Biuletyn Ośrodka Studiów nad Wyzwaniami Cywilizacyjnymi
CBB ASzWoj
Numer 4 | maj 2017

W numerze:

- **Microsoft** postuluje przyjęcie przez społeczność międzynarodową odpowiednika „Konwencji Genewskiej" w zakresie **cyber-wojny**.
- **Facebook** przyjmuje strategię obrony przez działaniami z zakresu wojny informacyjnej.
- Rząd Wielkiej Brytanii wchodzi w spór z **Twitterem** o dostęp do danych użytkowników.
- Armia USA z powodzeniem testuje techniki treningu z wykorzystaniem **elektronicznej stymulacji mózgu**.
- Francja i Wielka Brytania od kilku miesięcy zwiększają swoje zdolności do toczenia **walk w terenie miejskim** z użyciem ręcznej broni palnej.
- Rosyjski wicepremier uczestniczy w nagłośnieniu pokazu zdolności bojowych **nowego typu robota**.
- Chiński **system cyfrowego *ratingu* obywateli** paradoksalnie może obniżyć sterowność systemu politycznego.
- Estonia wprowadza kolejne usługi administracji publicznej oparte na **architekturze blockchain**.
- Powstają **programy imitujące i edytujące głos**, które są w stanie w 80% przypadków oszukać zabezpieczenia biometryczne.
- **Hybryda robotów i żywych zwierząt** metodą na poprawienie mobilności maszyn, która może zwiększyć ich potencjał na polu walk
- Postępy w pracach nad powstaniem **komputera kwantowego** mogą zagrażać bezpieczeństwu kryptograficznemu państwa.
- Rozwój **technologii oprysków modyfikujących kod genetyczny** roślin stwarza ryzyko powstania nowego typu broni biologicznej.

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

Jeden z dyrektorów Microsoftu proponuje stworzenie „Cyfrowej Konwencji Genewskiej"

KOMUNIKAT

4 maja 2017. Dnia 14 lutego br. szef działu prawnego i korporacyjnego Microsoftu, w trakcie wystąpienia plenarnego podczas prestiżowej konferencji dotyczącej cyber-bezpieczeństwa[1], wysunął postulat stworzenia „Cyfrowej Konwencji Genewskiej"[2]. Jego zdaniem cyberprzestrzeń stała się nowym polem walki. Tymczasem, jak powiedział przedstawiciel Microsoftu:

> „społeczność międzynarodowa nie ma środków, czyli właśnie prawa międzynarodowego, by przeciwdziałać negatywnym skutkom cyber-ataków inicjowanych przez państwa. Mamy globalne przepisy dotyczące broni konwencjonalnej, ale brakuje podobnego prawa o broni cyfrowej. Dlatego odwołuję się do konwencji genewskich uchwalonych w 1949 r. (…). Uchwalano je, by mieć na przyszłość prawo, które pomoże ochronić cywilów nawet w czasie wojny. Nikt wtedy nie przewidział, że podobnej ochrony potrzebować będziemy także przed zagrożeniami z cyberprzestrzeni w czasie pokoju"[3].

Propozycja przedstawiciela Microsoftu zakłada:

1. Wprowadzenie prawnego zakazu prowadzenia cyber-ataków na firmy z sektora prywatnego (w tym z branży technologicznej) oraz na infrastrukturę krytyczną.

2. Wspólne, aktywne działania firm sektora prywatnego w celu wykrywania i przeciwstawiania się tego rodzaju atakom (a także neutralizowania ich skutków).

3. Publiczne ogłaszanie luk w systemach IT w celu ich jak najszybszego uszczelnienia (a nie wykorzystywania do prowadzenia cyber-ataków).

4. Wprowadzenie ograniczeń dotyczących rozwijania cyber-broni.

5. Wprowadzenie zakazu rozpowszechniania rozwiązań w tym zakresie.

6. Ograniczanie wszelkich działań ofensywnych w cyberprzestrzeni.

Istotną cechą tej propozycji jest przekonanie, że firmy branży IT „powinny zobowiązać się do wspólnego działania zmierzającego do uczynienia z Internetu bezpiecznej przestrzeni. W tej roli branża powinna zachować neutralność i być czymś w rodzaju (…)

[1] RSA Conference 2017 (11-17.02.2017, San Francisco, USA). Jest to najbardziej znana konferencja branży informatycznej dotycząca bezpieczeństwa. Organizowana jest od 1991 roku. Obecnie każdego roku w cyklu konferencji uczestniczy ok. 45 tysięcy osób.

[2] Stenogram wystąpienia plenarnego Brada Smitha można znaleźć tutaj: https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf [odczyt: 04.05.2017].

[3] Wywiad dla Associated Press, za: S. Czubkowska, *Brad Smith z Microsoft: Cyfrowe konwencje genewskie*, 11.04.2017, http://www.gazetaprawna.pl/artykuly/1034225,brad-smith-microsoft-cyfrowe-konwencje-genewskie.html [odczyt: 04.05.2017].

neutralnej cyfrowej Szwajcarii, stając się dla chronionych podmiotów, skądkolwiek pochodzą, światowym gwarantem zaufania”[4].

Komentarz: Wystąpienie przedstawiciela Microsoftu (oraz jego wpis na blogu na ten temat[5]) zostało zrelacjonowane w światowych mediach (zarówno głównego nurtu, jak i specjalistycznych); było też szeroko dyskutowane i komentowane[6].

Omawianą propozycję można rozpatrywać na kilku poziomach.

1. Jest to wskazanie pewnego problemu, ważnego globalnie i szczególnie istotnego dla funkcjonowania branży IT.

2. Mamy tu do czynienia z silną artykulacją podmiotowości ze strony prywatnych gigantów cyfrowych. Sama propozycja jest wyrazem przekonania, że to właśnie branża IT powinna współtworzyć takie reguły. Deklarowana polityka neutralności ze strony firm IT jest wreszcie swoistą próbą osłabienia kontroli ze strony państw, w których firmy te funkcjonują (co prawnie ma jednak zagwarantować wspólnota międzynarodowa złożona właśnie z państw).

3. Wystąpienie wydaje się wyrazem niechęci części amerykańskiej branży IT względem administracji Donalda Trumpa i jego polityki (w tym cyber-polityki).

---

[4] *Brad Smith: Potrzebujemy Cyfrowej Konwencji Genewskiej,* https://enterprise.microsoft.com/pl-pl/articles/roles/it-leader/brad-smith-potrzebujemy-cyfrowej-konwencji-genewskiej, [odczyt: 04.05.2017].

[5] B. Smith, *The need for a Digital Geneva Convention*, 14.02.2017, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention [odczyt: 04.05.2017].

[6] A. Blake, *Microsoft president touts ‘Digital Geneva Convention’ during cybersecurity keynote speech*, http://www.washingtontimes.com/news/2017/feb/14/brad-smith-microsoft-president-touts-digital-genev [odczyt: 04.05.2017]; E. Weise, *Microsoft calls for 'digital Geneva Convention'*, https://www.usatoday.com/story/tech/news/2017/02/14/microsoft-brad-smith-digital-geneva-convention/97883896 [odczyt: 4.05.2017]; D. Post, *Microsoft’s Brad Smith on cyberattacks, cybersecurity, and ‘cyberspace’*, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/10/microsofts-brad-smith-on-cyberattacks-cybersecurity-and-cyberspace/?utm_term=.df482b509676 [odczyt: 4.05.2017]; D. Volz, *'Digital Geneva Convention' needed to deter nation-state hacking: Microsoft president*, http://www.reuters.com/article/us-microsoft-cyber-idUSKBN15T26V [odczyt: 04.05.2017]; J. Vanian, *Here’s Why Microsoft President Wants a Digital Geneva Convention*, http://fortune.com/2017/02/14/microsoft-president-digital-geneva-convention [odczyt: 4.05.2017]; J. Kurbalija, *Digital Geneva Convention: multilateral treaty, multistakeholder implementation,* http://www.huffingtonpost.com/entry/digital-geneva-convention-multilateral-treaty-multistakeholder_us_58b443c0e4b02f3f81e44a35 [odczyt: 04.05.2017]; T. Simonite, *Do We Need a Digital Geneva Convention?*, https://www.technologyreview.com/s/603639/do-we-need-a-digital-geneva-convention [odczyt: 4.05.2017]; E. Kaspersky, *A Digital Geneva Convention? A Great Idea,* https://www.forbes.com/sites/eugenekaspersky/2017/02/15/a-digital-geneva-convention-a-great-idea/#67d5c6021e6e [odczyt: 4.05.2017]; K. Conger*, Microsoft calls for establishment of a digital Geneva Convention*, https://techcrunch.com/2017/02/14/microsoft-calls-for-establishment-of-a-digital-geneva-convention [odczyt: 4.05.2017]; S. Czubkowska, B*rad Smith z Microsoft: Cyfrowe konwencje genewskie*, http://www.gazetaprawna.pl/artykuly/1034225,brad-smith-microsoft-cyfrowe-konwencje-genewskie.html [odczyt: 04.05.2017]; J. Szczęsny, *Pomysł prezydenta Microsoftu: „Cyfrowa Konwencja Genewska”*. Kto to podpisze?!, http://antyweb.pl/cyfrowa-konwencja-genewska [odczyt: 04.05.2017].

Rekomendacje:

1. Warto rozważyć monitorowanie, czy inicjatywa zostanie podjęta przez administrację USA (lub innego liczącego się gracza globalnego) – do chwili obecnej brak jest informacji na ten temat.

