Przyszłość inteligentnego środowiska

Robert Marcinkowski

Wprowadzenie. Inteligencja wojen?

Rozwój technologiczny cywilizacyjnej czołówki postępuje obecnie bardzo szybko. Przynosi ewidentne korzyści i wzrost jakości życia, lecz zarazem zmienia sposób interakcji człowieka z otoczeniem i w niespotykanym dotąd stopniu uzależnia go od rosnącej ilości otaczających go urządzeń. Oprócz korzyści musi to powodować nieznane dotąd, nowego typu zagrożenia. Każde narzędzie może w niepowołanych rękach stać się bronią. Co więcej, cywilne zastosowania wielu współczesnych technologii są w istocie wtórne względem ich pierwotnego, wojennego przeznaczenia. Fakt ten skłania wielu ludzi do nieprzemyślanego, a w każdym razie nieprecyzyjnego sądu, iż to wojnom zawdzięcza ludzkość postęp.

Sąd taki znajduje pewne (skądinąd koszmarne) uzasadnienie w odniesieniu do cywilizacji pojmowanej jako całość, lecz jest całkowicie nonsensowny jako recepta na drogę do dobrobytu – przez niewspółmierne cierpienia ofiar.

Historia uczy, że inteligencja doskonaląca techniki wojenne stanowiła raczej motor napędowy ekspansji kolejnych cywilizacji, zaś dobro i postęp pojawiały się z pewnym opóźnieniem. A zarazem – że nie wystarczyło inteligencji, by upadkom tychże cywilizacji zapobiec.

Mówiąc w ogromnym skrócie i uproszczeniu, gatunek *Homo sapiens* istotnie „wytworzył" inteligencję jako oręż walki, przetrwania i zmagania się z otoczeniem, lecz odbywało się to pod „podobnie nieludzkim" ciśnieniem selekcyjnym, co w ewolucji oznacza dla gatunku ogromną opresję i alternatywę: przystosowanie albo śmierć. Opresji takich nie przetrwała większość najbliższych genetycznych krewnych człowieka, znanych dziś z wykopalisk i skamielin.

Podobnym, choć znacznie czasowo bliższym skokiem cywilizacyjnym, napędzającym proces kształtowania się inteligencji i dającym supremację względem innych gatunków, było wynalezienie (a raczej wytworzenie) języka, a więc narzędzia komunikacji i transmisji wiedzy, zapewniającej m.in. skuteczność w polowaniach, a szerzej w międzygatunkowych (i międzyrasowych) interakcjach. Skojarzenie z Internetem jako wzmacniaczem komunikacji i – pośrednio – zbiorowej inteligencji nie jest tu bynajmniej przypadkowe.

Istotna uwaga uściślająca: termin ‚inteligencja' odniesiony do zbiorowości, a więc gatunków czy cywilizacji, jest czymś odmiennym od indywidualnych osobniczych zdolności mierzalnych ilorazem IQ.

Bardzo zbieżny jest natomiast z sensem zawartym w pojęciu inteligentnego budynku. Pojęcie inteligentnego budynku na tyle trwale weszło do powszechnego obiegu, że (w większości) przestaliśmy zwracać uwagę na zawarte w nim semantyczne nadużycie. Np. nasze auta są na ogół bardziej inteligentne od naszych domów, a rzadziej przypisujemy im inteligencję, w gruncie rzeczy z powodu przyzwyczajenia.

Na marginesie: obawy, jakie wzbudzać mogą znajdujące się w ludzkich rękach potężne narzędzia, a do takich zaliczają się technologie informatyczne, można zilustrować przez analogię do oporu, jaki w wielu krajach wzbudza np. energetyka jądrowa, kojarzona nawet wbrew rozsądkowi z zagrożeniem bronią nuklearną.

Internet Rzeczy (IoT: *Internet of Things*)

Problematyka budynków inteligentnych dotyczy otoczenia człowieka, lecz rozumianego przestrzennie jako względnie bliskie czy też (nawet uwzględniając zdalne sterowanie i sensorykę) lokalne. Natomiast rozwijające się już trendy prowadzą do kolejnych poszerzeń granic tego otoczenia, a w rezultacie do sytuacji, w której człowieka otacza już nie tyle budynek, co ciągła obecność zintegrowanego systemu, nieograniczona już przestrzennie, podobnie jak nie jest w ten sposób ograniczona sieć Internetu.

