimo ostrzeżeń specjalistów od cyberbezpieczeństwa kierowanych pod adresem firmy, baza ta była dostępna w sieci przez kilka miesięcy i kilkukrotnie była ofiarą ataku typu *ransomware*. Opinii publicznej nie poinformowano o tym ataku.

---

[29] Zabawki łączą się z Internetem na ogół dzięki technologii Bluetooth, za pośrednictwem aplikacji zainstalowanej na smartfonie rodzica, który tworzy konto na serwerze producenta. Zabawki korzystają z technologii rozpoznawania głosu i przetwarzania pytań dziecka na tekst komend, które wywołują „odpowiedź" zabawki.

[30] L. Franceschi-Bicchierai. 2015. *One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids*., http://motherboard.vice.com/read/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids [odczyt: 13.06.2017].

[31] T. Hunt, *Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages*, 28 February 2017, https://www.theregister.co.uk/2017/02/28/cloudpets_database_leak/ [odczyt: 13.06.2017].

[32] W. Meers, *Hello Barbie, Goodbye Privacy? Hacker Raises Security Concerns*, 1.12.2015, http://www.huffingtonpost.com.au/entry/hello-barbie-security-concerns_us_565c4921e4b072e9d1c24d22 [odczyt: 13.06.2017].

[33] L. Kelion, *Parents urged to boycott VTech toys after hack*, 10.02.2016, http://www.bbc.com/news/technology-35532644 [odczyt: 13.06.2017].

[34] Zob. oficjalną reklamę tego produktu: CloudPets Commercial, 12.05.2015, https://www.youtube.com/watch?v=EcxNHgYUz6s [odczyt: 13.06.2017].

W lutym 2017 roku niemiecki urząd regulacyjny Bundesnetzagentur (BNetzA) uznał jedną z tego rodzaju lalek („My Friend Cayla") za narzędzie szpiegujące, gdyż „bez wiedzy rodziców może nagrywać i transmitować rozmowy dziecka i innej osoby" i nakazał wycofanie jej z obiegu[35]. Istotne znaczenie miał fakt, iż wszystkie nagrania były przekazywane amerykańskiej firmie Nuance, która wykonuje m.in. usługi rozpoznawania głosu dla agencji wywiadowczych[36]. Zabawka ta była wcześniej krytykowana przez organizacje konsumenckie w USA; o fakcie tym donosiły także polskie media[37].

Zagrożenia związane z opisanymi tu zabawkami mają charakter analogiczny do zagrożeń związanych z inteligentnymi głośnikami wyposażonymi w funkcje wirtualnych asystentów[38]. Różni je jednak specyfika odbiorców – w przypadku zabawek są nimi dzieci. W licznych doniesieniach krajowych i zagranicznych podkreśla się na ogół ryzyko:

- wycieku nagrań głosu dziecka i wykorzystania ich do uzyskania okupu (np. w zamian za nieupublicznianie kompromitujących dziecko lub rodziców wypowiedzi);
- nieautoryzowanego nagrywania dźwięków z otoczenia dziecka oraz późniejszego wykorzystania tych danych w działalności przestępczej (np. przygotowania włamania do mieszkania);
- wykorzystania zabawki do ukrytej i szczególnie efektywnej reklamy adresowanej do dzieci[39].

Warto jednak zwrócić uwagę na bardziej długofalowe zagrożenia, jakie mogą wiązać się z użytkowaniem takich interaktywnych zabawek:

- mogą dawać rodzicom złudne poczucie, iż mówiąca ich głosem zabawka zaspokaja potrzeby dziecka w zakresie bliskości, wspólnej zabawy itp.,

[35] *Niebezpieczna lalka. Może szpiegować*, 18.02.2017, http://www.dw.com/pl/niebezpieczna-lalka-mo%C5%BCe-szpiegowa%C4%87/a-37614885 [odczyt: 13.06.2017]. Według doniesień, na pytanie dziecka: „Czy mogę powiedzieć ci sekret?" lalka ma odpowiadać: „Jasne, ale mów bardzo cicho. Obiecuję, że nikomu nie powiem; zostanie to między nami, bo jesteśmy przyjaciółkami"; lalka także zachwalała produkty firmy Disney. Zob. B. Chapell, *Banned In Germany: Kids' Doll Is Labeled An Espionage Device*, 17.02.2017, http://www.npr.org/sections/thetwo-way/2017/02/17/515775874/banned-in-germany-kids-doll-is-labeled-an-espionage-device [odczyt: 13.06.2017].

[36] B. Chapell, op.cit.

[37] Zob. np. R. Mościcki, *Niemiecki nadzór przeciw szpiegującym lalkom,* http://www.rp.pl/Biznes/302209919-Niemiecki-nadzor-przeciw-szpiegujacym-lalkom.html;

[38] Zob. komunikat CBB z bieżącego numeru Biuletynu pt. *Inteligentne głośniki Amazon Echo – wizja urządzenia podsłuchowego w każdym pomieszczeniu*.

