Biuletyn Ośrodka Studiów nad Wyzwaniami Cywilizacyjnymi
CBB ASzWoj
Numer 2 | marzec 2017

W numerze:

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

USA planują utworzenie cybernetycznego komponentu Gwardii Narodowej

KOMUNIKAT

24 marca 2017. W USA rozważany jest projekt stworzenia cybernetycznego komponentu Gwardii Narodowej. Podobne struktury z powodzeniem funkcjonują już w Estonii. Rozwiązanie takie pozwoliłoby na częściowe wykorzystanie umiejętności osób pracujących w sektorze prywatnym, a także może okazać się bardzo efektywne w obronie cybernetycznej w przypadku skoordynowanych ataków na dużą skalę. Obecnie w USA obserwowany jest znaczy niedostatek zasobów w ochronie cybernetycznej i rosnąca różnica potencjału pomiędzy zdolnościami ofensywnymi i defensywnymi tego kraju. Przejawem problemów w tej sferze był brak reakcji na złamanie w 2014 roku zabezpieczeń Office of Personnel Management (amerykańska agencja rządowa zarządzająca kadrami administracyjnymi) i wykradzenie danych dotyczących 18 milionów Amerykanów, w tym informacji pozyskanych w czasie procedur sprawdzających personel służb specjalnych.

Rekomendacje:

1. W procesie opracowywania zadań i funkcji WOT należy rozważyć powołanie cybernetycznego komponentu defensywnego, którego zadaniem byłoby wsparcie obrony cybernetycznej infrastruktury kraju, a także zwalczanie ataków cybernetycznych na poziomie taktycznym.
2. Należy dokonać szczegółowej analizy rozwiązań umożliwiających wykorzystanie potencjału i umiejętności członków Wojsk Obrony Terytorialnej w aspekcie cybernetycznym w koordynacji z Centrum Operacji Cybernetycznych MON.
3. W przypadku ujęcia kwestii cybernetycznych w problematyce budowy WOT, należy rozważyć możliwość wykorzystania przedmiotowych zdolności w trakcie pokoju w celu zwiększenia świadomości i odporności na ataki cybernetyczne, prowadzenia szkoleń, a także testów penetracyjnych i audytów. **[2/3]**

Nowa globalna strategia Facebook Inc.

KOMUNIKAT

21 marca 2017. W dniu 16 lutego 2017 założyciel serwisu Facebook Marc Zuckerberg opublikował manifest „Building Global Community”[1]. Ten bezprecedensowy tekst jest strategią rozwoju globalnego serwisu społecznościowego na najbliższe lata, gdzie główny nacisk zostanie położony na wsparcie działania różnych społeczności. Strategia ujawnia szereg projektów badawczo-rozwojowych oraz nowych funkcjonalności serwisu, które już teraz mają bezpośredni wpływ na zachowania społeczne, zmiany polityczne i w konsekwencji na bezpieczeństwo narodowe.

Wykaz najbardziej kontrowersyjnych nowych funkcjonalności serwisu:

1. **Przetwarzanie języka naturalnego** – użycie metod analizy danych niestrukturalizowanych (posty, komentarze, zdjęcia, pliki video, linki itp.), aby automatycznie identyfikować wiadomości przekazywane pomiędzy użytkownikami, które są niezgodne z polityką serwisu. Obecnie, według naszej wiedzy, tego typu analizy są wykonywane ręcznie przez redaktorów serwisu na podstawie doniesień użytkowników. Planowany system ma takie informacje identyfikować automatycznie i powiadamiać zespół redakcyjny. Testowana obecnie wersja systemu już automatycznie identyfikuje około 1/3 wszystkich alertów. Głównym problemem w opracowaniu tego systemów jest rozumienie języka naturalnego[2].
2. **Zarządzanie informacją** w kontekście problemu uwzględnienia różnorodności punktów widzenia (tzw. filter bubbles) oraz problemu wiarygodności publikowanych informacji (tzw. fake news). Planowane jest zastosowanie algorytmów, które będą:
    - funkcjonowały w sposób zbliżony do filtrów spamów, aby wykluczyć niepożądane wiadomości,
    - dodawały informacje uzupełniające daną wiadomość o alternatywne punkty widzenia,
    - uzupełniały daną wiadomość o weryfikację faktów (ang. fact checkers),
    - redukowały publikowanie informacji o charakterze sensacyjnym (ang. sensationalism)[3].
3. **Wspieranie aktywności obywatelskiej –** wspieranie uczestnictwa w wyborach poprzez:
    - informowanie o wyborach,
    - wsparcie procesu rejestracji do wyborów[4],
    - wsparcie wymiany informacji pomiędzy kandydatami a wyborcami.

Wnioski i rekomendacje

Narzędzia rozwijane przez Facebook pozwalają w sposób automatyczny, w dużej skali (nawet całego społeczeństwa) na sterowanie przekazem informacyjnym i aktywizację w trakcie wyborów. Oznacza to, że Facebook, kierowany określoną ideologią, może

w przyszłości wpływać na wyniki wyborcze w wybranych państwach i w ten sposób mieć wpływ na zmiany polityczne.

Ponadto należy zwrócić uwagę na zadziwiające zdanie w sekcji Safe Community (Bezpieczna Wspólnota): "*our community should **be able to help during wars***" („*nasza wspólnota powinna być w stanie pomagać podczas wojen*"). Oznacza to, że Facebook planuje zbudowanie funkcji serwisu działających aktywnie w stanie wojny!