Poszerzeniem w stosunku do pojęcia inteligentnego budynku jest pojęcie Inteligentnego Miasta. Przejście do kolejnego stopnia systemowej integracji nie zachodzi skokowo, lecz polega na tworzeniu coraz to nowych form zależności między obiektami. Inteligentne budynki funkcjonują jeszcze osobno, lecz obiekty Inteligentnego Miasta są już nie tyle budowlami, co najkrócej mówiąc, przenikającą je infrastrukturą.

Jak to najczęściej bywa w opisie względnie nowych zjawisk, już na wstępie pojawiają się kłopoty z nazewnictwem. Czy ma sens poszukiwanie celnego semantycznie spolszczenia? Google proponuje „Internet Przedmiotów", zaś jeszcze trafniejszy byłby może „Internet Obiektów", skoro nie wszystkie są *stricte* przedmiotami. Z podobnych zapewne powodów cały rozdział Wikipedii opatrzony jest uwagą, że „jako zbyt techniczny, może okazać się niezrozumiały dla czytelników"[1].

W ewolucji języka mnóstwo jest też przypadków, kiedy ostatecznie „przyjęły się" nazwy początkowo komiczne lub nonsensowne. Dlatego skoro wysyłamy nie mesydże, lecz całe esemesy[1] – możemy także żyć w przyszłym, przypuśćmy, Ajocie. Chodzi w każdym razie o „proponowaną formę rozwojową Internetu, w której przedmioty codziennego użytku mają łączność z siecią, pozwalającą im na wysyłanie i odbieranie danych" [1].

Do przedmiotów tych, jednoznacznie identyfikowalnych, zaliczają się także urządzenia gospodarstwa domowego i urządzenia noszone (*wearables*) [2].

Z obszernym wykładem propagującym ideę Internetu Rzeczy wystąpił w ubiegłym miesiącu Anton Ravindran[2] na Konferencji „Nowe technologie budowlane i projektowanie architektoniczne" zorganizowanej przez Instytut A-4 Wydziału Architektury Politechniki Krakowskiej. Ponieważ artykuł ten nie jest jeszcze powszechnie dostępny[3], chciałbym posłużyć się obszerniejszym cytatem:

„Nowe aplikacje IoT wykorzystujące chmurę obliczeniową (*cloud computing*), szerokopasmowy przesył informacji (*big data*) i analitykę biznesową umożliwiają rozprzestrzenienie się inicjatywy Smart City na całym świecie. Umożliwiają one wprowadzenie nowych funkcji, jak zdalne monitorowanie, sterowanie i zarządzanie, dzięki dostępowi do ogromnych ilości informacji w czasie rzeczywistym. W rezultacie oferują możliwości przekształcania miast i społeczności przez poprawę infrastruktury, tworzenie bardziej wydajnych i efektywnych kosztowo usług dla swoich obywateli, rozwój transportu publicznego czy zmniejszenie korków, przy równoczesnym wzroście bezpieczeństwa obywateli i zaangażowaniu ich na rzecz społeczeństwa. Miasta myślące o przyszłości, jak Singapur, uznają, że nie muszą zdawać się na lokalne rozwiązania typu Smart City, lecz wybierają bezpieczną całościową infrastrukturę integrującą także inne systemy. Artykuł zaprezentuje technologiczne rozwiązania IoT dla inteligentnych budynków i inteligentnych miast" (tłum. i podkreślenia – rm).