[39] Przykładowo, jedna z takich zabawek „opowiada swojej właścicielce na przykład o tym, że najbardziej lubi filmy Disneya. Nie jest to zaskoczeniem, bo dystrybutor aplikacji współpracuje z Disneyem" http://www.dw.com/pl/niebezpieczna-lalka-mo%C5%BCe-szpiegowa%C4%87/a-37614885 [odczyt: 13.06.2017].

skłaniając ich do poświęcania mniejszej ilości czasu z dzieckiem; może to skutkować problemami psychicznymi oraz spowolnieniem rozwoju dziecka;

- w obliczu rosnącej ekspansji tzw. głośników inteligentnych (zob. wyżej Komunikat o głośnikach Echo Amazona) należy oczekiwać wyposażania rosnącej ilości zabawek w funkcje wirtualnych asystentów i towarzyszy zabaw dziecka, w tym np. możliwość odpowiadania na pytania dzieci dotyczące otaczającego je świata. Otwiera to ogromne możliwości manipulacji dzieckiem, zarówno w odniesieniu do zasobu jego wiedzy, jak i światopoglądu oraz stanów emocjonalnych. To samo zagrożenie wiąże się zresztą z użytkowaniem przez dzieci samych głośników inteligentnych[40].

Z perspektywy bezpieczeństwa państwa gromadzenie wielkich ilości danych o dzieciach i możliwość wywierania na nie masowego wpływu należy uznać za niepokojące. Otwiera to m.in. ryzyko systemowego wykorzystywania tych danych do identyfikacji dzieci szczególnie uzdolnionych (np. takich, które zadają zabawce niestandardowe, inteligentne pytania) i podejmowania prób ich rekrutacji przez korporacje, a więc drenażu mózgów. Przy odpowiedniej skali rozpowszechnienia zabawki, może także ona tworzyć możliwości *diagnozowania* stanu młodej populacji (np. pod względem potencjału intelektualnego, chorób umysłowych, stanu wiedzy itp.), jak i *wpływania* na światopogląd oraz postawy dzieci i młodzieży.

Z wstępnej analizy głównych platform e-handlu wynika, że w Polsce zabawki: „Hello Barbie", robot „i-Que" oraz CogniToys Dino nie są jeszcze (powszechnie) dostępne. Dostępna jest natomiast (np. na platformie OLX.pl) lalka „My Friend Cayla" oraz wiele modeli tabletów „edukacyjnych" firmy VTech.

Rekomendacja: Polskie instytucje edukacyjne (Ministerstwo Edukacji Narodowej, np. poprzez Instytut Badań Edukacyjnych) powinny podjąć działania (np. opracować kampanię informacyjną) polegające na uświadamianiu rodzicom i nauczycielom zagrożeń związanych z interaktywnymi zabawkami oraz metod ochrony dzieci przed ich niepożądanym oddziaływaniem. Działania te powinny być w pierwszym rzędzie adresowane do personelu placówek edukacyjnych, w tym zawierać zalecenie powstrzymania się od zakupu interaktywnych zabawek na wyposażenie tych placówek, nad którymi nadzór sprawuje MEN. UOKiK powinien zadbać o monitorowanie doniesień o szczególnie groźnych produktach, a także zlecić własne analizy bezpieczeństwa psychologicznego dopuszczanych na polski rynek zabawek interaktywnych. **[5/8]**

[40] Aplikacje dołączone do takich zabawek dają rodzicom pewien, na ogół niewielki, zakres kontroli nad interakcją dziecka a zabawką. Na ogół jest to panel rodzica, który pozwala na przeglądanie nagrań, a więc umożliwia rodzicowi szpiegowanie dziecka. Rzadziej możliwe jest ograniczenie sposobu wykorzystania zabawki przez dziecko; np. CogniToys Dino pozwala ustalić porę, kiedy dziecko powinno skończyć zabawę by iść spać. Zob. E. McReynolds et al., *Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys*, CHI 2017, 6-11.05.2017, http://techpolicylab.org/wp-content/uploads/2016/01/Toys-That-Listen_CHI-2017.pdf [odczyt: 13.06.2017], s.3.

Możliwość identyfikacji twarzy na podstawie analizy aktywności mózgu

SYGNAŁ

22 czerwca 2017. Badacze z renomowanego California Institute of Technology (Caltech) w Pasadenie (USA) dokonali ważnego odkrycia dotyczącego aktywności mózgu, związanej z rozpoznawaniem twarzy[41]. Badanie prowadzone na makakach pokazało, że za rozpoznawanie twarzy odpowiada bardzo niewielka liczba komórek mózgowych (205 neuronów). Eksperymenty umożliwiły odtworzenie wyglądu ludzkich twarzy obserwowanych przez małpy wyłącznie na podstawie danych o aktywności mózgu.

Komentarz: Z perspektywy bezpieczeństwa państwa, o wiele istotniejszy od samego odkrycia mechanizmu kodowania twarzy przez mózg jest fakt, że mamy do czynienia z kolejnym potencjalnym przełomem w technologiach nadzoru. Można zakładać, że jeśli wyniki badań zostaną potwierdzone, to w przyszłości pojawi się możliwość np. rekonstrukcji twarzy przestępców i terrorystów w oparciu o analizę aktywności mózgu świadków albo ofiar przestępstw. Pojawią się również możliwości wykorzystania tego rodzaju narzędzi w pracy wywiadowczej i kontrwywiadowczej (również w kontekście bezpośredniej ingerencji w umysły ludzi i manipulowania neuronami). Należy systematycznie monitorować prace w tym zakresie oraz dokonać wstępnego rozpoznania, czy w Polsce prowadzone są badania tego rodzaju. **[8/5]**

[41] L. Chang, D. Y. Tsao, *The Code for Facial Identity in the Primate Brain*, 2017, „Cell" 169: 1013–1028, http://dx.doi.org/10.1016/j.cell.