Rekomendacje:

1. Stały monitoring rozwijanych funkcjonalności serwisu.
2. Monitorowanie strategii rozwoju firmy, zmian właścicielskich, oraz promowanych ideologii.
3. Monitorowanie skali aktywności i zaangażowania obywateli RP.
4. Rozważenie opracowania narzędzi zakłócających działanie algorytmów serwisu.
5. Opracowanie procedur potencjalnego wyłączenia działania serwisu na terenie RP w sytuacji wprowadzenia stanu wojennego. **[12/3]**

Ekspansja rosyjskiego serwisu VKontakte w polskim Internecie

ANALIZA

Rosyjski serwis społecznościowy VKontakte w ostatnich miesiącach rozwija się intensywnie w polskim Internecie. Serwis ten jest pod całkowitą kontrolą putinowskiego oligarchy Aliszera Usmanowa, który należy do najbogatszych ludzi w Rosji. Według przeprowadzonych analiz z Polski łączy się z VKontakte około 500 tys. użytkowników, w tym szacowana liczba Polaków nie przekracza obecnie 200 tys. Polscy użytkownicy tego serwisu to głównie młodzież z ugrupowań narodowych i skrajnie prawicowych.

Spółka VKontakte: historia i relacje własnościowe

Serwis społecznościowy VKontakte (ros. ВКонтáкте, dalej VK) został uruchomiony 10 października 2006 r. jako narzędzie do nawiązywania kontaktów pomiędzy studentami rosyjskich uczelni wyższych. Siedziba spółki (forma działalności VK to spółka z ograniczoną odpowiedzialnością) mieści się w Petersburgu. Założycielem VK jest zwany „rosyjskim Zuckerbergiem”[5] Paweł Durow (ur. 1984 r. w Leningradzie).

Obecnie serwis VK należy w 100% do Grupy Mail.Ru. Ten kluczowy na rynku usług internetowych w rosyjskojęzycznym Internecie podmiot skupił do września 2014 roku wszystkie udziały VK[6]. W lutym 2016 roku spółka MegaFon kupiła pakiet kontrolny Grupy Mail.Ru (63.8% akcji), co oznacza, że ta spółka telekomunikacyjna przejęła również kontrolę nad VK. Oligarcha Aliszer Usmanow posiada pakiet kontrolny spółki MegaFon. W efekcie zmian własnościowych VK jest częścią zbioru podmiotów, które **zapewniają infrastrukturę i kontrolują obieg informacji w znacznej części rosyjskojęzycznego Internetu**.

Zgodnie z danymi rosyjskiej firmy Brand Analytics twórcami informacji publikowanych na VK są w znaczącej większości ludzie do 34 roku życia (ponad 85% użytkowników, którzy podali swój wiek)[7]. Do starszego audytorium skierowany jest drugi najważniejszy serwis społecznościowy w Rosji czyli Odnoklasniki. Również on należy do Grupy Mail.ru, co jeszcze bardziej podkreśla centralne znaczenie, które dla rosyjskojęzycznego Internetu ma działalność tej grupy podmiotów gospodarczych.

Funkcjonalności VK

Od początku istnienia twórcom serwisu zarzucano, że skopiowali funkcjonalności i interfejs Facebooka oraz że do tej pory model biznesowy obu spółek jest podobny[8]. VK jest obecnie dostępny w „ponad 80” wersjach językowych[9]. Jedną z nich jest „język sowiecki”, w którym „przyjaciół” zastępują „towarzysze”. Serwis ma też profesjonalnie przygotowaną polską wersję językową. Serwis łączy w sobie rolę: Facebooka (w tym agregowanie informacji, które mają zainteresować użytkowników), stron z memami, radia *online*, odtwarzacza filmów, telewizji internetowej. Treści są zazwyczaj wgrywane bezpośrednio na serwery VK – obrońcy praw własności intelektualnej muszą korzystać z często nieskutecznej ścieżki odwoływania się do prawa Federacji Rosyjskiej i tego, jak sądy chronią na jej terytorium prawa autorskie. Spółka w nagłośnionych sprawach podporządkowywała się prawu Federacji oraz skargom podmiotów zagranicznych[10]. Właściciele strony zadbali, by nie można już było mówić o VK, że jest to strefa niczym

nieskrępowanej wolności oraz lekceważenia prawa[11]. Można jednak zaobserwować, że VK ma bardziej liberalne podejście do praw autorskich niż Facebook i inne podmioty działające w Internecie. Może to być znacząca zachęta do korzystania z VK jako źródła pirackich treści.

Dane zbierane przez VK i polityka prywatności

Zgodnie z „Zasadami" działania VK[12], na przestrzeganie których użytkownik wyraża zgodę w czasie rejestracji, VK ostrzega, że prawo Federacji Rosyjskiej decyduje o sposobie traktowania danych osobowych użytkowników i innych danych tworzonych przez nich lub powstających w trakcie ich pobytu na stronach VK. Spółka przyznaje, że nie tylko sądy, ale również organy wymiaru sprawiedliwości i inne instytucje w „przypadkach opisanych w prawie FR" mają prawo zażądać ujawniania danych użytkowników i informacji na ich temat. Dane pozostawiane przez użytkowników mogą być też przekazywane „stronom trzecim", by umożliwić im ochronę praw i interesów innych użytkowników oraz „przeciwdziałanie, kontrolowanie/badanie i/lub zwalczanie działań nielegalnych". Może tu chodzić o podmioty gospodarcze, które zajmują się analizowaniem danych z mediów społecznościowych na rzecz innych podmiotów – w tym instytucji państwowych. W „Zasadach" VK odrzuca swoją odpowiedzialność za rodzaj i pochodzenie treści publikowanych przez użytkowników. Zgodnie z „Zasadami" odpowiedzialność za zawartość danej podstrony ponosi jej „właściciel" – czyli zarejestrowany użytkownik.

„Polityka prywatności" VK zakłada[13], że serwis gromadzi i przetwarza dane osobowe użytkowników niezbędne do zarejestrowania się na stronie: imię, nazwisko, płeć, nr telefonu oraz/lub adres poczty elektronicznej. Do danych osobowych przetwarzanych przez stronę zaliczają się też informacje przekazane na swój temat przez użytkownika – serwis prosi o podanie: statusu związku, daty i miejsca urodzenia, adresu domowego, wykształcenia.