„Obiekty" połączone systemem mają więc stworzyć całe materialne otoczenie człowieka. Najmniejsze z nich to np. implanty monitorujące akcję serca, czy biochipy dla hodowli zwierząt. Większe, w skali zbliżonej do inteligentnego budynku, oprócz wdrażanych już:

- automatyki oświetlenia, ogrzewania (z sekwencyjną termostatyką itd.),
- wentylacji i klimatyzacji,
- systemu zabezpieczeń,

obejmują także pralko-suszarki, chłodziarki i zamrażarki, kuchenki mikrofalowe, a nawet ekspresy do kawy – znajdujące się w zasięgu zdalnego monitorowania i sterowania za pomocą sieci WiFi. Czujniki i przełączniki wszystkich tych urządzeń podłączone do koncentratora głównego, zwanego także „Bramą", mogłyby być sterowane przez użytkownika zdalnie za pomocą telefonu komórkowego, tabletu, a nawet z zainstalowanych w mieście terminali.

Lecz na skali budynku nie kończą się, rzecz jasna, potencjalne możliwości sieci. W większych obszarach mogłaby działać automatyka pożarnicza, zabezpieczenie wód przybrzeżnych czy wreszcie monitoring wszystkich istniejących pojazdów w czasie rzeczywistym, pozwalający na minimalizację korków i całkowitą kontrolę ruchu drogowego. Wszystkich możliwych zastosowań nie sposób wymienić.

Głosy krytyczne

Oprócz ewidentnych zalet systemu nie sposób nie dostrzec jednak czyhających na użytkownika potencjalnych zagrożeń, w tym zwłaszcza rozwijających się (równie dynamicznie) nowych form przestępczości komputerowej, zyskującej niespotykane dotąd pola ekspansji.

Głosy krytyczne padać mogą z różnych stron, w niejednolitym stopniu zasługujących na uwagę. W Internecie może wypowiadać się całe spektrum osób, od rozsądnych ekspertów po kompletnych ignorantów. Jakimi więc kryteriami powinniśmy się kierować w obszarach na ogół po prostu nieznanych, czyli w tym przypadku w ocenie zarzutów wobec nowej technologii?

Może przez analogię: jeśli poznanie technik włamań i kradzieży samochodów jest najszybszym źródłem informacji, wskazującym słabe punkty producentom zabezpieczeń pojazdów – to w sprawie ochrony danych komputerowych należałoby podobną uwagę poświęcić technikom stosowanym przez hakerów.

Hakerzy i twórcy zabezpieczeń toczą ze sobą coś więcej niż pojedynek. To skomplikowana relacja angażująca ogromną ilość środowisk (z dziedzin choćby bankowości, polityki, mediów, instytucji rządowych czy militarnych), w której każda z antagonistycznych stron może – co więcej – zmienić front i wystąpić przeciw dotychczasowym sojusznikom.

W artykule „Jak przeżyć w świecie IoT. Jak ustrzec się hakerów, używając inteligentnych urządzeń" [4] (tłum. rm) znajdujemy ostrzeżenia przed sytuacjami związanymi z urządzeniami domowego użytku, a więc nieporównanie mniej groźnymi, ale za to opisanymi dokładnie i jawnie. Np. niewinny odtwarzacz multimedialny (google Chromecast) może serwować użytkownikom treści emitowane przez hakera. Zagrożenie atakiem (tu: anteną kierunkową) mogą oni zmniejszyć, uruchamiając urządzenie „w odleglejszych częściach domu". Równie niewinna kamera IP, którą można zdalnie monitorować śpiące niemowlę, może też zdradzić listę adresów mailowych i uczynić (zwłaszcza VIP-a) ofiarą np. oszczerczej kampanii.

A czym mógłby zaszkodzić nam ekspres do kawy? I tu jednak odpowiedź znajdują atakujący: wyciekiem hasła do domowej sieci. Czy konieczny jest więc PIN do każdego kawowego ekspresu? Sprzedawcy twierdzą, że nie, lecz ich argumentacja brzmi nie do końca uspokajająco. Ich zdaniem bowiem zbyt krótkie jest po prostu czasowe okno potencjalnego ataku, a więc haker musiałby pozostawać na dłużej „gdzieś w pobliżu", czyli w zasięgu domowej sieci.

Te i podobne zagrożenia, niemające globalnego charakteru, mogą w istocie być jeszcze niegroźne, lecz postęp technologiczny sprawia, że sytuacja ta dynamicznie się zmienia. Sam artykuł posiada zastanawiający podtytuł: „Hakerstwo IoT dla początkujących".