Nowa technologia imitowania ludzkiego głosu zagrożeniem dla procedur bezpieczeństwa

ANALIZA[42]

18 maja 2017. Pod koniec kwietnia br. kanadyjski start-up Lyrebird zademonstrował nową technikę imitowania głosu dowolnej osoby na podstawie bardzo krótkiego nagrania jej wypowiedzi[43]. Technika ta pozwala na odczytanie komunikatu wprowadzonego w formie tekstowej głosem dowolnie wybranej rzeczywistej osoby. Choć prace nad komputerową syntezą mowy trwają od dawna, nowość techniki wynika z faktu, iż pozwala ona na syntetyzowanie mowy w czasie rzeczywistym (a więc przy minimalnym opóźnieniu liczonym w ułamkach sekundy, co m.in. umożliwia zastosowanie techniki w trakcie trwania jakiejś konwersacji). Pozwala to znacznie obniżyć koszty, a także otwiera szereg nowych obszarów zastosowania. Zaprezentowane przez twórców symulacje mowy dla laika brzmią realistycznie, choć ekspert zwróci uwagę na pewne niedoskonałości (np. brak odgłosów oddychania, mlaśnięć itp.).

Komentarz. Z zapowiedzi twórców narzędzia wynika, że w ciągu najbliższych kilku lat stanie się ono powszechnie dostępne[44]. Technologia syntezy mowy nie jest niczym nowym. Nowością nie są również algorytmy, na których taka synteza się opiera (tj. sztuczne sieci neuronowe). W porównaniu do wcześniejszych rozwiązań tego typu, zaproponowany przez Lyrebird proces tworzenia wzorca mowy konkretnej osoby przebiega jednak szybciej, może wykorzystywać krótsze i słabej jakości próbki głosu, zmieniać intonację oraz nadawać mowie emocje. Kwestią kluczową z punktu widzenia bezpieczeństwa wydaje się fakt, iż technologia ta opuszcza laboratorium i wkrótce zapewne wejdzie na rynek jako niedrogi produkt.

Należy liczyć się z pojawieniem się zarówno amatorskich, jak i bardziej profesjonalnych „audio-montaży" na potrzeby rozrywki, ale także walki informacyjnej. Radykalnie zwiększyłoby to poziom zgiełku informacyjnego w sieci i wymusiło konieczność wprowadzenia procedur błyskawicznego dementowania wprowadzonych w obieg komunikatów akustycznych. Pojawi się także możliwość instrumentalnego wykorzystywania możliwości narzędzia do zrzucania na nie odpowiedzialności za niepożądane wypowiedzi, z których ich autorzy będą chcieli się wycofać. W efekcie, upowszechnienie technologii może podważyć wiarygodność i zaufanie do komunikacji głosowej, obecnie – zwłaszcza w erze fake newsów – uznawanej za bardziej wiarygodną od samych tekstów.

---

[42] Zob. Komunikat. *Postęp w technologii klonowania głosu ludzkiego zagrożeniem dla bezpieczeństwa państwa*, „Biuletyn OSWC" nr 4/2017, s. 21.

[43] B. Gholipour, *New AI Tech Can Mimic Any Voice*, 2.05.2017, https://www.scientificamerican.com/article/new-ai-tech-can-mimic-any-voice/ [odczyt: 22.05.2017]. Zob. też stronę firmy: https://lyrebird.ai/press.

[44] N. Lomas, *Lyrebird is a voice mimic for the fake news era*, 25.04.2017, https://techcrunch.com/2017/04/25/lyrebird-is-a-voice-mimic-for-the-fake-news-era/ [odczyt: 22.05.2017].

W celu lepszego zrozumienia zagrożeń związanych z możliwością wykorzystania tego narzędzia do manipulowania nastrojami decydentów i polityki publicznej warto rozważyć, jak mogłyby przebiegać pierwsze godziny (i dni) po tragedii smoleńskiej 2010 r., gdyby tuż po niej pojawiły się w mediach zmontowane rozmowy pasażerów czy obsługi lotniska. Potencjalnie narzędzie to może być również wykorzystywane do wspierania akcji dezorganizujących różne działania państwa. Przykładowo, w ważnej chwili polityk może usłyszeć głos w telefonie swoich bliskich wzywających pomocy – mimo iż będzie się liczył z tym, że głos może być nieprawdziwy, to zdarzenie może wywołać zamieszanie. Inny scenariusz to choćby pojawienie się w sytuacji zagrożenia sfałszowanego orędzia prezydenta.

System obecnie posiada następujące słabości: szum w tle i tzw. „robotowy" oddźwięk; nie tworzy też naturalnych odgłosów oddychania i ruchów aparatu mowy (np. mlaskania języka), które na poziomie komunikacji ludzkiej także niosą ze sobą pewne znaczenie. Te elementy umożliwiają odróżnianie mowy naturalnej od sztucznej. Tym niemniej dla niczego niepodejrzewającego słuchacza sztucznie wygenerowana wypowiedź może jawić się jako autentyczna. Należy też zakładać, że wspomniane niedoskonałości wkrótce zostaną naprawione i w najbliższej przyszłości pojawią się narzędzia zdolne do wyprodukowania imitacji trudno odróżnialnych nawet dla ekspertów.