2. W miarę możliwości warto dążyć do ograniczania sytuacji, w której reguły gry, również na polu polityki, ustalane są w polu specyficznego globalnego partnerstwa publiczno-prywatnego. Tego rodzaju konwencja, która mogłaby mieć duże znaczenie dla Polski, powinna ewentualnie zostać uzgodniona na poziomie państw. **[8/4]**

Facebook wypowiada wojnę wojnie informacyjnej

KOMUNIKAT

5 maja 2017. Zespół cyber-bezpieczeństwa Facebooka opublikował w dniu 27 kwietnia 2017 raport „Information Operations and Facebook”[7]. Jest to bezprecedensowe opracowanie omawiające przegląd operacji informacyjnych przeprowadzanych w serwisie Facebook przez podmioty zewnętrzne (rząd państwa agresora albo grupy przestępcze) oraz strategię ochrony przed tego typu operacjami w przyszłości.

Operacja informacyjna jest definiowana jako sekwencja działań podejmowanych przez zorganizowany podmiot, aby zniekształcać/zakłócać wewnętrzną sytuację polityczną państwa podlegającego agresji i bardzo często uzyskiwać strategiczną przewagę w kontekście geopolitycznym. Operacje tego typu są realizowane poprzez propagowanie fałszywych informacji, akcje dezinformacyjne (np. operacje pod „obcą banderą”) oraz tworzenie sieci fałszywych kont użytkowników, aby manipulować opinią publiczną.

Autorzy raportu podkreślają szczególną rolę mediów społecznościowych w operacjach informacyjnych, w tym zwłaszcza Facebooka, który ma olbrzymi zasięg oddziaływania na całe społeczeństwa. Użycie Facebook’a do operacji informacyjnych daje agresorom następujące możliwości:

1. Niezwykle duży zasięg dotarcia z informacją w skali globalnej, nie spotykany nigdy wcześniej w historii ludzkości (prawie 2 mld aktywnych użytkowników na całym świecie).
2. Każdy użytkownik może być potencjalnym aktywnym wzmacniaczem (ang. *amplifier*) w zakresie kreowania, modyfikowania i przekazywania informacji. Oznacza to, że umiejętnie prowadzone operacje mogę uzyskiwać realne wsparcie nieświadomych użytkowników.

Dotychczas zaobserwowane operacje informacyjne pogrupowano w trzy kategorie:

1. Spersonalizowane zbieranie informacji mające na celu kradzież wrażliwych danych osobowych oraz wywieranie różnego rodzaju manipulacji opinią publiczną.
2. Tworzenie fałszywego „kontentu” (treści) polegające na zorganizowanym kreowaniu informacji, historii, memów, zdjęć, itp.
3. Propagowanie i wzmacnianie nieprawdziwych przekazów informacyjnych poprzez wykorzystywanie fałszywych kont użytkowników.

Facebook deklaruje determinację, aby identyfikować, zatrzymywać i zapobiegać operacjom informacyjnym. Jest to niezwykle ważna deklaracja w kontekście roli mediów społecznościowych i ich wpływu na społeczeństwo oraz sytuację polityczną. **[12/2]**

[7] J. Weendon, W. Nuland i A. Stamos, *Information Operations and Facebook*, 27.04.2017, https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf [odczyt: 05.05.2017].

Londyn w sporze z Twitter Inc. o blokadę dostępu do danych wykorzystywanych w nadzorze elektronicznym

KOMUNIKAT

10 maja 2017. Spółka Twitter Inc. zablokowała dostęp do niektórych danych na temat użytkowników serwisu, ponieważ dane te były na zlecenie instytucji państwowych wykorzystywane przez podmioty prywatne do prowadzenia nadzoru elektronicznego[8]. Blokada wywołała protesty brytyjskiego rządu[9]. Wysoki rangą przedstawiciel Twittera informował w listopadzie 2016 roku, że firma „jest poważnie zaniepokojona" wykorzystywaniem jej danych do prowadzenia nadzoru elektronicznego, a „używanie publicznie dostępnych interfejsów programistycznych aplikacji Twittera (*ang. Twitter's public APIs*) lub naszych produktów opartych na danych do śledzenia lub profilowania uczestników protestów i aktywistów jest absolutnie nieakceptowane i zakazane".

Komentarz. Prywatne podmioty gospodarcze oferują instytucjom państwowym narzędzia analityczne, które działają w oparciu o dane na temat aktywności użytkowników Internetu. Coraz częściej wielkie korporacje działające w sieci, które mają potencjał zbierania danych na temat swoich użytkowników, deklarują, że dążą do jak największej ochrony ich prywatności. Programy tajnych służb ujawnione przez Edwarda Snowdena i WikiLeaks oraz działania takich podmiotów gospodarczych jak Cambridge Analytica[10] uwrażliwiają użytkowników sieci na zagrożenia, które wynikają z wykorzystania danych na ich temat.

Rekomendacje. W procedurach zakupu narzędzi analizujących aktywność podejrzanych osób lub środowisk w Internecie (w tym w mediach społecznościowych) należy brać pod uwagę, że podmioty dostarczające takie narzędzia mogą stracić dostęp do części lub wszystkich danych, które stanowią podstawę ich działalności. Istnieje również zagrożenie operacyjne wynikające z ujawnienia korzystania przez instytucje państwowe z takich rozwiązań, a co za tym idzie – ryzyko powstania szkód wizerunkowych. **[4/8]**

---

[8] K. McCann, *Government 'blocked' from accessing Twitter data to help spot terrorist plots*, „The Telegraph", 25.04.2017, http://www.telegraph.co.uk/news/2017/04/25/government-blocked-accessing-twitter-data-help-spot-terrorist/ [odczyt: 10.04.2017]; N. Lomas, *UK government irate at Twitter's surveillance API crack down*, „Techcrunch", 26.04.2017, https://techcrunch.com/2017/04/26/uk-government-irate-at-twitters-surveillance-api-crackdown/ [odczyt: 10.05.2017]; S. Hopkins, *Twitter 'Preventing Government From Monitoring Terror-Related Content' Twitter says surveillance is 'absolutely unacceptable and prohibited'*, „Huffington Post UK", 26.04.2017, http://www.huffingtonpost.co.uk/entry/twitter-preventing-government-from-monitoring-terror-related-content_uk_59004a27e4b081a5c0f8d43d [odczyt: 10.05.2017].

[9] C. Moody, *Developer Policies to Protect People's Voices on Twitter*, „blog.twitter.com", 22.11.2016, https://blog.twitter.com/2016/developer-policies-to-protect-people-s-voices-on-twitter [odczyt: 10.05.2017]; zob. H. Warel, *UK accuses Twitter of shirking responsibility in fight against terror*, „Financial Times", 26.04.2017, https://www.ft.com/content/120f8468-2a98-11e7-bc4b-5528796fe35c [odczyt 10.05.2017].

[10] C. Cadwalladr, *The great British Brexit robbery: how our democracy was hijacked*, „The Observer", 7.05.2017, https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy [odczyt: 10 maja 2017].

Amerykańscy specjalsi testują techniki przezczaszkowej elektrostymulacji mózgu

KOMUNIKAT

31 maja 2017. Prestiżowy amerykański portal military.com informuje, że wybrane amerykańskie elitarne jednostki specjalne (SEALS) testują techniki przezczaszkowej elektrostymulacji mózgu do poprawy zdolności bojowych[11]. Technika ta polega na wykorzystaniu niewielkich impulsów elektrycznych (wysyłanych przez urządzenie w postaci słuchawek), które mają pomagać w aktywowaniu mięśni podczas treningu fizycznego, co skutkuje większą wydajnością treningu[12]. Badania opublikowane na stronie producenta urządzenia (firmy Halo Neuroscience) prowadzone na zawodowych sportowcach (m.in. skoczkach narciarskich) wskazują, że stosowanie tych technik pozwala istotnie zwiększyć wyniki sportowe[13]. Testy, których prowadzenie potwierdziło już kilku amerykańskich dowódców wojskowych, są elementem szerszej strategii zbliżenia pomiędzy wojskiem USA a innowacyjnymi firmami z Doliny Krzemowej (np. firmami Alphabet Inc. oraz LinkedIn)[14]. Wśród celów eksperymentu dowódcy wymieniali m.in. wydłużenie okresu szczytowej koncentracji uwagi z 20 minut nawet do 20 godzin, poprawę umiejętności strzeleckich snajperów, poprawienie wyszkolenia pilotów, utrzymanie wysokiego poziomu wyszkolenia przy zwiększonej dawce snu (tj. zmniejszeniu intensywności treningu) lub utrzymanie obecnej intensywności szkoleń dla zwiększenia zdolności bojowych.

Komentarz: Oficjalny charakter deklaracji amerykańskich wojskowych może wskazywać, że opisywane eksperymenty prowadzone były już od dłuższego czasu, zaś ich efekty pozwalają obecnie na praktyczne wdrażanie. Należy zakładać, że analogiczne badania prowadzą także jednostki specjalne szeregu innych krajów, w tym Rosji. Oceniając wiarygodność doniesień, należy ostrożnie podchodzić do deklaracji firm współpracujących z amerykańskim wojskiem. Technologie, o których mowa, są dostępne komercyjnie i chwalenie się ich skutecznością jest elementem strategii

[11] H. H. Seck, *Super SEALs: Elite Units Pursue Brain-Stimulating Technologies*, 2.04.2017, http://www.military.com/daily-news/2017/04/02/super-seals-elite-units-pursue-brain-stimulating-technologies.html [odczyt: 10.04.2017].