Nieco poważniejszy jest z kolei problem wtargnięcia na teren chroniony systemem. Autorzy opisują sposoby ominięcia czujników bez aktywowania alarmu i „pokonanie ich ich własną bronią". Każdy rodzaj czujnika ma fizykalne podłoże działania i np. niektóre dadzą się oszukać zwykłym magnesem.

Wykiwać Inteligentne Miasto[4]

Można podejrzewać wielu autorów wpisów o nadmierną panikę, jednak autorzy (reprezentujący firmę Kaspersky Lab) zwracają uwagę na fakty i zagrożenia w sposób (niestety) poważny i wiarygodny. Demonstrują mianowicie metody atakowania systemu jako całości z terminali dostępnych publicznie.

Infrastruktura informatyczna występuje w przestrzeni miejskiej coraz

powszechniej. Oprócz lotnisk i dworców znajduje się już w biurach, urzędach, a także w punktach sprzedaży biletów i dziesiątkach innych łatwo dostępnych miejsc. Terminale dostępne są przez całą dobę, mają powtarzalną konstrukcję i połączone są w sieci, co oznacza, że nawet pojedyncze, „punktowe" wtargnięcie do systemu może szybko poszerzyć swój zasięg. Co więcej, terminale przetwarzają także dane wrażliwe, w tym poufne osobowe i finansowe. „Udany" atak hakerski oznacza zarządzanie siecią przez osoby niepowołane, wyciek danych, a co najmniej możliwość poważnych zniszczeń wywołanych przez instalację wrogiego oprogramowania.

Podsumowanie

Inteligencja człowieka powstała w rezultacie naturalnej ewolucji i sztuczna inteligencja materialnego otoczenia są podobne z nazwy, lecz w istocie bardzo się różnią. Ich istotną cechą wspólną jest możliwość wykorzystania ich zarówno w dobrych, jak i złych celach.

Potężne narzędzie (tu: informatyczny makrosystem) nie jest samo z siebie bezpieczne w użyciu. W niepowołanych rękach może stać się groźną bronią.

Bezpieczeństwo w inteligentnym mieście nie jest więc bynajmniej oczywiste. Tym niemniej tendencja globalizacyjna w rozwoju sieci rysuje się wyraźnie. Oprócz inteligentnych budynków i inteligentnych miast powstaje więc wizja idąca dalej – Internetu Wszechrzeczy. W wizji tej kolejne wcielenie Internetu tworzy już całościowy alternatywny świat, w którym integracje i podziały przebiegają zupełnie inaczej niż na politycznych mapach.

Przypisy

1. Trudno przecież wysyłać cały Short Message System, a tym bardziej pisać go.
2. Anton Ravindran – przewodniczący Światowego Forum Naukowo-Technologicznego (GSTF: *Global Science and Technology Forum*), adiunkt – profesor Wydziału Systemów Informacyjnych na Uniwersytecie Bina Nusantara w Indonezji.
3 *Internet Rzeczy (IoT) i jego wpływ na społeczności i miasta* [w:] *New building technologies and architectural design*. Publikacja w opracowaniu na PK. [6].
4 *Fooling the Smart City* [5].

Literatura

[1] Wikipedia English, *Internet of Things*, 16.11.2016, tłum. rm.
[2] https://pl.wikipedia.org/wiki/Internet_rzeczy#cite_note-1
[3] Ashton K.: *That ‚Internet of Things' Thing*. 09.12.2012.
[4] https://securelist.com/analysis/publications/72595/surviving-in-an-iot-enabled-world/ 2016-10-29. Autorzy: Victor Alyushin i Vladimir Krylov, 5.11.2015, 10:59.
[5] *Fooling the Smart City*, Denis Makrushin, Vladimir Dashchenko 15.09.2016, 8:59 https://securelist.com/analysis/publications/76060/fooling-the-smart-city/
[6] Ravindran A.: *Internet Rzeczy (IoT) i jego wpływ na społeczności i miasta* [w:] *New building technologies and architectural design*. Publikacja w opracowaniu na PK.

Robert Marcinkowski – Instytut A-4, WAPK