Nie wiemy na razie, czy narzędzie jest w stanie imitować głos w dowolnym języku, czy też wyłącznie w języku angielskim. Informacje na ten temat są sprzeczne. Z demonstracyjnych próbek (tj. głosów Hillary Clinton, Baracka Obamy i Donalda Trumpa) dostępnych na stronie lyrebird.ai/demo wynika, iż jest to możliwe dla wypowiedzi w języku angielskim. Jeden z autorów narzędzia, w wywiadzie dla „Scientific American" wspomina, iż jest ono „language-agnostic", co może sugerować uniwersalność. Zarówno ta kwestia, jak i sama skuteczność narzędzia dla języka angielskiego wymagają jednak potwierdzenia[45].

Wśród **bezpośrednich konsekwencji** upowszechnienia omawianej technologii – nawet w jej obecnym kształcie – można wymienić:

1. Unieważnienie głosowych systemów weryfikacji tożsamości – np. w systemach bankowych[46];
2. Podważenie wartości dowodowej nagrań w postępowaniu sądowym;
3. Podważenie zaufania odbiorców do przekazów medialnych (zwłaszcza w połączeniu z najnowszymi technikami manipulacji obrazu, w tym animacji mimiki twarzy[47]) a także wszelkiej komunikacji telefonicznej;

[45] Obecnie dostępne źródła są bardzo skąpe i nie pozwalają na bliższą weryfikację omawianego tu narzędzia.

[46] W przytoczonym już artykule D. Simmonsa zrelacjonowano zwieńczoną powodzeniem próbę przełamania przez dziennikarza i jego brata-bliźniaka biometrycznych zabezpieczeń głosowych, jakie w 2016 roku wprowadził w Wielkiej Brytanii bank HSBC.

[47] J. Thies, M. Zollhofer, M. Stamminger, C. Theobalt, M. Nießner, *Face2Face: Real-time Face Capture and Reenactment of RGB Videos*, „Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition", 2016, http://www.graphics.stanford.edu/~niessner/thies2016face.html [odczyt: 22.05.2017].

4. Pojawienie się nowych technik reklamy i propagandy (np. w kontekście kampanii wyborczych czy komunikacji politycznej);
5. Pojawienie się nowych typów przestępczości, w tym wyłudzeń opartych o znany schemat oszustw „na wnuczka".

Można też wskazać na potencjalne **długofalowe konsekwencje** społeczne. Będą wśród nich:

1. Pojawienie się nowego typu wrażliwych danych osobowych – nagrań głosu stanowiących podstawę do „skopiowania". Istotnym problemem – społecznym i prawnym – stanie się ochrona tych danych przed nieautoryzowanym przejęciem i wykorzystaniem.
2. Pojawienie się nowych pól nieufności w relacjach międzyludzkich oraz międzyinstytucjonalnych.

W przeszłości mieliśmy do czynienia z analogicznym rozwojem wypadków w odniesieniu do obrazu. Pojawienie się możliwości cyfrowej edycji obrazów znacznie obniżyło wiarygodność dowodów wizualnych w dyskursie publicznym, choć ich zupełnie nie unieważniło – m.in. dzięki technikom detekcji śladów edycji, a także pracochłonności tych zabiegów, które dają dostatecznie wiarygodne rezultaty. Można wręcz twierdzić, że mimo dostępności tych technik, monitoring wizyjny nie tylko nie stracił na znaczeniu, a wręcz stale dynamicznie się rozwija.

Sami autorzy technologii wśród możliwych jej zastosowań wymieniają m.in. syntezę mowy na potrzeby osób niemych, zastosowanie w dubbingu filmowym. Deklarują także, że swe odkrycie upubliczniają jak najszybciej i tylko w ograniczonym zakresie, aby ostrzec wszystkich o zagrożeniach, jakie ich technologia niesie ze sobą[48]. Jak podał w wywiadzie dla BBC jeden z twórców, rozważane jest m.in. zaopatrywanie stworzonych za pomocą ich narzędzia nagrań swoistym „znakiem wodnym", który pozwoli szybko i jednoznacznie rozpoznać ich status imitacji[49]. Można prognozować, że kwestią czasu jest pojawienie się innych narzędzi o podobnych funkcjach, pozbawionych jednak tego rodzaju zabezpieczeń. Co więcej, trzeba założyć, że nawet imitacje łatwo identyfikowalne mogą być nierzadko odbierane przez duże grupy odbiorców jako prawdziwe, podobnie jak ma to miejsce obecnie w odniesieniu do tzw. *fake news*.

Rekomendacje:

1. Sugeruje się przetestowanie systemu i sprawdzenie jego skuteczności w imitowaniu języka polskiego, gdy tylko będzie to możliwe.
2. Należy przeprowadzić przegląd stosowanych w Polsce systemów biometrii opartych o głos w celu wykrycia w nich podatności na omawiane zagrożenie.
3. Należy przeszkolić decydentów i wybranych urzędników w zakresie możliwych zagrożeń.

[48] D. Simmons, *BBC fools HSBC voice recognition security system*, 19.05.2017, http://www.bbc.com/news/technology-39965545 [odczyt: 22.05.2017]

[49] Tamże.