VK przetwarza też inne informacje, które powstają w trakcie pobytu użytkowników na stronie. Dotyczą one urządzeń, adresu IP, systemu operacyjnego, przeglądarki, geolokacji, dostawcy usług internetowych, listy kontaktów, „danych pozyskanych za pomocą kamery, mikrofonu i innych podobnych urządzeń"[14]. Przetwarzane są też informacje zgromadzone za pomocą ciasteczek oraz wszelka zawartość stworzona przez użytkownika. Co istotne, VK zbiera i przetwarza informacje pozostawione przez innych użytkowników na stronie danej osoby – ze szczególnym uwzględnieniem „notatek wykonanych na nagraniach wideo oraz zdjęciach"[15]. Istotnym punktem „Zasad" są reguły usuwania danych dopiero po 210 dniach po podjęciu przez użytkownika decyzji o likwidacji konta[16]

VK na świecie i w Polsce

Zgodnie z podstawowymi danymi podawanymi przez VK[17] ten serwis społecznościowy ma:

- 95 milionów regularnych (aktywnych miesięcznie) użytkowników;
- pięć miliardów wiadomości jest przesyłanych dziennie za jego pomocą;
- użytkownicy dokonują dziennie jednego miliarda „polubień";
- 77% użytkowników korzysta z serwisu za pomocą telefonów i tabletów.

Zgodnie z danymi zebranymi i udostępnianymi przez należący do amerykańskiej spółki analitycznej „Alexa internet Inc."[18] serwis VK jest najpopularniejszą stroną w Rosji, 15. na świecie i 10. w Polsce.

Statystyki spółki Alexa dla naszego kraju wskazują, że przeciętny użytkownik spędza dziennie na tej stronie nieco ponad 12 minut. W tym czasie odwiedza przeciętnie 5.23 strony. Te same dane odpowiednio dla „Google.pl" i „Facebook.com" (1. i 3. miejsce w Polsce[19]) wskazują, że użytkownicy spędzają na tych stronach 8:19 oraz 14:50 minut, w tym czasie średnio odwiedzają 9.38 i 5.63 strony. Ranking Alexa dla VK wskazuje awans tego portalu – w skali globalnej – z 21. miejsca rankingu w sierpniu 2016 roku do 13. miejsca na świecie w styczniu 2017 roku. Obecnie VK zajmuje w rankingu Alexa 15 miejsce (patrz Rysunek 1).

Rysunek 1. Pozycja VK w rankingu „Alexa.com" – od marca 2016 r. do marca 2017 r. PrintScreen z 16 marca 2017 r.

Zgodnie z danymi „Alexa.com" 53% użytkowników VK jest z Rosji. Znaczna ich część pochodzi z innych państw b. Związku Radzieckiego. W pierwszej dziesiątce znalazło się jednak również 5 państw spoza ZSRR (patrz tabela 2). Z polskiej perspektywy kluczowe znaczenie ma to, że z naszego kraju wywodzi się około 2.2% spośród globalnej liczby użytkowników VK. Przy założeniu, że jest ich 95 milionów, oznaczałoby to w przybliżeniu 2 miliony użytkowników serwisu, którzy korzystają z VK z terytorium Polski.

Tabela 1. Dane z portalu „Alexa.com", pobrane 22 lutego 2017

Państwo	Procent użytkowników	Ranking w danym kraju
Rosja	53.0%	1
Ukraina	7.5%	2
Niemcy	4.4%	13
Kazachstan	3.8%	3
Białoruś	2.8%	1
Polska	2.2%	10
USA	2.2%	128

Holandia	1.8%	6
Azerbejdżan	1.7%	5
Chiny	1.5%	95

Similarweb, czyli inny znaczący serwis internetowy zajmujący się rankingowaniem stron internetowych, wskazał, że 15 marca 2017 r. VK był piątą najważniejszą stroną internetową na świecie (drugie miejsce wśród serwisów społecznościowych) i najważniejszą stroną internetową w Rosji. Zgodnie z rankingiem Similarweb dla Polski VK jest 15. najistotniejszą stroną w Polsce. Pośród mediów społecznościowych wyższe miejsca zajmują w Polsce tylko: Youtube, Facebook i Instagram (odpowiednio 2., 3. i 13. miejsce w rankingu). **Żadna polska rodzima sieć społecznościowa nie znalazła się w tych rankingach powyżej VK**.

Dane Alexa wskazują, że VK mógłby mieć nawet 2 miliony użytkowników łączących się z tym serwisem z Polski. Jednak w trakcie próby kupienia reklam skierowanych (tzw. reklam „targetowanych") tylko do osób znajdujących się na terenie naszego kraju system sprzedaży reklam VK twierdzi, że jest w stanie wskazać 543.000 takich osób[20], tak więc można przyjąć, że **maksymalnie około 500 tyś. osób korzysta na terytorium Polski z VK**. Można założyć, że większość ruchu użytkowników polskiego Internetu, który jest odpowiedzialny za wysokie miejsce VK w rankingach analizujących Polskę, łączy się ze znajdującą się na naszym terytorium znaczną ilością osób pochodzących z państw, w których istotną rolę odgrywa język rosyjski. Biorąc zatem pod uwagę obywateli Ukrainy i Białorusi logujących się z terenu Polski do VK, należy przyjąć, że **Polaków na tym serwisie jest nie więcej niż 200 tyś.**

Przyczyny wyboru VK przez Polaków:

1. VK ma opinię serwisu społecznościowego, który nie cenzuruje treści i w którym nie ma ograniczeń wynikających z poprawności politycznej[21]. Przykładowo zdjęcia oraz nagrania pornograficzne są łatwo dostępne, bezpośrednio pośród innych wyszukiwań filmów lub fotografii. Wystarczy zawęzić wyszukiwania do treści, które są przeznaczone tylko dla osób powyżej 18. roku życia.
2. W październiku 2016 roku Facebook zablokował konta polskich organizacji narodowych. Pojawiły się wśród ich przedstawicieli głosy – relacjonowane następnie przez media – że narodowcy przenoszą się na serwis, który nie zniszczy tworzonych przez nich nakładem czasu i innych zasobów społeczności internetowych. Takim serwisem miał być VK. Powracającym wątkiem związanym z zachętami do zbiorowego przejścia na ten serwis było określanie Facebooka jako „Pejsbook". Postawy antysemickie wydawały się znaczącym argumentem na rzecz zmiany serwisu.
3. Jednym z elementów zachęcania do zarejestrowania się na VK jest budowanie wrażenia symetrii pomiędzy działalnością tajnych służb prowadzoną na VK oraz na FB. Z analizy wypowiedzi osób deklarujących chęć zmiany serwisu społecznościowego z Facebooka na VK oraz wyjaśniających przewagę VK nad Facebookiem wynika, że użytkownicy podejmują świadomą decyzję, kto będzie obserwował ich działania. Pojawia się wypowiadane wprost założenie, że skoro VK i Facebook są infiltrowane przez służby, to lepiej dać się obserwować

Rosjanom i korzystać z tego, że polskie służby i wymiar sprawiedliwości nie będą w stanie pozyskać informacji lub pomocy prawnej od Federacji Rosyjskiej.

4. Zainteresowanie Polaków VK może być związane z zainteresowaniem rosyjską kulturą, chęcią prowadzenia działalności biznesowej lub posiadaniem znajomych i rodziny na obszarze działania rosyjskojęzycznego Internetu.

Rekomendacje

Należy przyjąć, że serwis VK:

1. Jest prawdopodobnie integralnym narzędziem prowadzenia wojny informacyjnej przez Federację Rosyjską, w tym operacji dezinformacyjnych skierowanych przeciw RP.
2. Dane użytkowników serwisu podlegają bezpośredniej penetracji i analizie przez służby Federacji Rosyjskiej FSB oraz GRU. Wrażliwe dane poszczególnych użytkowników i całych społeczności mogą podlegać analizie na zbliżonym poziomie jak w serwisie Facebook włącznie z wykorzystaniem algorytmów sterujących dostępem do informacji.

W tych dwóch kontekstach rekomendowane jest monitorowanie VK:

1. W połączeniu z infiltracją za pomocą specjalnie stworzonych tożsamości grup związanych z Polską i polskojęzycznych oraz tworzenie grup za pomocą stworzonych tożsamości.
2. W celu rozpoznania:
    a. Nowych funkcjonalności, w tym szczególnie tych, które odwołują się do analizy i eksploracji danych użytkowników.
    b. Aktualnej polityki prywatności.
    c. Prowadzonych programów badawczo-rozwojowych.
3. W celu rozpoznania aktywności w wojnie informacyjnej Federacji Rosyjskiej sugerowanie jest prowadzenie systematycznych działań polegających na identyfikowaniu trolli i stosowanych przez nich typów narracji.

Celowe byłoby monitorowanie mechanizmów dyfuzji informacji typu *fake news* z VK do polskich mediów. **[4/12]**

Krzemowa Dolina organizuje się politycznie przeciwko Trumpowi

KOMUNIKAT

17 marca 2017. Wpływowy amerykański portal Politico informuje[22], że kierownictwo i szeregowi pracownicy różnych przedsiębiorstw z sektora IT zlokalizowanych w Krzemowej Dolinie, podjęli działania na rzecz zorganizowania wspólnego frontu politycznego przeciwko prezydentowi Donaldowi Trumpowi. Robocza nazwa inicjatywy to „Win the Future".

W styczniu br. administracja prezydenta Trumpa poinformowała o wprowadzeniu ograniczeń dla migrantów z siedmiu krajów muzułmańskich (Iraku, Syrii, Iranu, Sudanu, Libii, Somalii i Jemenu). W geście protestu przeciwko tej decyzji prezes UBERa (globalnej korporacji oferującej usługi parataksówkarskie) Travis Kalanick zrezygnował z członkostwa w gronie doradców prezydenta USA ds. gospodarki[23]. Zainspirowało to pracowników z Krzemowej Doliny do podjęcia zorganizowanych, aktywnych form politycznej walki z prezydentem Trumpem. Przedsięwzięcie to można potraktować poważnie, ponieważ pracownicy i właściciele firm sektora IT z Krzemowej Doliny, którzy zorganizują się politycznie, mogą stać się wpływowym czynnikiem, istotnie oddziałującym na kształt amerykańskiej oraz międzynarodowej polityki. Menedżerów i specjalistów z tej branży określa się mianem „digital upper klas" (z ang. „cyfrowa klasa wyższa"), co wskazuje, że przedstawiciele sektora zaawansowanych technologii cyfrowych stają się pewną formą współczesnej arystokracji. Mają oni zasoby, finansowe i techniczne, do stania się istotną grupą interesu. Rosnący postęp technologiczny i upowszechnianie się właściwych mu narzędzi i praktyk będzie sprzyjał wzrostowi znaczenia tej grupy. Już w przeszłości środowisko to kojarzone było raczej ze światopoglądem liberalnym, przeciwnym Partii Republikańskiej. Jednakże teraz dostrzec można wyraźne próby konsolidacji i koordynacji tej dotychczas, jak się wydaje, rozproszonej grupy. Cechą branży IT w USA jest to, że jest to sektor bardzo indywidualistyczny. W Stanach swoje związki zawodowe – bardzo silne – ma większość branż (np. kierowcy ciężarówek, scenarzyści hollywoodzcy), a w sektorze IT takiego uzwiązkowienia do tej pory nie było. Istotne znaczenie ma także dość liczna obecność wśród pracowników z Doliny Krzemowej emigrantów z różnych krajów Azji, także tych o przewadze ludności wyznania muzułmańskiego. Co więcej, istotnym elementem tożsamości „cyfrowej elity" z Doliny Krzemowej jest także kosmopolityzm.