[12] A. Barnwell, *This crazy new wearable uses 'neurostimulation' to prime your brain and body for exercise*, 11.03.2016, http://www.digitaltrends.com/wearables/neurostimulation-headphones-boost-workout-effectiveness/ [odczyt: 13.04.2017].

[13] *Bihemispheric Transcranial Direct Current Stimulation with Halo Neurostimulation System over Primary Motor Cortex Enhances Rate of Force Development in an Isometric Lateral Pinch Force Task*, 10.02.2016, https://halo-website-static-assets.s3.amazonaws.com/whitepapers/mvc.pdf [odczyt 30.05.2017]; *A Real – World Investigation into the Benefits of Transcranial Direct Current Stimulation to the Primary Motor Cortex on Muscular Performance in Elite Athletes*, 10.02.2016, https://halo-website-static-assets.s3.amazonaws.com/whitepapers/mjp.pdf [odczyt: 14.04.2017]. Oczywiście, do wyników badań sponsorowanych przez samego producenta trzeba podchodzić sceptycznie.

[14] R. Sisk, *Pentagon Wants Brain-Stimulating Headset to Improve Combat Skills*, 26.06.2016, https://www.dodbuzz.com/2016/07/26/pentagon-taps-tech-firm-for-headset-to-improve-combat-skills/ [odczyt: 13.04.2017].

marketingowej[15]. Na obecnym etapie nie sposób ocenić, czy mamy do czynienia z marketingową „bańką" pompowaną przez entuzjazm menadżerów i trenerów z obszaru amerykańskiego sportu zawodowego i US Navy. Wyniki tu przytaczane mają charakter wstępny: nie wiadomo nic o trwałości efektów technologii, o efektach ubocznych; wyniki uzyskano na małych próbach, brak również dostępu do szczegółowych danych. Przede wszystkim nic nie wskazuje, że wyniki zostały powtórzone przez niezależny od Halo Neuroscience zespół. Środowiska badaczy pozostają sceptyczne wobec doniesień firmy i oczekują na publikację wyników w recenzowanych czasopismach[16]. Sceptycyzm jest uzasadniony: w przeszłości wiele analogicznych technologii budziło początkowo duży entuzjazm, by ostatecznie zawieść oczekiwania. Niemniej, należy zakładać, że zarówno w sferze militarnej, jak i w innych sferach życia społecznego (medycyna, sport, rozrywka, edukacja) techniki te wkrótce mogą prowadzić do silnego zaostrzenia konkurencji pomiędzy jednostkami i państwami. W początkowej fazie, gdy brakuje jeszcze regulacji prawnych, można się spodziewać, że poszczególni przedstawiciele różnych środowisk (np. żołnierze, sportowcy, studenci i naukowcy) będą na własną rękę eksperymentować z technikami neurowspomagania. Eksperymenty takie mogą mieć także nieoczekiwane, negatywne skutki uboczne. Zarówno wskazane wyżej, jak i szersze wykorzystanie technik elektrostymulacji, zrodzi wkrótce m.in. pytanie o granice odpowiedzialności (moralnej i prawnej) osób podlegających takiej stymulacji (istotne zwłaszcza w kontekście żołnierzy). W dalszej przyszłości można się spodziewać jednak upowszechnienia takich technik, których stosowanie może być nawet wymagane od kandydatów do pewnych zawodów (np. zawodowych pilotów lub chirurgów – od których sprawności może zależeć ludzkie życie).

Rekomendacje:

1. Należy monitorować doniesienia na temat zastosowań techniki przezczaszkowej elektrostymulacji mózgu, w tym zwłaszcza zastosowań bojowych, celem ustalenia skuteczności działania dostępnych obecnie urządzeń, a także zakresu ich wykorzystania przez wojska poszczególnych państw. Należy też monitorować trendy w zakresie wykorzystania odnośnych urządzeń przez osoby prywatne do różnych celów.
2. Sugerujemy pozyskanie kilku zestawów opisywanego tu urządzenia Halo Sport i przetestowanie ich skuteczności eksperymentalnie, w trybie podwójnej ślepej próby. Cena urządzenia wynosi ok. 750 USD i jest ono powszechnie dostępne na zagranicznych platformach zakupowych. Sugerowane jest przeprowadzenie zarówno prób laboratoryjnych, jak terenowych. W zależności od wyników takiego testu, należy rozważyć przeprowadzenie własnych badań – zarówno na obecnie dostępnych urządzeniach, jak i nad rozwojem własnych do celów wojskowych. **[5/10]**

[15] Jakiś czas temu firma reklamowała się sloganem, że „Amerykańskie wojsko przyspieszyło szkolenie pilotów I snajperów o 50% stosując neurotechnologię podobną do Halo Sport"; zob. np. H. Seck, *Super SEALs, op. cit.* Obecnie hasło to zniknęło ze strony producenta.

[16] S. Reardon, *Performance boost paves way for "brain doping,"* „Nature", 2016, t. 531, s. 283–284. W publikacji tej przytoczono z rezerwą wyniki czterech badań, opublikowanych w prestiżowych czasopismach, które – choć przeprowadzone na małych próbach – zinterpretowano jako potwierdzenie efektu elektrostymulacji u sportowców.

Francja i Wielka Brytania zwiększają swój potencjał do walki w terenie miejskim z wykorzystaniem broni palnej

ANALIZA

22 kwietnia 2017. Od kilku miesięcy we Francji i Wielkiej Brytanii trwają przygotowania do zwiększenia zdolności prowadzenia działań przy pomocy broni palnej w warunkach miejskich. Brytyjski „The Guardian" poinformował o zmianie podejścia brytyjskiej policji względem procedur dotyczących interwencji z wykorzystaniem broni palnej[17]. Dotychczasowa, ostrożna w porównaniu np. z USA doktryna interwencji z bronią palną zostaje zmieniona m.in. w celu umożliwienia policjantom ostrzeliwywania pojazdów, co do których istnieje podejrzenie, że przeprowadzany jest za ich pomocą atak terrorystyczny. Zwiększona ma być także liczba brytyjskich policjantów uzbrojonych w broń palną oraz mają oni zostać wyposażeni w specjalną amunicją przystosowaną do atakowania pojazdów. Dotychczas brytyjska policja słynęła z powściągliwości w zakresie stosowania środków przymusu bezpośredniego. Normalny brytyjski policjant (tzw. „*bobby*") nie jest uzbrojony w broń palną. Posiadają ją tylko funkcjonariusze specjalni, tzw. AFO (Authorised Firearms Officer). Na skutek doświadczeń z ostatnich miesięcy, gdzie w zamachach terrorystycznych na terenie UE sprawcy używali pojazdów mechanicznych, przyjęto założenie, że atak może zostać powstrzymany przy pomocy strzału w stronę pojazdu. Tego rodzaju ostrzał jest niebezpieczny, ponieważ istnieje duże ryzyko rażenia osób trzecich.

Informacje z Wielkiej Brytanii należy zestawić z doniesieniami z Francji. Dnia 30 marca 2017 na spotkaniu seminaryjnym poświęconych wyposażeniu sił specjalnych SOFINS (*Special Operation Forces Innovation Network Seminar*) ujawniono, że francuskie jednostki interwencyjne żandarmerii narodowej GIGN (Groupe d'Intervention de la Gendarmerie Nationale) wyposażone zostaną w czeski kabarin CZ 805 Bren 2 w wersji na amunicję 7,62x39 mm, właściwą dla karabinu AK47 (Kałasznikowa). Należy podkreślić, że nie jest to natowski standard amunicji. Prawdopodobnie francuscy żandarmi wybrali typ amunicji, który będzie lepiej sprawdzał się przy ostrzeliwywaniu pojazdów mechanicznych.

Kluczowe znaczenie ma także informacja, że w ostatnich miesiącach armia francuska podjęła decyzję o zastąpieniu dotychczasowego karabinu podstawowego FAMAS niemieckim HK 416F[18]. Zamówiono 102 tysiące nowych karabinów, z czego ponad połowę ma stanowić wersja ze skróconą lufą. Wartość kontraktu to 200 mln euro. Karabin FAMAS nie jest przy tym sprzętem, który można by uznać za przestarzały i wymagający pilnej wymiany. Ważne w kontekście francuskim jest także symboliczne

[17] S. Chesterman, *Armed police to be trained to shoot through windscreens to stop vehicle attacks*, "The Guardian", 19.04.2017, https://www.theguardian.com/uk-news/2017/apr/19/armed-police-to-be-trained-to-shoot-through-windscreens-to-stop-vehicle-attacks [odczyt 5.05.2017].