4. Warto rozważyć opracowanie procedur i scenariuszy reagowania na pojawiające się w przestrzeni publicznej spreparowane komunikaty godzące w interes państwa i/lub porządek publiczny.
5. Należy przetestować reagowanie (np. podczas ćwiczeń w wojsku albo w służbach) na próby wpływania na decyzje za pomocą sfabrykowanych nagrań.
6. Należy podjąć prace legislacyjne zmierzające do uregulowania statusu nagrań głosu ludzkiego. Sugerujemy przyjęcie zakazu nieautoryzowanego wykorzystywania tych nagrań do tworzenia imitacji[50]. **[5/13]**

[50] Pewne aspekty prawne możliwości imitacji ludzkiego głosu omawia J. Gershman, *Imitation Game: The Legal Implications of Voice Cloning*, 25.04.2017, https://blogs.wsj.com/law/2017/04/25/imitation-game-the-legal-implications-of-voice-cloning/ [odczyt: 22.05.2017]. Autor sugeruje, że aktualne prawodawstwo amerykańskie relatywnie dobrze chroni ludzki głos jako jedno z dóbr osobistych (podobnie jak twarz) i tworzenie imitacji może nieść za sobą poważne sankcje prawne.

Kontrola aktywności w mediach społecznościowych w procedurze przyznawania wizy do USA

SYGNAŁ

2 czerwca 2017. Departament Stanu USA przyjął 23 maja br. suplement do wniosków wizowych[51]. Analiza przekazywanych w nim informacji umożliwia przeprowadzenie sprawdzeń aktywności wnioskodawców w świecie cyfrowym. Informacje mają być wyszukiwane na temat osób, w wypadku których „uznano, że wymagają dodatkowego sprawdzenia w związku z terroryzmem lub innymi mającymi związek z bezpieczeństwem narodowym wątpliwościami, które mogą uniemożliwić przyznanie wizy”[52]. Takie osoby proszone są o podawanie informacji z poprzednich pięciu lat o: nazwach kont prowadzonych przez wnioskodawcę w mediach społecznościowych, adresach poczty elektronicznej i numerach telefonicznych. Dodatkowe wymagane informacje zawierają dane biograficzne z poprzednich 15 lat – np. o historii i źródłach finansowania podróży międzynarodowych, zatrudnieniu i miejscach zamieszkania.

Komentarz: Chociaż Departament Stanu USA przewiduje, że dodatkowe przeszukiwanie będzie dotyczyło tylko ok. 65 tys. osób rocznie, to służby konsularne USA zyskują nowe narzędzie do odmowy wjazdu do Stanów Zjednoczonych wybranych, często w sposób arbitralny, osób. Możliwość zastosowania nowych procedur wobec polskich obywateli sprawia, że pojawia się zagrożenie powstania dodatkowych napięć związanych z wizami w relacjach polsko-amerykańskich. Polska w swojej polityce cyfrowo-informatycznej powinna rozważyć wprowadzenie dodatkowych zabezpieczeń danych elektronicznych swoich obywateli, przy jednoczesnym zapewnianiu sobie możliwie szerokiego dostępu do danych obywateli obcych państw. **[4/6]**

[51] Y. Torbati, *Trump administration approves tougher visa vetting, including social media checks*, depesza Reutersa z 1.06.2017, http://www.reuters.com/article/us-usa-immigration-visa-idUSKBN18R3F8 [odczyt: 2.06.2017].

[52] State Department/D.T. Donahue, *Notice of Information Collection Under OMB Emergency Review: Supplemental Questions for Visa Applicants*, 4.05.2017, https://www.federalregister.gov/documents/2017/05/04/2017-08975/notice-of-information-collection-under-omb-emergency-review-supplemental-questions-for-visa, [odczyt 2.06.2017]; formularz jest dostępny m.in. na stronie Ambasady USA w Turcji, https://tr.usembassy.gov/wp-content/uploads/sites/91/2017/05/DS-5535-Supplemental-Questions-for-Visa-Applicants.pdf, [odczyt: 2.06.2017].

Zagrożenie cyfrowej infrastruktury wyborczej atakami hakerów: przypadek USA

SYGNAŁ

28 czerwca 2017. Na początku czerwca br. do mediów wyciekł tajny dokument NSA, informujący o dokonanym przed zeszłorocznymi wyborami prezydenckimi w USA ataku hakerskim na infrastrukturę systemu wyborczego[53]. Z dokumentu wynika, że rosyjscy hakerzy związani z wywiadem wojskowym przed wyborami przypuścili udany atak na jedną z firm produkujących oprogramowanie do maszyn wyborczych (była to najprawdopodobniej firma VR Systems). Operacja trwała od sierpnia do listopada 2016 roku. W pierwszej fazie, w sierpniu 2016 roku, hakerzy uzyskali dostęp do kont pracowników wspomnianej firmy. W drugiej fazie, na przełomie października i listopada, wykorzystując uzyskane informacje, wysłali zainfekowane e-maile do 122 lokalnych urzędników zaangażowanych w proces wyborczy. Nie wiadomo, jaki był rzeczywisty efekt tego ataku, ale gdyby choć jeden z adresatów otworzył zainfekowany załącznik, hakerzy zyskaliby możliwość dostępu do systemu.

Komentarz: Wyciek materiału NSA oraz równoległe działania władz USA (sankcje wobec Rosji, wysłuchania przed Senatem[54]) wydają się potwierdzać, że cyfrowa infrastruktura wyborcza była i jest rzeczywistym obszarem zainteresowania hakerów, których łączy się z Rosją. Biorąc pod uwagę podatność systemów informatycznych na ataki, należy spowalniać w Polsce wszelkie inicjatywy, które idą w kierunku cyfryzacji procesu wyborczego. Przy tym nie idzie tylko o możliwą podatność infrastruktury wyborczej na cyberataki, co może wypaczyć wyniki głosowania. Równie **istotnym zagrożeniem może być duży potencjał delegitymizacji wyników wyborów**. **[8/3]**

[53] M. Cole, R. Esposito, S. Biddle, R. Grim, *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, „The Intercept", 05.06.2017, dostępny: https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ [odczyt: 30.06.2017]; powyższa publikacja zawiera również link do kopii pdf oryginalnego dokumentu NSA, który wyciekł do redakcji „The Intercept".