Rekomendacje:

1. Obserwowanie rozwoju inicjatywy Win the Future zwłaszcza pod kątem potencjału mobilizacji elektoratu dotychczas mniej aktywnego politycznie.

2. Obserwowanie prób budowania przez tę inicjatywę sieci kontaktów międzynarodowych i inspirowania powstawania podobnych grup w innych krajach, w tym w Polsce. **[3/8]**

Chiński system zautomatyzowanej oceny obywateli: perspektywa cyfrowego totalitaryzmu

ANALIZA

3 marca 2017. Rząd Chin planuje wdrożenie od 2020 r. narodowego systemu reputacji, tj. procedur indywidualnej, cyfrowej, zautomatyzowanej oceny obywateli. System ma promować zachowania uznane za „prospołeczne" i sankcjonować niepożądane. Obecnie w fazie pilotażu znajduje się 8 konkurencyjnych rozwiązań testowanych na różnych grupach odbiorców: od mieszkańców poszczególnych miast (w tym Szanghaju) po grupy użytkowników serwisów internetowych[24]. Docelowo, system ma integrować dane nt. obywatela z baz administracji publicznej, wymiaru sprawiedliwości, mediów społecznościowych oraz aktywności konsumenckiej, w postaci jednolitego wyniku podawanego w punktach. Prezentowane głównie przez dziennikarzy zachodnich ustalenia na temat praktycznych aspektów działania testowanych rozwiązań wskazują na ryzyko ukształtowania się nowego typu systemu inwigilacji obywateli. Gdyby okazał się on skuteczny, mógłby w znaczący sposób zwiększyć możliwości państw autorytarnych (obok Chin także np. Rosji) do zacieśnienia kontroli nad własną populacją (a w dalszej perspektywie wywierania wpływu na ludność państw trzecich, np. Polski).

Oficjalne założenia systemu zostały przedstawione w dostępnym publicznie dokumencie rządowym z 2014 r. Dokument ten przywołuje decyzję podjętą podczas 3. Plenum 18. Kongresu Komunistycznej Partii Chin (w roku 2013), aby „ustanowić i zrealizować system kredytu społecznego, nagradzać uczciwość i karać nieuczciwość"[25]. W dokumencie z 2014 r. pomysł wprowadzenia ww. systemu uzasadnia się znaczną skalą nieprawidłowości w różnych dziedzinach życia społecznego (np. unikania podatków, nadużyć w sferze prawa pracy, oszustw finansowych, nieuczciwości naukowej itp.). Jako główny cel wskazuje się „wspieranie rządu" w kilkunastu obszarach, w tym: produkcji (promocja standardów bhp), finansów, podatków, ustalania cen, przetargów, ruchu drogowego (wszelkie naruszenia mają obniżać rating obywatela), handlu elektronicznego, reklamy, opieki zdrowotnej (ocena lekarzy) i kontroli urodzeń (tu mechanizmu nie dookreślono), ekologii, praw autorskich, a także – w szeroko rozumianej sferze aktywności społeczno-ekonomicznej jednostek (tu: ocena pracy przedstawicieli zawodów zaufania publicznego, personelu medycznego, nauczycieli, badaczy, pracowników mediów, przewodników turystycznych, weterynarzy). Jako osobny obszar wskazano „aplikacje i usługi internetowe"; tu przedmiotem oceny ma być „zachowanie obywateli-internautów online, ze wskazaniem ich kredytu". Elementem rankingu obywateli miałyby być też dane z wymiaru sprawiedliwości nt. ewentualnych kłopotów z prawem. Dokument zawiera także wskazówki nt. strategii masowego upowszechnienia wiedzy o nowym systemie, wykorzystania nauki i naukowców do zarządzania systemem, perspektywę analogicznych do centralnego systemów lokalnych (na skalę miasta lub wsi). Podsumowując, zarysowana w dokumencie wizja ma doprowadzić do sytuacji, w której osoby uznane za wiarygodne są nagradzane pod każdym względem, zaś niegodne zaufania spotykają się z trudnościami na każdym kroku.

Publikacja dokumentu spotkała się ze znacznym oddźwiękiem na Zachodzie[26]. Najwięcej zainteresowania mediów zachodnich wzbudził system Credit Sesame wdrażany przez spółkę Ant Financial Services powiązaną z gigantem e-handlu – grupą Alibaba[27]. Korzysta on z danych nt. 300 mln (wg innych źródeł: 400 mln) kupujących za pośrednictwem serwisów Alibaby, a także historii płatności za pośrednictwem Alipay, która jest największą platformą płatności online w Chinach. Według pierwszych doniesień, dane te miały być wykorzystywane w pierwszym rzędzie do określenia zdolności kredytowej danej osoby[28].

Choć szczegóły algorytmu punktacji nie są znane publicznie, internauci testujący system (w tym dziennikarze), metodą prób i błędów odkrywają mechanizm jego działania (co jest nagradzane wyższym wynikiem, a co jest karane), a także – sankcje i przywileje wiążące się z niskim lub wysokim wynikiem w rankingu. Przykładowe nagrody dla osób z wyższym wynikiem to: preferencyjne traktowanie klientów w największym serwisie matrymonialnym, możliwość wypożyczania samochodu bez depozytu, możliwość darmowego wypożyczania różnych przedmiotów (niezbędny wynik powyżej 600 pkt)[29], szybszy check-out w niektórych hotelach (pow. 650 pkt), uproszczenie formalności wizowych do Singapuru (pow. 700 pkt.)[30]. Przykładowe sankcje pozostają na razie głównie w sferze spekulacji. Niektórzy wskazują na obniżanie punktacji za zakup gier wideo lub na potencjalne (po 2020 roku) sankcje takie jak wolniejszy dostęp do Internetu czy zamknięcie drogi do niektórych zawodów[31]. Choć komentatorzy przestrzegają przed demonizacją systemu (jako objawem niezrozumienia Chin na Zachodzie)[32], warto podkreślić, że przywileje dla osób z wyższą punktacją z perspektywy osób o niższym rankingu są *de facto* sankcjami.