[18] M. Cabriole, *Le fusil d'assaut allemand HK 416 F remplacera bien le célèbre FAMAS*, "La Tribune", 24.09.2017, http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/le-hk-416-f-allemand-remplace-le-celebre-fusil-d-assaut-famas-601929.html [odczyt 5.05.2017].

znaczenie tego karabinu[19]. Istotne jest to, że Francja sama posiada bardzo rozwinięty przemysł zbrojeniowy i z nieraz przesadną dumą stara się polegać w różnych obszarach na rodzimej produkcji. Mimo to, zdecydowano się na produkt niemiecki. Może to oznaczać, że Paryżowi zależało na dość szybkiej realizacji kontraktu. Druga istotna okoliczność jest taka, że większość zamówionych karabinów będzie miała skróconą lufę[20]. Zazwyczaj większość typów jednostek liniowych uzbraja się w broń długą o standardowej długości, zaś wersje skrócone rezerwuje się dla wojsk desantowych i załóg pojazdów. Broń taka ma mniejszy zasięg niż wersja klasyczna, ale jest bardziej poręczna w walce w terenie miejskim. Tymczasem Amerykanie, po doświadczeniach w wojnie w Iraku i Afganistanie poważnie dyskutują wymianę karabinu podstawowego[21], na taki, który będzie miał większy zasięg. Sytuacja ta wskazuje, że Amerykanie rozważają wariant, w którym ich armia przygotowana jest do walki w warunkach „polowych", co odpowiadałoby sytuacji np. na Bliskim Wschodzie (Irak, Afganistan, być może Syria). Natomiast Francja i Wielka Brytania powiększają swój potencjał do toczenia walk w terenie miejskim. Może to być zarówno interwencja antyterrorystyczna, jak i przedsięwzięcia właściwe dla zwalczania wojny hybrydowej.

Rekomendacje:

1. Należy rozważyć scenariusze wystąpienia w zachodnich państwach UE (przede wszystkim Niemcy oraz Francja i Wielka Brytania) walk w dużych miastach będących serią aktów terroryzmu, bądź elementem wojny hybrydowej, wojny domowej, napięć etnicznych czy eskalacji kryzysu migracyjnego. Szczególną uwagę należy zwrócić na te elementy scenariuszy, które dotyczyć będą reakcji Polski na potencjalną eskalację konfliktu, zagrożeń niestabilnością oraz fal migracji z państw objętych konfliktem.

2. Rozważając wybór uzbrojenia dla polskich WOT warto zwrócić uwagę na zmianę podejścia do kwestii karabinu podstawowego, jaka ma miejsce we Francji. **[3/2]**

[19] N. Guibert, *Famas, vie et mort d'un symbole national*, "Le Monde", 23.09.2016, http://www.lemonde.fr/m-le-mag/article/2016/09/23/famas-vie-et-mort-d-un-symbole-national_5002185_4500055.html [odczyt 5.05.2017].

[20] Eric. B., More details of the Heckler & Koch HK416F for France, "Field Journals", 17.01.2017, https://fieldjournals.com/2017/01/17/more-details-of-the-heckler-koch-hk416f-for-france/ [odczyt: 5.05.2017]

[21] J.P. Avery, Physics Demands A New Basic Combat Weapon, "Military Review", 7-8.2012, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20120831_art004.pdf [odczyt: 5.05.2017].

Wicepremier Rosji nagłaśnia nagranie możliwości bojowych eksperymentalnego androida

KOMUNIKAT

23 kwietnia 2017. Dnia 14 kwietnia br. wicepremier Federacji Rosyjskiej Dmitrij Rogozin, który odpowiada za przemysł zbrojeniowy i kosmiczny, nagłośnił za pomocą mediów społecznościowych[22] krótki film demonstrujący m.in. celne strzelanie do tarcz z dwóch pistoletów przez humanoidalnego robota F.E.D.O.R.[23] Nagranie zostało opatrzone przez wicepremiera Rogozina wyjaśnieniem, że:

> „Robot typu F.E.D.O.R. zademonstrował zdolność strzelania z dwóch rąk. Trwają prace nad umiejętnościami motorycznymi i algorytmami podejmowania decyzji. Bojowa robotyka – kluczem do stworzenia myślących maszyn. Chodzi tu szczególnie o lotnictwo i kosmos. Trening strzelecki – to sposób na nauczenie maszyny wybierania priorytetów i natychmiastowego podejmowania decyzji. My nie tworzymy terminatora, a sztuczną inteligencję, która będzie mieć ogromne znaczenie praktyczne w wielu różnych sferach”[24].

Komentarz: Zdjęcia robota i wyjaśnienia Rogozina zyskały znaczący rezonans w mediach – również zachodnich[25]. Pokaz został zinterpretowany przez część komentatorów[26] jako informacja ze strony Rosji, że jest gotowa do wykorzystania na polu bitwy autonomicznych systemów bojowych, które będą zastępowały żołnierzy i będą samodzielnie podejmowały decyzję o użyciu przemocy. Fedor jest konstruowany przez spółkę „NPO Androidnaja Technika”[27], która korzysta w tym celu z funduszy Ministerstwa ds. Sytuacji Nadzwyczajnych FR. Spółka współpracuje też z rosyjskim

---

[22] D. Rogozin, *Русские боевые роботы - парни с железным характером*, Wpis opublikowany na Twitterze, 14.04.2017, https://twitter.com/Rogozin/status/852869162493935617 [odczyt 19.04.2017].

[23] Skrót rozwija się jako „Final Experimental Demonstration Object Research”.

[24] W czterech wpisach ilustrowanych fotografiami Fedora na strzelnicy i opublikowanych 13.04.2017 na Twitterze, twitter.com/Rogozin [odczyt: 19.04.2017].

[25] Przykładowo: N. Griszczenko, *Робот-космонавт Федор научился стрелять с двух рук*, „Russkoje Orużje”, 14.04.2017, https://rg.ru/2017/04/13/robot-kosmonavt-fedor-nauchilsia-streliat-s-dvuh-ruk.html [odczyt: 19.04.2017]; S. Jones, *'We are not creating a Terminator': Russia denies risk as Putin's 'robot army' is trained to shoot guns*, „Mirror Online”, 17.04.2017, http://www.mirror.co.uk/news/world-news/we-not-creating-terminator-russia-10237755 [odczyt: 19.04.2017]; *It's not a Terminator': Putin's 'robot army' trained to shoot guns but Russia denies risk*, „Daily Record”, 17.04.2017, http://www.dailyrecord.co.uk/news/uk-world-news/its-not-terminator-putins-robot-10240379 [odczyt: 19.04.2017]; D. Furness, *Russia's deputy prime minister insists gun-toting robot is not a Terminator*, „Digital Trends”, 18.04.2017, http://www.digitaltrends.com/cool-tech/fedor-russia-space-robot/ [odczyt 19.04.2017]; P. Nag, *As Putin denies building robot army, video of Russian robot shooting like Terminator goes viral,* „Internationa Business Times”, 18.04.2017, http://www.ibtimes.sg/putin-denies-building-robot-army-video-russian-robot-shooting-like-terminator-goes-viral-9338 [odczyt 19.04.2017]; T. O'Connor, *Russia Built a Robot That Can Shoot Guns and Travel to Space*, „newsweek.com”, 19.04.2017, http://www.newsweek.com/russia-built-robot-can-shoot-guns-and-travel-space-586544 [odczyt 21.04.2017].

[26] Por. wskazane wyżej teksty nt. strzeleckiego testu Fedora.

[27] Strona internetowa spółki: http://npo-at.com/ [odczyt: 19.04.2017].

Narodowym Centrum Rozwoju Technologii i Podstawowych Elementów Robotyki[28], które działa pod nadzorem rządowego Funduszu Badań Zaawansowanych[29]. Według informacji z mediów rosyjskich, które są często powielane przez media zachodnie, Fedor ma odgrywać ważną rolę w rosyjskim programie kosmicznym: jako pilot statków kosmicznych, załogant Międzynarodowej Stacji Kosmicznej, budowniczy baz księżycowych i marsjańskich[30]. Fedor pierwotnie miał być tylko zdalnie sterowanym zastępcą człowieka, robotem ratunkowym, awatarem ratowników w niebezpiecznych dla zdrowia i życia sytuacjach. Demonstrowanie nowych umiejętności Fedora pokazuje możliwości przemysłu zbrojeniowego i kosmicznego FR. W tym sensie Fedor jest narzędziem reklamowania potencjalnych produktów eksportowych tego kraju. Nagłośnienie udanego eksperymentu ze strzelaniem może być także przykładem walki informacyjnej. Nie można bowiem wykluczyć, że faktyczne możliwości robota są niewielkie, np. że Fedor został tylko zaprogramowany do zrealizowania określonego zadania lub że na każdym etapie eksperymentu z prowadzeniem ognia był zdalnie sterowany przez ludzkiego operatora.

Rekomendacje: należy monitorować realne możliwości Fedora i innych robotów tworzonych w FR. Elementem takiego monitoringu powinno być ustalenie, na ile mamy do czynienia z systemem zdalnie sterowanym lub zaprogramowanym do realizacji określonych działań, a na ile z robotami autonomicznymi, kierowanymi przez bardziej zaawansowane rodzaje sztucznej inteligencji (np. opartej o uczenie maszynowe). **[4/5]**

[28] Ros. Национальный Центр Развития Технологий и Базовых Элементов Робототехники.

[29] ros. Фонд перспективных исследований. Strona internetowa Funduszu: http://fpi.gov.ru/ [odczyt: 19.04.2017].

[30] Zob. np. A. Bogdanow, *'Федор' отправится в облет Луны*, rozmawiał Smitrij Stugowiec, „Informacyonnoje Agientstwo Rossii TASS", 13.12.2016, http://tass.ru/opinions/interviews/3865192 [odczyt 19.04.2017]; A. Grigoriew, *Роботы станут помощниками космонавтов в открытом космосе*, nie wskazano nazwiska autora wywiadu, „Rossija Siegodnia – Ria Nowosti", 12.04.2017, https://ria.ru/interview/20170412/1492061943.html [odczyt 19.04.2017].