[54] Syntetyczny komentarz w tym zakresie: Ł. Olejnik, *Cyberbezpieczeństwo systemu wyborczego USA. Ciąg dalszy*, 21.06.2017, dostępny: http://prywatnik.pl/2017/06/21/cyberbezpieczenstwo-systemu-wyborczego-usa-ciag-dalszy/ [odczyt: 30.06.2017]

Do fazy testów klinicznych przechodzi nowa technika odczytywania sygnałów z mózgu w celu bezpośredniego sterowania maszynami

SYGNAŁ

22 maja 2017. Jak informuje „New Scientist", nowa technika tworzenia interfejsów mózg-maszyna (systemów umożliwiających sterowanie urządzeniami sygnałami elektrycznymi płynącymi bezpośrednio z mózgu) będzie testowana w 2018 roku na sparaliżowanych osobach[55]. Badana w projekcie finansowanym przez DARPA[56] technika polega na wprowadzeniu do mózgu elektrod za pomocą żyły szyjnej[57].

Dotychczas wykorzystywane dwie podstawowe techniki tworzenia interfejsów mają poważne wady. Pierwsza z nich zakłada łączenie mózgów z urządzeniami przez wprowadzanie elektrod przez czaszkę do wybranego obszaru mózgu, co prowadzi do zapaleń oraz powstawania blizn i w efekcie utraty łączności. Druga technika polega na prowadzeniu pomiarów przezczaszkowych, za pośrednictwem elektrod umieszczonych na skórze głowy. Opisana w „New Scientist" nowa technika nie wywołuje zapaleń i pozwala na precyzyjne odbieranie sygnałów z obszarów mózgu otaczających żyły, w które wprowadzone zostały elektrody. Badania te są znane już od roku[58]; o ich potencjale i finansowym wsparciu przez rząd USA informował w 2016 r. Barack Obama.

Komentarz: Interfejsy mózg-maszyna przedstawiane są jako narzędzia umożliwiające osobom sparaliżowanym sterowanie robotycznym szkieletem zewnętrznym (egzoszkieletem) lub protezami. Poszukiwanie nowych technik tworzenia interfejsów mózg-komputer ma jednak również potencjalne zastosowania militarne. **[4/6]**

[55] A. Klein, *Brain control via blood vessel stent*, „New Scientist", 20.05.2017, s. 12.

[56] Amerykańska rządowa Agencja Zaawansowanych Projektów w Dziedzinie Obronności.

[57] Jest to wykorzystanie rozwiązań stosowanych w kardiologii przy odbudowywaniu osłabionych naczyń krwionośnych. Mowa jest o stentach – czyli „sprężynkach" umieszczanych wewnątrz naczynia krwionośnego w celu przywrócenia jego drożności i zwiększenia trwałości.

[58] T. J. Oxley i in., *Minimally invasive endovascular stent-electrode array for high-fidelity, chronic recordings of cortical neural activity*, „Nature Biotechnology" 34, opublikowany online 8.02.2016, s. 320-327.

Postęp w tworzeniu hybrydy owada i maszyny

SYGNAŁ

27 maja 2017. W połowie stycznia 2017 roku badacze z powiązanej z Massachusetts Institute of Technology (MIT) firmy Draper poinformowali o postępach w pracy nad stworzeniem ważki-cyborga[59].

Komentarz: Hybrydy zwierząt i maszyn powstają od kilku lat[60]; o ile jednak dotąd naukowcy byli w stanie przejmować kontrolę „tylko" nad mięśniami zwierząt, o tyle w projekcie Dragonfleye dąży się do przejęcia kontroli nad systemem nerwowym owada[61]. Sukces w tym zakresie pozwoli na bardziej precyzyjne sterowanie ruchami zwierzęcia. Badacze z firmy Draper kreślą perspektywę dalszej miniaturyzacji testowanej obecnie technologii, w tym zamontowania „osprzętu" na pszczołach, co mogłoby pomóc podtrzymać zapylanie roślin w sytuacji zagłady tych owadów[62]. Prawdopodobne są także zastosowania militarne, w szczególności w obszarze rekonesansu i nadzoru.

Rekomendacje: Należy monitorować postępy w dziedzinie tworzenia hybryd zwierząt i maszyn pod kątem nowych zagrożeń terrorystycznych i militarnych. **[5/2]**

---

[59] *Equipping Insects for Special Service*, 19.01.2017, http://www.draper.com/news/equipping-insects-special-service [odczyt: 27.03.2017]. Projekt DragonflEye jest prowadzony w konsorcjum z Howard Hughes Medical Institute (HHMI).

[60] W roku 2016 badacze z Korei Południowej opublikowali wyniki badań, które dotyczyły możliwości zdalnego sterowania ruchami żółwia; zob. C.-H. Kim, B. Choi, D.-G. Kim, S. Lee, S. Jo, P.-S. Lee, *Remote Navigation of Turtle by Controlling Instinct Behavior via Human Brain-computer Interface*, „Journal of Bionic Engineering", 13(3)/2016: 491-503. Prowadzono także testy na większych owadach, np. locustach czy dużych żukach. Opisywane tu badania konsorcjum firmy Draper dotyczą ważki – owada bardziej sprawnego w lataniu.