Wnioski:

1. Obecnie efektywne stosowanie zautomatyzowanego systemu oceny obywateli jest trudne m.in. z uwagi na wysokie koszty wdrożenia i obsługi; należy się spodziewać, że koszty te drastycznie spadną wraz z szybkim rozwojem sztucznej inteligencji; tym samym, systemy te staną się dla różnych rządów (i innych podmiotów, np. wielkich korporacji) bardziej atrakcyjne.
2. Wdrożenie skutecznego, całościowego systemu może dawać władzy (zwłaszcza już autorytarnej) bezprecedensowe zdolności w zakresie neutralizacji oporu obywateli, atomizacji społeczeństwa, izolacji dysydentów itp.

Prognoza: czego się spodziewać?

1. Należy oczekiwać, że analogicznie do krajowych systemów oceny pojawią się systemy indywidualnego profilowania i nadzoru obywateli danego państwa przez państwa obce; w kontekście Polski szczególnie niebezpieczne mogłoby być opracowanie takiego systemu przez Rosję, do wykorzystania zwłaszcza w wariancie jakiejś formy „okupacji" naszego kraju.
2. Pojawi się ryzyko „zhakowania" punktacji obywatela poprzez niezależne od zasadniczego algorytmu zaniżenie jego indywidualnej oceny, np. ze względu na krytykę władzy; można się także spodziewać powstania czarnego rynku obrotu punktami oraz nowych form przestępczości.

3. W razie przyjęcia jakiejś wersji analogicznego systemu w krajach zachodnich (w tym w Polsce) należy oczekiwać kontrowersji związanych z potencjałem inwigilacji, a także intensywnych sporów politycznych wokół kryteriów (algorytmu) punktacji.

Rekomendacje:

1. Podjąć własne, pogłębione analizy aktualnej postaci i prawdopodobnej ewolucji systemu oceny obywateli w Chinach na materiałach w języku chińskim; fakt, iż opracowanie niniejsze oparto wyłącznie na źródłach dostępnych w języku angielskim może skutkować zniekształceniem obrazu sytuacji.
2. Uważnie monitorować pojawianie się i funkcjonowanie analogicznych systemów w krajach zachodnich oraz w Rosji (słowa kluczowe: *citizen score, social credit system*).
3. Rozważyć podjęcie prac (na tym etapie: koncepcyjnych) nad stworzeniem własnej wersji systemu kredytu społecznego, z uwzględnieniem wartości powszechnie cenionych w polskim społeczeństwie, a także – interesów państwa polskiego. System taki mógłby uwzględniać koncepcję „gamifikacji" (zakłada ona, że ludzie są bardziej skłonni podejmować pewne działania, jeśli nada im się atrakcyjną formę gry), promując zachowania społecznie pożądane, a zniechęcając do zachowań destruktywnych;
4. Przeanalizować strukturę własności funkcjonujących w Polsce platform (w tym zwłaszcza platform handlu elektronicznego), które mogą stanowić punkt wyjścia do tworzenia opisywanych tu systemów oceny obywateli. Zagraniczna kontrola nad tego podmiotami (jak w przypadku Allegro) umożliwia podmiotom zewnętrznym podjęcie próby stworzenia takiego systemu dla ludności Polski (w celach sprzecznych z racją stanu) oraz utrudnia ewentualny projekt budowy systemu własnego. **[3/12]**

Przydatność metod opartych na zjawisku „mądrości tłumu" do rozpoznawania zjawisk z obszaru bezpieczeństwa narodowego

ANALIZA

Jednym z ważnych narzędzi służących rozwiązywaniu problemów i przewidywaniu wydarzeń są tzw. rynki predykcyjne. Bazują one na efekcie określanym jako „mądrość tłumu", który polega na tym, że odpowiednio dobrana liczna grupa ludzi może dokonywać przewidywań lub rozwiązywać słabo zdefiniowane problemy skuteczniej niż osoby uznawane za ekspertów w danej dziedzinie. Lepsze wyniki uzyskiwane w takich grupach nie są konsekwencją sumy kompetencji jej członków: grupa zazwyczaj jest „mądrzejsza" od najmądrzejszych członków.

Warunki, jakie musi spełnić grupa, by wyzwolony został efekt mądrości tłumu, są następujące: (1) duże zróżnicowanie grupy, (2) brak interakcji między członkami (jeżeli indywidualne rozwiązania będą uzgadniane, grupa uzyska wynik daleki od optymalnego), (3) brak informacyjnego atraktora, czyli nie może istnieć jedna, ogólnie dostępna informacja, którą będą sugerowali się członkowie grupy (np. jeżeli ich zadaniem będzie przewidzenie wyników wyborów politycznych, a dostępne będą przewidywania sondażowe, to grupa uzyska gorsze przewidywania), (4) musi istnieć system integracji indywidualnych rozwiązań (czasami może być to zwykle sumowanie i wyciąganie średniej arytmetycznej, często stosuje się jednak dużo bardziej złożone algorytmy), (5) wysoki poziom motywacji, by udzielać najtrafniejszych rozwiązań i przewidywań (osiąga się to uzależniając wysokość nagród od trafności).

Najlepszym znanym zastosowaniem koncepcji mądrości tłumu są rynki predykcyjne (rynki przyszłości). Pierwsze rynki predykcyjne otwarto w 1988 r. przy Uniwersytecie Iowa. Otwarcia dokonano przy okazji wyborów prezydenckich w USA: przewidywania rynku przebiły wyniki sondażu wyborczego Gallupa. W 1996 roku uruchomiono *The Hollywood Stock Exchange*, rynek poświęcony przewidywaniu kwestii powiązanych ze światem filmowym: jakie zyski uzyska dana produkcja, kto zdobędzie Oscara etc. Ponownie rynki predykcyjne okazały się skuteczniejsze w przewidywaniu, niż inne podejścia. W kolejnych latach powstawały rynki predykcyjne poświęcone przewidywaniu wydarzeń ekonomicznych, powodzenia projektów technologicznych, problemom medycznym, epidemiom oraz rozmaitym katastrofom etc. Duże korporacje, miedzy innymi Google i Ford, inwestują w tworzenie własnych rynków predykcyjnych, angażując do gry własnych pracowników.