Chiński system zautomatyzowanej oceny obywateli: możliwe konsekwencje wdrożenia

KOMENTARZ do analizy z Biuletynu 2 OSWC

4 maja 2017. Rząd Chin planuje wdrożenie od 2020 r. narodowego systemu reputacji (*citizen scoring*) sankcjonującego zachowania obywateli uznawane za niepożądane. Byłby on rozwinięciem funkcjonujących już systemów ratingu kredytowego i uwzględniałby między innymi dane z baz wymiaru sprawiedliwości, zachowywania konsumenckie oraz aktywność danej osoby w sieciach społecznościowych. Obecnie w fazie pilotażu znajduje się 8 konkurencyjnych rozwiązań, testowanych na różnych grupach odbiorców. Założenia systemu są takie, że wysokość ratingu obywatela określałaby jego szanse życiowe, a dokładniej dostęp do rozmaitych stanowisk, usług i reglamentowanych dóbr. Rating danej osoby byłby również przypuszczalnie znany innym obywatelom[31].

Komentarz: Rozwijany system jest wyrazem dążenia Chińskiej Republiki Ludowej do regulowania możliwie dużej liczby aspektów aktywności swoich obywateli. Zbieranie przez Chiny informacji o obywatelach wydaje się zrozumiałe, gdy uwzględnimy system polityczny tego państwa: każdy system ograniczający wolności obywateli automatycznie pozbawia się możliwości łatwego monitorowania narastających napięć społecznych. Rating obywatelski, bazujący na automatycznych systemach zbierania danych jest dogodną alternatywą dla inwigilacji społeczeństwa za pośrednictwem agentury.

Warto jednak pamiętać, że upowszechnienie wiedzy o ratingu poszczególnych obywateli i powiązanie z nimi konkretnych bodźców ekonomicznych może mieć także negatywne następstwa dla systemu społecznego.

Tak sugeruje między innymi koncepcja efektu wypierania motywacji wewnętrznej (ang. *motivation crowding-out effect*)[32]. Efekt ten polega na tym, że w sytuacji, gdy próbujemy wzmocnić bodziec społeczny o bodziec ekonomiczny, ten drugi ma tendencję nie do wzmacniania, lecz do wypierania tego pierwszego.

Dobrze ilustracje to eksperyment przeprowadzony w izraelskich przedszkolach[33]. Rodzice spóźniający się z odebraniem swoich pociech są powszechnym problemem. W ramach eksperymentu standardowy mechanizm oparty na nieformalnych sankcjach obyczajowych (konieczność tłumaczenia się, poczucie wstydu etc.) próbowano wzmocnić o bodziec ekonomiczny w postaci grzywny za spóźnienie. Innowacja przyniosła skutki odwrotne od zamierzonych: liczba spóźnień drastycznie wzrosła, podobnie jak czas ich trwania. Rodzice potraktowali grzywnę za spóźnienie jako cenę za

[31] Pilotażowe systemy ratingu obywatelskiego zostały omówione w analizie *Chiński system zautomatyzowanej oceny obywateli: perspektywa cyfrowego totalitaryzmu*, 3 marca 2017, Biuletyn Ośrodka Studiów nad Wyzwaniami Cywilizacyjnymi CBB ASzWoj, numer 2, marzec 2017. Równolegle analizę systemów przeprowadził Ośrodek Badań Azji CBB: analiza koncentrowała się na systemach ratingu jako remedium na niedorozwój sektora usług finansowych, w tym zwłaszcza systemu kredytowego w Chinach. Niniejszy komentarz odnosi się tylko do pierwszej z wymienionych analiz.

[32] B. Frey i R. Jegen, *Motivation Crowding Theory*, „Journal of Economic Surveys", 2001, vol. 15, nr 5, ss. 589-611.

[33] U. Gneezy i A. Rustichini, *A Fine is a Price*, „Journal of Legal Studies", 2000, vol. 29, nr 1, ss. 1-18.

ponadwymiarową opiekę nad dzieckiem, a nie jako sankcję. Dodatkowo bodziec finansowy unieważnił umowę społeczną i wyeliminował nieformalną, obyczajową kontrolę nad zachowaniami. Jak się wydaje, kluczowe jest nie tyle samo wypieranie, co nieodwracalność tego procesu: norma ekonomiczna zastępuje normę społeczną w sposób trwały. I tak, gdy wycofano grzywny jako nieskuteczne narzędzie kontroli społecznej, liczba spóźnień nie tylko nie wróciła do pierwotnego poziomu, ale jeszcze bardziej wzrosła: spóźnieni rodzice nie tylko nie musieli płacić, ale także nie czuli się już zobowiązani do przepraszania lub tłumaczenia swoich działań.

Podobny mechanizm obserwowano w innych kontekstach, a także powielano eksperymentalnie w laboratoriach[34]. Generalnie badania sugerują, że silne regulacje wspomagane przez wymierne nagrody stanowiące odpowiednik wynagrodzenia sprawiają, że ludzie przestawiają się z działania nakierowanego na wspólnotę, które zakłada częściową rezygnację z własnych korzyści, na działanie egoistyczne[35]. Dodatkowo systemy oparte na zachętach ekonomicznych sprawiają, że ludzie zaczynają podejmować próby „ograniа" systemu. Związane jest to z faktem, że ludzie, jeżeli zacząć ich wynagradzać według ilościowych wskaźników, szybko odkrywają, że nie trzeba wcale robić tego, co ma reprezentować dany wskaźnik, lecz wystarczy maksymalizować samą jego wartość. Ujmując to inaczej, wskaźniki mają tendencję do autonomizacji względem celów, którym służą.

Odnieśmy to do systemu ratingu obywatelskiego. Jeżeli teoria wypierania motywacji jest słuszna, to system *citizen score* może okazać się receptą nie tyle na posłusznego obywatela, ile na zredukowanie postaw pro-wspólnotowych. Obywatele nie tylko przyjmą bardziej egoistyczne postawy, ale będą również dążyć do wykorzystania systemu. Już w tej chwili trwają próby rozszyfrowania konkretnych zasad działania systemu oceny obywatelskiej prowadzone m.in. przez zachodnich dziennikarzy.

Podobne spojrzenie na *citizen score*, choć z innej perspektywy, oferuje praca antropologa kultury Rogera Caillois pt. „Żywioł i ład"[36]. Autor przekonuje, że każde społeczeństwo zawierać musi elementy porządku (ładu) społecznego, ale nie może również obyć się bez elementów spontanicznych (żywiołu). Brak ładu oznacza dezintegrację systemu społecznego. Jednak przeregulowanie skutkować będzie również niewydolnością systemu społecznego związaną ze złożonością, ewentualnie ujawnionymi paradoksami regulacji, a w efekcie jego rozpadem.

Skrajna regulacja – a właśnie ją najprawdopodobniej przyniesie wdrożenie *citizen score* – tłumi jednostki kreatywne i innych „pozytywnych dewiantów" stanowiących źródło wielu korzystnych zmian społecznych, a także może utrudniać włączanie w struktury władzy jednostek charyzmatycznych, które – jeżeli uniemożliwi im się awans – mogą

[34] K. McGraw, *The Detrimental Effects of Reward on Performance: A Literature Review and a Prediction Model, [w]* M. Lepper i D. Greeene (red.), The Hidden Costs of Reward: New Perspectives of Human Behaviour, New York 1978, Lawrence Erlbaum Associates, ss. 33-65.

[35] D. Ariely, *Potęga irracjonalności. Ukryte siły, które wpływają na nasze decyzje*, Wrocław 2009, Wydawnictwo Dolnośląskie.

[36] R. Caillois, *Żywioł i ład, wyboru dokonał A. Osęka*, Warszawa 1973, Państwowy Instytut Wydawniczy.

stanowić zagrożenie dla ładu społecznego jako przywódcy przyszłych rewolt[37]. Teoretycznie można by zaprojektować rating premiujący zachowania pozytywnych dewiantów, problem polega jednak na tym, że (1) przypuszczalnie rozwiązanie takie premiowałoby również dewiacje negatywne, a także (2) wymagałoby określenia z góry, które dewiacje uznać należy za pożądane, co jest często niemożliwe do wykonania z wyprzedzeniem.

Obie koncepcje ukazują w różny sposób problem, z którym być może będą musiały zmierzyć się Chiny po wprowadzeniu ratingu. Generalnie Chiny kreują się na arenie międzynarodowej jako państwo, które planuje nie w perspektywie jednej kadencji politycznej (pięć lat), jednej dekady, czy nawet pokolenia, ale w wielu dekad. Dzięki rozciągniętej perspektywie czasowej Chiny jako system społeczny mogą czuć się odporne na czynniki, które wstrząsają społeczeństwami oraz kulturą państw zachodnio-europejskich. Jeżeli uznać takie ujęcie za trafne, oznacza to, że Chiny potrzebują mniej czynników spontanicznych, niż inne państwa, z którymi konkurują. Pytaniem otwartym pozostaje, czy Chiny mogą obyć się bez żywiołowości, dokonując regulacji zachowań, które dotychczas były poddane jedynie częściowej kontroli.