[61] W grudniu 2016 roku badacze japońscy opublikowali wyniki badań, które obejmowały konstrukcję pojazdu, którym może kierować ćma. Ćmy – podobnie jak wiele innych owadów – dobrze wyczuwają zapach. Z zadaniem tym natomiast na razie kiepsko radzą sobie roboty. Badacze skonstruowali więc pojazd, którym ćma kieruje tak, by dotrzeć do źródła określonego zapachu. To krok w kierunku robotów imitujących owady. Zob. N. Ando, S. Emoto, R. Kanzaki, *Insect-controlled Robot: A Mobile Robot Platform to Evaluate the Odor-tracking Capability of an Insect*, „Journal of Visualized Experiments" (118), e54802, doi:10.3791/54802 (2016). Zob. też: M. Price, *Watch this moth drive a scent-controlled car*, 3.01.2017, http://www.sciencemag.org/news/2017/01/watch-moth-drive-scent-controlled-car [odczyt: 27.03.2017].

[62] *Summary for policymakers of the assessment report of the intergovernmental science-policy platform on biodiversity and ecosystem services (IPBES) on pollinators, pollination and food production*, 2016, Intergovernmental Science-Policy Platform on Biodiversity and Ecosystem Services (IPBES), http://www.ipbes.net/sites/default/files/downloads/pdf/spm_deliverable_3a_pollination_20170222.pdf [odczyt: 27.03.2017].

Szwedzi pod kontrolą chipów

SYGNAŁ

19 czerwca 2017. W Szwecji wprowadzono możliwość przejazdów koleją na podstawie zapisu na wszczepionym do ręki pasażera chipie. Jest to pierwsza tego typu usługa na świecie.

Zainteresowanym projektem osobom wszczepia się w rękę układ scalony. Po opłaceniu przejazdu koleją, dany zakup jest następnie przypisywany do chipa, który stanowi elektroniczny bilet na zakupiony przejazd. Konduktorzy w czasie kontroli skanują dłonie pasażerów i odczytują dane[63].

Analogiczne rozwiązanie przyjęła szwedzka firma Epicenter. Chipy wszyte w ręce jej pracowników pozwalają im mieć dostęp do różnych stref biura, a docelowo mają również pozwalać płacić za usługi. Prowokuje to do postawienia pytania o granice zakresu kontroli zachowań pracowników[64].

Zarzuty możliwej kontroli osób z chipami są jednakże odpierane m. in. przez rzecznika szwedzkiej kolei, stwierdzeniami, że można być również śledzonym poprzez użycie karty kredytowej czy telefonu komórkowego[65].

Komentarz: Chipowanie ludzi w sprawach ułatwiających codzienne sprawy łatwo może zostać wykorzystane do innych, mniej transparentnych celów. Mikroukłady elektroniczne wszczepione w ludzkie organizmy stanowią bowiem typową technologię podwójnego, czy – w świecie Internetu Rzeczy – wielokrotnego zastosowania. **[6/3]**

[63] S. Best, T. Collins*, Would you get your travel card implanted into your HAND? Swedish commuters raise concerns over security and privacy by using microchips to pay for their journey*, 14.06.2017, http://www.dailymail.co.uk/sciencetech/article-4604366/Swedish-commuters-using-microchips-pay.html [odczyt: 30.06.2017].

[64] N. Grimm, *Swedish employees agree to free microchip implants designed for office work*, 03.04.2017, http://www.abc.net.au/news/2017-04-03/swedish-employees-agree-to-microchip-implants/8410018 [odczyt: 30.06.2017].

[65] H. Coffey, *Swedish commuters can use futuristic hand implant microchip as train tickets*, 16.06.2017, http://www.independent.co.uk/travel/news-and-advice/sj-rail-train-tickets-hand-implant-microchip-biometric-sweden-a7793641.html [odczyt: 30.06.2017].

Alphabet Inc. (dawniej Google Inc.) sprzedało podmioty zależne zajmujące się robotyką

KOMUNIKAT

9 czerwca 2017. W dniu 8 czerwca ukazały się potwierdzone przez Alphabet Inc. informacje o sprzedaży przez tę spółkę dwóch podmiotów zależnych zajmujących się robotyką (Boston Dynamics oraz Schaft) japońskiej korporacji SoftBank Group[66]. Jej prezes poinformował, że celem zakupu jest wykorzystanie osiągnięć liderów na polu konstruowania robotów mobilnych, które będą „kluczowym czynnikiem w kolejnym etapie rewolucji informacyjnej".

Komentarz: Google Inc. stworzyło dział zajmujący się robotyką. W 2013 i 2014 roku spółka dokonała serii zakupów czołowych start-upów z tej dziedziny. Po odejściu z Google kierownika działu robotyki, spółka zmieniła długofalowe plany w stosunku do kupionych podmiotów. Pojawiły się informacje – obecnie potwierdzone – o chęci zrezygnowania z robotyki przez Google, ponieważ nie daje ona szans na szybkie wprowadzenie nowych produktów na rynek[67].