Instytucje publiczne również korzystały z tego rozwiązania. Otworzenie rynków terrorystycznych planował Departament Obrony Stanów Zjednoczonych. Chodziło o wykorzystanie mądrości zbiorowej do przewidywania zamachów. Niefortunna nazwa oraz niekorzystna recepcja publiczna (rynek postrzegano jako grę hazardową, w której obstawiało się śmierć obywateli) sprawiły, że Pentagon wycofał się z tego przedsięwzięcia. Nie była to jednak jedyna, ani ostatnia próba zastosowania tego podejścia w dziedzinie bezpieczeństwa narodowego.

Zanim omówimy jedno z takich zastosowań, trzeba bliżej objaśnić, jak zbudowany jest rynek predykcyjny. Uczestnicy rynku (od kilkudziesięciu do kilku tysięcy graczy) dokonują zakładów: obstawiają warianty przyszłości, kupując odpowiednie udziały.

W przypadku większości rynków gracze stoją wobec tzw. binarnych wyborów (zjawisko x zajdzie lub nie zajdzie w określonym czasie). Zagregowane wyniki zakładów prezentowane są w postaci pojedynczego parametru: prawdopodobieństwa wydarzenia w skali od 0 do 100%. Zazwyczaj gracze mogą skupować większą ilość udziałów. Decydując się na mniejszy lub większy wolumen „udziałów w przyszłości" gracze wyrażają swoje przekonania co do tego, jaka będzie przyszłość, ale także jak bardzo pewni są swego osądu: im więcej udziałów skłonny jest zakupić gracz, tym pewniejszy jest swojego przewidywania. Jest to bardzo ważne, gdyż umiejętność oceny własnej pewności, jest równie istotna w dziedzinie podejmowania decyzji, co sama treść predykcji. Wielu ludzi przeszacowuje swoją pewność, ryzykownie inwestuje i traci pieniądze. W efekcie „pechowy" i zbyt pewny siebie gracz bankrutuje i wypada z rynku (mechanizm selekcji) albo lepiej kalibruje swoją wiedzę (mechanizm uczenia się). Rynki predykcyjne, w których uczestniczy wciąż podobna pula osób, z czasem osiągają coraz lepsze wyniki w przewidywaniu. Bardzo interesujące jest to, że nie ma większej różnicy, czy na rynku gra się prawdziwymi pieniędzmi, czy wirtualną walutą, której nie można wypłacić z systemu. W obu przypadkach gracze są silnie zmotywowani do formułowania jak najtrafniejszych predykcji.

Wśród badaczy panuje zgoda, że rynki predykcyjne dostarczają przewidywań i szacunków co najmniej tak samo dobrych jak inne metody, na przykład sondaż przedwyborczy, które bazowałyby na podobnej próbie ludzi. Rynki predykcyjne są wolne również od ograniczeń takich metod jak panele eksperckie, w których często dochodzi do wytworzenia się syndromu myślenia grupowego. Badacze przyznają jednak, że rynki te mają wiele słabości. Mają one m.in. te same ograniczenia, co zwykłe rynki (np. mogą zawieść w wyniku niskiej płynności). Konieczne jest również zachowanie wspomnianych wyżej podstawowych warunków mądrości tłumu.

Świetnym przykładem implementacji mądrości tłumu w obszarze bezpieczeństwa narodowego jest *Good Judgment Project* (GJP). Działa on od lipca 2011 r. Twórcami GJP są Philip E. Tetlock, Barbara Mellers i Don Moore, a sam projekt realizowany jest przez amerykańską agencję *Intelligence Advanced Research Projects Activity* (IARPA): wzorowaną na DARPA organizację, która stawia sobie jako jeden z głównych celów rozwój innowacyjnych technologii wywiadowczych. GJP jest próbą wykorzystania mechanizmu rynków predykcyjnych do przewidywania wydarzeń politycznych na świecie, które są w zakresie zainteresowania wywiadu amerykańskiego. Należy podkreślić jednak, że nie jest to rynek predykcyjny w ścisłym znaczeniu: posiada on wiele elementów rynku predykcyjnego, ale został uzupełniony o kilka dodatkowych rozwiązań, które znacząco podniosły jego skuteczność. GJP to w istocie powrót do idei rynków terrorystycznych.

GJP zwyciężał w konkursach na przewidywania organizowanym przez IARPA na przestrzeni lat 2011-2013. Konkurs miał wyłonić najlepszy program przewidywania przyszłych, niepewnych wydarzeń w oparciu o kompetencje grupy. W konkursie rywalizowało pięć programów. W ramach każdego z nich można było stosować dowolne metody doboru uczestników i treningu, stosować własne metody agregacji, wprowadzać specjalne systemy nagród etc. Uczestnikom programów przedstawiono 200 pytań z dziedziny polityki zagranicznej, światowej gospodarki etc. Algorytm GJP pozwolił przewidzieć wydarzenia w 86,2% przypadków, zyskując o 60% lepszy wynik, niż grupa kontrolna, działająca w trybie standardowej mądrości tłumu, w której

szacunki agregowano w oparciu o zwykłą średnią arytmetyczną i o 40% lepszy, niż pozostałe programy biorące udział w konkursie organizowanym przez IARPA.