Chiński system ratingu obywatelskiego należy uznać za eksperyment społeczny na ogromną skalę. Nie jest zrozumiałe, jakie dokładnie korzyści władze chcą uzyskać dzięki silniejszej regulacji zachowań i działań swoich obywateli. Prawdopodobne wyjaśnienie, mówi, że przyjęto założenie, iż już w tej chwili społeczeństwo chińskie jest zdemoralizowane i ewentualne interwencje nie mogą pogorszyć morale obywateli: interpretacja taka pozostaje zgodna z dokumentami rządowymi, w których, w kontekście systemu scoringu przytaczane są dane na temat skrajnej korupcji społeczeństwa chińskiego. Przesłanki teoretyczne wskazują jednak, że państwo to ryzykuje stabilnością własnego systemu społecznego.

Eksperyment ten jest ryzykowny, gdyż nawet relatywnie krótka ekspozycja na bodźce wypierające motywację wewnętrzną niszczy dotychczas obowiązującą umowę społeczną. Innymi słowy, nawet kilkuletni eksperyment z ratingiem obywatelskim w skali państwa czy choćby prowincji może oznaczać potrzebę żmudnego usuwania jego skutków przez kolejne pokolenie.

Oczywiście pamiętać należy, że mamy tu do czynienia ze społeczeństwem, które w warstwie nie tylko politycznej, ale i obyczajowej już obecnie nagradza postawy zachowawcze oraz silnie sankcjonuje wszelkie odstępstwa od wyraźnych norm i rytuałów. Nie zostało naukowo wykazane, że zjawisko wypierania motywacji wewnętrznej obowiązuje w innych kręgach kulturowych niż zachodnioeuropejski. Neuropsychologowie sugerują, że nastawienie pro-wspólnotowe zakładające eliminację zachowań pasożytniczych typu „jazda na gapę" oraz poświęcanie części indywidualnych korzyści jest tym, co pozwoliło naszemu gatunkowi uzyskać przewagę nad innymi[38]. Niewykluczone, że współcześnie cechy te są tłumione w pewnych kręgach kulturowych lub skutecznie zastępowane przez odgórne systemy regulacji.

[37] Ostatni z zakomunikowanych problemów był w Chinach tradycyjnie rozwiązywany dzięki instytucji egzaminów cesarskich otwartych dla każdego. Obecnie dostrzegalne są pewne pozostałości tej tradycji w postaci egzaminów na stanowiska państwowe, jednak ich znaczenie wyraźnie maleje.

[38] Zob. np. M. Gazzaniga, *Istota człowieczeństwa. Co czyni nas wyjątkowymi*, Sopot 2011, Smak Słowa.

Istnieje też możliwość, że efekt wypierania motywacji wewnętrznych zachodzi dopiero wtedy, gdy osoba poddawana bodźcowaniu ma zaspokojone podstawowe potrzeby życiowe: badania nad wypieraniem motywacji prowadzone były głównie wśród obywateli społeczeństw rozwiniętych takich jak Izrael, Szwajcaria, czy USA, którzy nie mieli problemów z zaspokojeniem podstawowych potrzeb życiowych.

Przytoczone wątpliwości nie zmieniają faktu, że należy uważnie przyglądać się chińskiemu eksperymentowi, gdyż może mieć on istotne znaczenie dla sytuacji geopolitycznej. Chiny, ze względu na swój potencjał demograficzny, militarny i kulturowy, dzięki relacjom handlowym łączącym je z innymi krajami, a także wpływom politycznym zyskały status jednego z kluczowych podmiotów procesów globalnych. Wydawać się mogą gigantem, dla którego panowania zagrożeniem jest jedynie poziom wewnętrznej spójności. *Citizen score* może być czynnikiem, który tą spójność podkopie.

Rekomendacja: Należy śledzić wpływ eksperymentów z *citizen score* na integralność kulturową i społeczną Chin. Ewentualne powodzenie chińskiego eksperymentu nie powinno być traktowane jako dowód, że analogiczny system sprawdziłby się w społeczeństwach o odmiennej kulturze. **[10/5]**

Kolejne postępy rewolucji *blockchain* w administracji publicznej w Estonii

KOMUNIKAT

30 kwietnia 2017. Od przeszło dwóch lat w Estonii korzystać można z usług notarialnych za pośrednictwem cyfrowej platformy opartej na technologii blockchain. Jej specyfika polega na tym, że każdy użytkownik jednocześnie przechowuję historię zmian dokumentacji dokonywanych przez innych użytkowników, jednocześnie mając dostęp jedynie do „swoich" danych. W konsekwencji – na gruncie dziś dostępnych technologii – jest niemal niemożliwe, aby sfałszować tak przechowywane dane. Jednocześnie użytkownicy mają szybki i wygodny dostęp do potrzebnych usług. W połowie marca wpływowy branżowy portal medyczny PWS poinformował, że Estonia wprowadza także technologię blockchain w służbie zdrowia[39].

Tradycyjny notariusz swoim autorytetem poświadczał autentyczność składanych w jego obecności oświadczeń i pilnował zgodności podejmowanych działań z prawem. W technologii *blockchain* zgodność z prawem, a raczej z procedurami administracyjnymi, jest pilnowana przez cyfrowy algorytm. Natomiast autorytet instytucjonalny tradycyjnego notariusza w technologii *blockchain* jest zastąpiony przez rozmnożenie złożonego oświadczenia po wszystkich pozostałych blokach w sieci. Czyli przykładowo: trudno będzie sfałszować testament, ponieważ potencjalnie cały pozostały łańcuch sieci będzie przechowywał jego inną, wcześniejszą chronologicznie wersję. W Estonii można za pomocą cyfrowego notariusza rejestrować już np. obieg faktur, umowy cywilno-prawne, zawarcie małżeństwa, narodziny dziecka[40].

W kontekście służby zdrowia technologia *blockchain* zapewnić może błyskawiczny dostęp do zdrowotnej historii obywatela (grupy krwi, przebytych chorób, branych leków, ewentualnych alergii etc.) na wypadek interwencji medycznej, czy na potrzeby postępowania o ubezpieczenie. Technologia ta oferować może także wsparcie diagnostyczne na poziomie pojedynczych osób, grup spokrewnionych (ważne przy chorobach genetycznych), czy też wspólnot sąsiedzkich (istotne przy chorobach zakaźnych). Kluczowe znaczenie ma fakt, że w technologii *blockchain* działania te odbywać się mogą szybko i przy zapewnieniu wysokiego poziomu bezpieczeństwa przechowywanych danych.

Prognoza. Należy spodziewać się dalszego wprowadzania technologii *blockchain* w kolejnych dziedzinach administracji publicznej zarówno w Estonii, jak i w innych państwach. Prawdopodobnie towarzyszyć temu będą zintensyfikowane próby wyszukiwania słabych punktów zabezpieczeń i innych podatności na atak hakerski.

Rekomendacja. Należy monitorować funkcjonowanie usług e-administracji opartych o architekturę blockchain, zwłaszcza pod kątem faktycznej niepodatności na ataki

[39] J. Marshall, *Estonia prescribes blockchain for healthcare data security*, 16.03.2017, http://pwc.blogs.com/health_matters/2017/03/estonia-prescribes-blockchain-for-healthcare-data-security.html [odczyt: 30.04.2017].

[40] I. Allison, *Bitnation and Estonian government start spreading sovereign jurisdiction on the blockchain*, 8.02.2017, dostępne: http://www.ibtimes.co.uk/bitnation-estonian-government-start-spreading-sovereign-jurisdiction-blockchain-1530923 [odczyt: 29.04.2017].

hackerskie i próby fałszerstwa. Estonia od dekady jest pionierem w implementacji usług e-administracji i nie bez powodu niemal dziesięć lat temu stała się ona obiektem poważnego cyber-ataku, który sparaliżował część cyber-infrastruktury tego państwa. Należy potraktować Estonię jako swoisty poligon, na którym można zaobserwować, jak radzą sobie w praktyce systemy oparte na architekturze *blockchain* i na ile wiarygodne są zapewnienia o ich bezpieczeństwie. **[3/12]**

Postęp w technologii klonowania głosu ludzkiego zagrożeniem dla bezpieczeństwa państwa

KOMUNIKAT

4 maja 2017. W chwili obecnej na rynek wprowadzane są systemy klonowania ludzkiego głosu, które z powodzeniem oszukują automatyczne systemy rozpoznawania mowy.

Metoda klonowania głosu polega na wychwytywaniu wzorca mowy danej osoby: wystarczy nagranie około 160 fraz, by sklonować głos dowolnego człowieka[41]. Na podstawie wzorca można stworzyć dowolną wypowiedź w określonym języku. Możliwa jest jednocześnie manipulacja takimi parametrami jak szybkość lub intonacja wypowiedzi. Przykładowe aplikacje to Lyrebird kanadyjskiego start-up o tej samej nazwie[42] oraz projekt o nazwie VoCo, który rozwija spółka Adobe Systems Incorporated[43].

Sama imitacja dźwięku nie jest nowością. Nowością jest niezwykle niska cena usługi, jej szybkość i niezawodność. Do niedawna nagranie słownika dla sztucznego głosu (na przykład dla osoby go pozbawionej) było procesem wymagających przynajmniej 8 godzin pracy w studio i kosztowało 3 tys. EUR[44]. Dziś to samo można zrobić zdalnie, przez telefon, odczytując zadane zdania. Sam głos generowany jest w przeciągu sekund. W przypadku oprogramowania takiego jak Festvox[45] wystarczy pięciominutowe nagranie pobrane z YouTube, by stworzyć wiarygodny klon głosu. Jak wykazali badacze z University of Alabama (Birmingham), klon głosu uzyskanego tą metodą oszukiwał oprogramowanie biometryczne stosowane przez banki jako zabezpieczenie dostępu do konta w ponad 80% przypadków[46]. Ludzie dawali się oszukać tylko w połowie przypadków (test przeprowadzono przy wykorzystaniu darmowego i ogólnie dostępnego programu).