Boston Dynamics jest znane z tworzenia robotów humanoidalnych oraz czteronożnych, przypominających i naśladujących zwierzęta a także z wykonywania projektów na rzecz amerykańskiej DARPA oraz testów, które przeprowadzają na produktach Boston Dynamics siły zbrojne USA[68]. Schaft jest natomiast pionierem w zakresie tworzenia robotów dwunożnych, które odnosiły sukcesy w konkursach organizowanych przez DARPA.

Z komentarzy analityków firm zajmujących się robotyką wynika, że brakuje wiedzy na temat tego, jakie są dalsze perspektywy rozwoju dwóch wskazanych wyżej podmiotów i jakich wyników pracy oraz w jakiej perspektywie czasowej będzie od nich oczekiwał ich nowy japoński właściciel.

---

[66] Brak wskazanego autora informacji, *SoftBank Announces Agreement to Acquire Boston Dynamics. Companies to Collaborate in Advancing the Development of Smart Robotics Technologies*, 8.06.2017, http://www.businesswire.com/news/home/20170608006407/en/SoftBank-Announces-Agreement-Acquire-Boston-Dynamics [odczyt: 9.06.2017]; K. Leswing, *Google finds a buyer for two robotics companies it didn't want anymore*, „Bussines Insider" 9.06.2017, http://www.businessinsider.com/softbank-buys-boston-dynamics-and-schaft-from-google-2017-6?IR=T [odczyt: 9 czerwca 2017]; P. Alpeyev i M. Bergen, *SoftBank Agrees to Buy Robot Maker Boston Dynamics From Google Parent Alphabet*, „Bloomberg" 9.06.2017, https://www.bloomberg.com/news/articles/2017-06-09/softbank-agrees-to-buy-robot-maker-boston-dynamics [odczyt: 9.06.2017].

[67] A. Fitzpatrick, *Google Reportedly Selling the Company That Makes Insane Humanoid Robots*, „Time" 17.03.2016, http://time.com/4263163/google-selling-boston-dynamics-robots/ [odczyt: 9.06.2017].

[68] Patrz np.: Sygnał, *Zaprezentowano robota bojowego, który wkrótce może zmienić sytuację na polu walki*, „Biuletyn OSWC" nr 2/2017, s. 27; Komunikat, *Korpus Piechoty Morskiej US wznawia testy bojowego robota kroczącego*, „Biuletyn OSWC" nr 3/2017, s. 16.

Oba przedsiębiorstwa są obecnie znane głównie z widowiskowych akcji marketingowych, w trakcie których prezentowane są ich prototypy. Silnie oddziaływujące na wyobraźnię nagrania z przypominającymi zwierzęta lub ludzi robotami zazwyczaj w Internecie rozprzestrzeniają się „wirusowo". Często budzą jednak jednocześnie niekorzystne skojarzenia z robotami zabójcami z twórczości *science fiction*. Pojawiły się spekulacje, że to obawy wizerunkowe skłoniły Alphabet Inc. do rezygnacji z robotyki[69].

Rekomendacje: Dalsze losy Boston Dynamics oraz Schaft są warte uwagi, ponieważ ich prototypy robotów mają potencjał do wyznaczania standardów i w konsekwencji kierunków rozwoju rynku. Warte rozważenia wydaje się również sprawdzenie, czy polski system prawny jest przygotowany do, przykładowo, określania odpowiedzialności cywilnej i karnej za konsekwencje działania autonomicznych robotów przemieszczających się jak ludzie lub zwierzęta i funkcjonujących w obszarach zarezerwowanych dotychczas dla ludzi. **[4/3]**

[69] D. Muoio, *Boston Dynamics employees were frustrated with Google's plan for a household robot*, „Bussines Insider" 29.05.2016, http://www.businessinsider.com/why-google-and-boston-dynamics-are-parting-ways-2016-5?IR=T [odczyt: 9.06.2017].

Wyciek kodu źródłowego Windows 10

SYGNAŁ

25 czerwca 2017. W dniu 24 czerwca przedstawiciel Microsoftu oficjalnie potwierdził serwisowi internetowemu „The Verge", że nastąpił wyciek kodu źródłowego systemu operacyjnego Windows 10. Następstwem tego faktu może być wzrost ryzyka łamania zabezpieczeń tego systemu.

W szczególności rośnie ryzyko związane z atakiem za pomocą złośliwego oprogramowania typu *ransomware*. Jest to szczególnie niebezpieczny rodzaj trojana, który najczęściej instaluje się na dysku po pobraniu jakiegoś pliku, szyfruje zawartość dysku komputera i blokuje do niej dostęp domagając się np. uiszczenia okupu. Masowy atak tego typu (przeprowadzony przy pomocy oprogramowania WannaCry) miał miejsce w połowie maja br. i szacuje się, że zainfekowanych zostało kilkaset tysięcy urządzeń na całym świecie. Jest to już kolejna informacja rzucająca cień na bezpieczeństwo systemu operacyjnego Windows 10.

Rekomendacja. Warto rozważyć przeprowadzenie audytu na temat zakresu używania tego systemu w polskich instytucjach publicznych i oszacować skalę zagrożeń związanych z potencjalnym atakiem. Niektóre negatywne następstwa ataku *ransomware* można łatwo zredukować za pomocą kopii zapasowych przechowywanych na zewnętrznych serwerach lub dyskach. Warto upewnić się, czy i w których instytucjach państwowych istnieją i faktycznie przestrzegane są stosowne procedury wymuszające odpowiednio częste tworzenie kopii zapasowych. **[3/10]**