---

[41] Taki wynik osiągnęło oprogramowanie CandyVoice opracowane dla klonowania w językach francuskim i angielskim; aktualnie jest ono w fazie betatestów.

[42] https://lyrebird.ai/demo [odczyt: 4.05.2017].

[43] Pozwala on na edycję zapisów ludzkich wypowiedzi, w tym na zmianę ich znaczenia; istotne jest to, że program umożliwia edycję dźwięku w formacie tekstowym: nie musimy edytować samego dźwięku w formacie wizualizacji fali dźwiękowej, lecz możemy przestawiać słowa w tekście korespondujące z poszczególnymi dźwiękami, a program sam dokonuje przeskładu wypowiedzi. VoCo pozwala również na wstawianie do wypowiedzi słów, które nie zostały wypowiedziane. Innymi słowy, VoCo robi z dźwiękiem to samo, co PhotoShop robił z obrazem.

[44] Usługę dostarcza np. Acapela Group, zob. *Cloning voices. Imitating people's speech patterns precisely could bring trouble*, "The Economist", 20.04.2017 http://www.economist.com/news/science-and-technology/21721128-you-took-words-right-out-my-mouth-imitating-peoples-speech-patterns?fsrc=scn/tw/te/bl/ed/cloningvoicesimitatingpeoplesspeechpatternspreciselycouldbringtroubl e [odczyt: 4.05.2017].

[45] Jest to darmowe oprogramowanie rozwijane na Carnegie Mellon University http://www.festvox.org/ [odczyt: 4.05.2017].

[46] K. Shonesy, *UAB research finds automated voice imitation can fool humans and machines*, 25.10.2015 https://www.uab.edu/news/innovation/item/6532-uab-research-finds-automated-voice-imitation-can-fool-humans-and-machines [odczyt: 4.05.2017].

Komentarz: Rozwój systemów służących do edycji i klonowania głosu na podstawie nagrań dostępnych w przestrzeni medialnej otwiera zupełnie nowe możliwości w dziedzinie wojny informacyjnej, w tym szerzenia fałszywych wiadomości. O ile współczesny odbiorca jest przyzwyczajony do fotomontaży i zdjęć poddanych edycji, o tyle brak w społeczeństwie wiedzy o możliwości dokonywania podobnych manipulacji dźwięku. Jeszcze bardziej niepokojąca jest możliwość automatyzacji procesu edycji (np. możliwość skoordynowanego ataku hakerskiego mającego na celu podmianę wypowiedzi w różnych serwisach informacyjnych).

W świetle rozwoju technologii klonowania dźwięku wszelkie zabezpieczenia bazujące na rozpoznaniu głosu powinny zostać uznane za niewystarczające. Nawet jeśli technologia ta nie jest w stanie oszukać człowieka, to należy założyć, że w niedługim czasie stanie się to możliwe.

Rekomendacje:

Zabezpieczenia dostępu bazujące na rozpoznawaniu mowy należy uznać za niewystarczające, a wiedzę o istnieniu możliwości klonowania głosu należy uwzględnić w szkoleniach z zakresu bezpieczeństwa. Technologie klonowania i edycji mowy rozwijane są obecnie dla popularnych języków takich jak angielski czy francuski. Ustalić należy, czy takie rozwiązania są rozwijane dla języka polskiego, ewentualnie czego wymagałoby stworzenie tego typu oprogramowania.

Warto rozważyć opracowanie własnego systemu klonowania i rozpoznawania mowy (lub dokonanie inżynierii odwrotnej istniejącego oprogramowania) w celu lepszego zrozumienia technologii i opracowania ewentualnych zabezpieczeń. Pomocne w tym zakresie mogą okazać się wynik prac Polskiej Platformy Bezpieczeństwa Wewnętrznego prowadzonych we współpracy z Future Voice System nad systemami rozpoznawania i przetwarzania mowy polskiej na tekst[47]. **[10/4]**

[47] http://futurevoicesystem.pl/realizowane-projekty/system-rozpoznawania-mowy/ [odczyt: 4.05.2017].

Nowa technika wspierająca mobilność robotów – pasożytowanie na zwierzętach

SYGNAŁ

13 maja 2017. Zespół południowokoreańskich i singapurskich badaczy przeprowadził udany eksperyment, który polegał na stworzeniu hybrydy robota z żółwiem[48]. Przed głową zwierząt umieszczone zostały zestawy 5 diod LED zamontowanych co 30 stopni i podajniki żywności. Celem było stworzenie mechanizmu nagradzania żółwi przysmakami za podążenie w kierunku, w którym znajduje się świecąca dioda. Zwierzęta zostały w wyniku treningu uwarunkowane do precyzyjnego wykonywania poleceń. Istotne jest też to, że źródłem energii elektrycznej dla takich robotów może się stać ruch zwierząt lub emitowane przez nie ciepło.

Komentarz: „Pasożytowanie" na zwierzętach to kolejna – po gąsienicach, kołach czy nogach – studiowana przez robotyków technika, która zwiększa mobilność robotów lądowych. Roboty „pasożytujące" są w stanie dostać się do miejsc niedostępnych dla innych robotów i ludzi[49]. Co więcej, rozwiązanie polegające na stworzeniu hybrydy jest mniej inwazyjne i tym samym mniej problematyczne etycznie niż rozwijane równolegle techniki sterowania zwierzętami za pomocą elektrod wszczepionych bezpośrednio w ich mózgi.

Rekomendacja: Warto przeanalizować, czy stosowane w Polsce systemy bezpieczeństwa fizycznego są w stanie wykrywać miniaturowe roboty szpiegowskie – w tym roboty „pasożytujące" na zwierzętach. **[4/3]**

[48] D.-G. Kim, S. Lee, C.-H. Kim, S. Jo i P.-S. Lee, *Parasitic Robot System for Waypoint Navigation of Turtle*, „Journal of Bionic Engineering", Volume 14, Issue 2, 4.2017, ss. 327-335, https://doi.org/10.1016/S1672-6529(16)60401-8 [odczyt abstraktu: 13.05.2017]; tekst przedstawił: T. Revell, *Robot riders hitch lifts on hungry turtles*, „New Scientist", 13.05.2017, s. 10; artykuł jest również dostępny na stronie: https://www.newscientist.com/article/mg23431254-400-parasitic-robot-controls-turtle-its-riding-by-giving-it-snacks/ [odczyt: 13.05.2017].

[49] Uzasadnieniem dla prowadzenia badań nad sterowaniem zwierzętami są zazwyczaj operacje poszukiwawcze i ratunkowe.

Grupa hakerska The Shadow Brokers upubliczniła pakiet *exploitów* systemów operacyjnych Microsoftu, które miały zostać wykradzione NSA

KOMUNIKAT

4 maja 2017 (zaktualizowany 31 maja 2017). Dnia 14 kwietnia br. grupa hakerska The Shadow Brokers upubliczniła zestaw programów typu *exploit* umożliwiających łamanie zabezpieczeń systemów operacyjnych Windows (różne wersje). Jak podaje grupa, pakiet narzędzi został wykradziony NSA[50]. Pakiet miał być wcześniej wystawiony na czarnym rynku, ale w związku z brakiem kupca gotowego zapłacić żądaną sumę, materiał miał zostać udostępniony ogółowi internautów.

Zestaw programów pochodzi z roku 2013, a więc przypuszczalnie nie pozwala na przełamywanie zabezpieczeń systemu Windows 10. Jak doniósł sam Microsoft, jego systemy operacyjne zostały zabezpieczone przed atakami z użyciem wielu programów znajdujących się w pakiecie już dawno temu i to bez ostrzeżenia ze strony NSA. Pierwsza aukcja *exploitów* została ogłoszona 8 stycznia br. Przynajmniej od tego momentu NSA musiała zdawać sobie sprawę, że wyciekły jej narzędzia i miała czas na ostrzeżenie Microsoftu o zagrożeniu[51]. Microsoft nie poinformował jakoby został ostrzeżony o zagrożeniu. Jednak wypuszczenie łatki MS17-010 dnia 14 marca, na miesiąc przez udostępnieniem pakietu *exploitów*, sugeruje, że tak właśnie się stało. Brak informacji o podziękowaniach dla odkrywcy luk bezpieczeństwa sugeruje, że ostrzeżenie przekazała NSA.

Za najbardziej niebezpieczny element pakietu wskazać należy opracowany przez należący do NSA The Equation Group program FUZZBUNCH. Pozwala on przeprowadzać zautomatyzowane ataki na Windows XP, 7 i 8.x, oraz Windows Server NT, 2000, 2003, 2008 i 2012. Najnowsze systemy są zabezpieczone, nie ma jednak gwarancji, że po kolejnej aktualizacji Windows 10 nie zostaną przywrócone jego podatności, co ma związek z faktem, że kod tego systemu zawiera obszerne fragmenty kodu Windowsa NT[52]. Należy założyć, że istniejące oprogramowanie stanie się podstawą do opracowania kolejnej generacji *exploitów*, wirusów lub robaków. Microsoft zalecił aktualizację Windows 10 lub pobranie pakietu poprawek bezpieczeństwa.

Komentarz: W kontekście opisywanej sytuacji nasuwają się dwie hipotezy. Pierwsza mówi o krecie w NSA. Druga jest taka, że pakiet został wypuszczony celowo przez NSA: szkody wyrządzone przez jego upublicznienie są niewielkie, a takie działanie daje

[50] *Latest Exploit Dump By Shadow Brokers Contains Easy-To-Use Windows Exploits, Most Already Patched By Microsoft*, 17.04.2017, https://www.techdirt.com/articles/20170416/08190937159/latest-exploit-dump-shadow-brokers-contains-easy-to-use-windows-exploits-most-already-patched-microsoft.shtml [odczyt: 4.05.2017].

[51] *The Shadow Brokers Vulnerability Equities Process: NSA Has Had at Least 96 Days to Warn Microsoft About These Files*, 14.04.2017, https://www.emptywheel.net/2017/04/14/the-shadow-brokers-vulnerability-equities-process-nsa-has-had-at-least-96-days-to-warn-microsoft-about-these-files/ [odczyt: 4.05.2017].

[52] A. Goliński, *FUZZBUNCH nie daje szans Windows: cyberbronie NSA dostępne w Sieci*, 14.04.2017 https://www.dobreprogramy.pl/FUZZBUNCH-nie-daje-szans-Windows-cyberbronie-NSA-dostepne-w-Sieci,News,80523.html [odczyt: 4.05.2017].

wyobrażenie potencjału tej organizacji, która jak dotąd nie miała sposobu, by zademonstrować swoją sprawność na polu cyber-wojny.

Zmasowany atak typu *ransomware* przeprowadzony przy pomocy programu WannaCry z maja br., którego ofiarą padło między innymi brytyjskie National Health Service oraz hiszpańska Telefónica wykorzystał *exploit* EternalBlue należący do pakietu upublicznionego 14 kwietnia[53]. Fakt, że za pomocą tego programu udało się skutecznie zaatakować ponad 300 tys. komputerów z systemami operacyjnymi Microsoftu na świecie świadczy dobitnie o tym, z jakim opóźnieniem użytkownicy aktualizują zabezpieczenia (łatka z marca br. zapobiegała atakowi).

Rekomendacje:

1. Pakiet *exploitów* opublikowany przez hakerów stanowi próbkę możliwości w zakresie prowadzenia cyber-wojny, jakimi dysponuje NSA. Ma on już cztery lata, ale daje pewne wyobrażenie (na zasadzie ekstrapolacji) o obecnym potencjale agencji i jako taki powinien stać się obiektem zainteresowania rodzimych organizacji rozwijających arsenał do prowadzenia cyber-wojny.
2. Atak WannaCry pokazuje, że newralgicznym punktem w zabezpieczeniach systemu są ludzie, który nieregularnie aktualizują oprogramowanie. **[10/5]**

[53] A. Hern i S. Gibbs, *NHS seeks to recover from global cyber-attack as security concerns resurface*, "The Guardian", 13.05.2017, https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20 [odczyt: 31.05.2017].

Molekuła z potencjałem wykorzystania w komputerach kwantowych

SYGNAŁ

18 maja 2017. W laboratoriach IBM została zsyntetyzowana nowa cząsteczka – triangulen – mająca potencjał do wykorzystania przy konstrukcji komputerów kwantowych[54]. Badacze z IBM oraz Univeristy of Warwick, przy użyciu mikroskopu sił atomowych oraz skaningowego mikroskopu tunelowego, manipulując pojedynczymi atomami, stworzyli molekułę, której budowa jest częściowo zbliżona do grafenu. Możliwość syntezy triangulenu została teoretycznie przewidziana w latach 1950., ale do tej pory nie udawało się tego dokonać.

Komentarz. Triangulen posiada właściwości magnetyczne, które sprawiają, że może się nadawać do przechowywania informacji oraz wykorzystania przy budowie komputerów kwantowych. Zakończone powodzeniem prace w tym zakresie są kolejną wskazówką, że w niedługim czasie czeka nas przełom na polu tworzenia komputerów kwantowych. Pojawienie się tego rodzaju komputerów będzie miało istotny wpływ na bezpieczeństwo państwa – m.in. w kontekście efektywności kryptografii. Należy podkreślić, że IBM tworzy prototyp takiego komputera[55]. **[8/10]**

[54] P. Ball, *Elusive triangulene created by moving atoms one at a time*, „Nature" 542, 16.02.2017, s. 284–285, http://www.nature.com/news/elusive-triangulene-created-by-moving-atoms-one-at-a-time-1.21462 [odczyt: 18.05.2017]; N. Pavliček i in., *Synthesis and characterization of triangulene*, „Nature Nanotechnology" 12, s. 308–311 (2017); N. Pavliček, *IBM & Warwick Image Highly Reactive Triangular Molecule for the First Time, 13.02.2017,* https://www.ibm.com/blogs/research/2017/02/ibm-warwick-image-highly-reactive-triangular-molecule-for-the-first-time [odczyt: 18.05.2017].

[55] http://www.research.ibm.com/quantum [odczyt: 18.05.2017].

Opryski tymczasowo zmieniające cechy roślin: krok w stronę inżynierii genetycznej bez trwałej modyfikacji kodu genetycznego

KOMUNIKAT

28 kwietnia 2017. Zespół badaczy z University of Queensland w Brisbane (Australia) stworzył oprysk, który umożliwia czasowe, ale względnie długotrwałe dezaktywowanie wybranych genów w roślinie[56]. Podobna technologia była od kilku lat rozwijana przez koncern biotechnologiczny Monsanto[57]. Istota tej technologii polega na wykorzystaniu sztucznie wytworzonych, krótkich odcinków RNA, które „doczepiają się" do docelowych genów rośliny. Efektem tego jest „wyciszenie" wybranych genów: przestają one wywierać wpływ na rozwój rośliny.

Preparaty testowane przez Monsanto działały maksymalnie przez kilka dni, tymczasem oprysk stworzony przez zespół z Australii (nazywany BioClay) zabezpieczał uprawy tytoniu przez ponad 20 dni, dezaktywując przez ten czas geny wirusa w komórkach roślinnych. Było to możliwe dzięki wykorzystaniu w oprysku nie tylko RNA, ale też nanocząsteczek minerałów.

Komentarz: Technologia wyciszania genów jest krokiem w kierunku inżynierii genetycznej nie wymagającej modyfikacji RNA/DNA. Technologia ta najprawdopodobniej szybko zostanie skomercjalizowana i wdrożona w rolnictwie jako alternatywa (bądź uzupełnienie) dla wykorzystywanych do tej pory pestycydów. Oznacza to zatem, że uzyska ona wsparcie w obszarze badań i rozwoju, co może w niedługiej przyszłości doprowadzić do wydłużenia okresu działania oprysku. Istnieje szerokie spektrum potencjalnego zastosowania: od wykorzystania zmodyfikowanych oprysków jako broni biologicznej skierowanej przeciwko uprawom w trakcie wojen konwencjonalnych, aż po tworzenie sprejów, które będą działały w analogiczny sposób na ludzi (choć nie wiadomo, żeby ktokolwiek w chwili obecnej prowadził takie prace).

Warto zwrócić uwagę, że technologia tego rodzaju może być potencjalnie wykorzystana przez zorganizowane grupy przestępcze zajmujące się uprawą roślin służących do wytwarzania narkotyków (mak, konopie, koka), jeśli pozwoli to na zwiększenie plonów, wzmocnienie niektórych cech roślin albo przeciwdziałanie opryskom realizowanym przez siły policyjne. Z tego powodu technologia ta może być rozwijana poza kontrolą państwa.

Podstawową barierą w upowszechnieniu tej technologii jest koszt wytworzenia RNA. Jeszcze kilka lat temu wytworzenie 1 grama RNA wymagało nakładów rzędu 100 tysięcy dolarów. Wyraźne jest jednak dążenie do radykalnego obniżenia tej ceny. Firmy

[56] N. Mitter, El. A. Worrall, K. E. Robinson, P. Li, R. G. Jain, Ch.Taochy, S. J. Fletcher, B. J. Carroll, G. Q. (Max) Lu i Z. Ping Xu, *Clay nanosheets for topical delivery of RNAi for sustained protection against plant viruses*, „Nature Plants" 3, 2017; M. Le Page, *Gene-silencing spray lets us modify plants without changing DNA*, https://www.newscientist.com/article/2117460-gene-silencing-spray-lets-us-modify-plants-without-changing-dna [odczyt: 28.04.2017]; J. Condliffe, *Spray-On RNA Protects Plants from Viruses for Weeks*, https://www.technologyreview.com/s/603330/spray-on-rna-protects-plants-from-viruses-for-weeks/ [odczyt: 28.04.2017].

[57] A. Regalado, *The Next Great GMO Debate*, https://www.technologyreview.com/s/540136/the-next-great-gmo-debate/ [odczyt: 28.04.2017].

biotechnologiczne, takie jak amerykańska APSE, dążą to osiągnięcia stanu, w którym koszt 1 grama RNA zostanie zredukowany do 2 dolarów.

Rekomendacje:

1. Należy monitorować prace rozwojowe oraz wykorzystania tej technologii przez duże koncerny biotechnologiczne (w rodzaju Monsanto).

2. Szczególną uwagę należy zwrócić na ewentualny spadek kosztów wytwarzania tego typu oprysków. **[8/10]**