Uzyskanie takich efektów było możliwe dzięki czterem innowacjom: (1) rekrutacja i zatrzymywanie lepszych członków panelu, (2) specjalny trening poznawczy ograniczający stronniczość, (3) społeczne zaangażowanie uczestników panelu na zasadzie organizowania ich pracy w trybie zespołów roboczych i rynku predykcyjnego, (4) lepsze metody wydobywania mądrości z tłumu. Szacuje się, że ostatni punkt zaważył na różnicy miedzy GJP a grupą kontrolną bardziej niż trzy pozostałe innowacje razem wzięte. W GJP silny nacisk został położony na tzw. superprognostów: 1% osób, które samodzielnie uzyskiwały niezwykle wysoką trafność przewidywań, niekiedy uzyskując wyniki o 30% lepsze niż wyniki zawodowych analityków amerykańskiego wywiadu.

GJP można traktować jako ukoronowanie bogatej tradycji badań nad mądrością tłumu i wiedzą ekspercką. GJP ucieleśnia w sobie najlepsze rozwiązania odkryte i doskonalone na przestrzeni lat. GJP pokazuje, że w dziedzinie badań nad mądrością tłumu zgromadzono ogromną ilość wiedzy o charakterze inżynieryjnym w ścisłym tego słowa znaczeniu.

Wnioski:

Rynki predykcyjne nie mogą zastąpić wiedzy eksperckiej, ani systemów ekspertowych, ale w tych obszarach, gdzie mamy do czynienia z problemami słabo zdefiniowanymi (czyli wszędzie tam, gdzie trzeba bazować na wnioskowaniach zawodnych), uzyskują one lepsze rezultaty, niż dowolni pojedynczy specjaliści z danego obszaru.

Rekomendacje:

Należy przetestować podobny rodzimy system na potrzeby przewidywania wydarzeń związanych ze zjawiskami zewnętrznymi i wewnętrznymi istotnymi z perspektywy interesu RP i bezpieczeństwa narodowego. Problemy, w których rozwiązaniu mogłoby okazać się pomocne to podejście, obejmują:

- określanie prawdopodobieństwa wybuchu konfliktów zbrojnych,
- przewidywanie zmian na rynkach paliw,
- przewidywanie sytuacji na rynkach finansowych,
- selekcja i przewidywanie rozwoju technologii, które mogą w istotny sposób wpłynąć na procesy rynkowe lub społeczne,
- przewidywanie wyników wyborów politycznych w innych krajach oraz ewentualnej zmiany władzy.

Rozwiązanie bazujące na idei rynków predykcyjnych może stanowić relatywnie tanie uzupełnienie obecnego potencjału analitycznego wykorzystywanego w celu zapewnienia bezpieczeństwa RP.

Podejście takie może posłużyć do wyłaniania z tłumu specjalistów o wyjątkowych zdolnościach, których identyfikacja nie była możliwa w ramach dotychczasowego modelu rekrutacji i szkolenia analityków. **[10/8]**

Źródła informacji wykorzystane w opracowaniu:

The Journal of Prediction Markets http://ubplj.org/index.php/jpm/index

http://www.goodjudgment.com/

http://tippie.biz.uiowa.edu/iem/

R. Erikson, C. Wlezien. Markets vs. polls as election predictors: An historical assessment. „Electoral Studies" 2012, Vol. 31, ss. 532-539.

L. Hong, S. Page. Groups of diverse problem solvers can outperform groups of high-ability problem solvers. „PNAS" 2004, Vol. 101 No. 46, ss. 16385-16389.

P. Tetlock. Expert Political Judgment. How Good Is It? How Can We Know? 2005, Princeton: Princeton University Press.

P. Tetlock, B. Mellers, N. Rohrbaugh, E. Chen. Forecasting Tournaments: Tools for Increasing Transparency and Improving the Quality of Debate. „Current Directions in Psychological Science" 2014, Vol. 23, No. 4, ss. 290- 295.

Europejskie ośrodki walki z dezinformacją: przegląd

ANALIZA

13 marca 2017. Narastająca od 2013 roku wojna informacyjna Rosji przeciwko Ukrainie, kampania poprzedzająca referendum w sprawie Brexitu oraz wybory prezydenckie w USA w roku 2016 przyczyniły się do wzrostu – wśród krajów UE – świadomości znaczenia bezpieczeństwa informacyjnego oraz skali zagrożeń hybrydowych, zwłaszcza ze strony Rosji. W reakcji na te wydarzenia, na przestrzeni ostatnich dwóch lat kilka krajów powołało finansowane ze środków publicznych centra walki z dezinformacją. Część z nich deklaruje wyłącznie cele defensywne (sprawdzanie i prostowanie informacji), inne – także ofensywne (aktywna polityka komunikacyjna). Powstało także kilka ośrodków ponadnarodowych i wiele ośrodków pozarządowych, stawiających sobie za cel systematyczną weryfikację informacji. Niniejsza analiza zawiera wstępny wykaz takich ośrodków, a także krótkie omówienie ich działalności.

Ośrodki ponadnarodowe

1. **East StratCom** – ośrodek unijny, utworzony podczas posiedzenia Rady Europejskiej (organu UE) w dn. 19-20 marca 2015 r., z siedzibą w Brukseli. Ośrodek deklaruje następujące cele ogólne:
   - prowadzenie proaktywnych kampanii komunikacji strategicznej, wyjaśniających kluczowe obszary polityki unijnej i tworzących pozytywną narrację nt. UE;
   - doraźną komunikację na aktualne tematy i zagadnienia istotne dla polityki UE;
   - analizę trendów dezinformacji, wyjaśnianie dezinformacji i obalanie mitów[33].

   Według deklaracji, zespół ogranicza się do działań defensywnych, tj. do prostowania przekłamań. Co istotne, ważnym obszarem działania organizacji są kraje tzw. Wschodniego Partnerstwa UE, w szczególności: Armenia, Azerbejdżan, Białoruś, Gruzja, Mołdawia i Ukraina. W obszarze tym, zakłada się poprawę komunikacji strategicznej UE oraz dostarczanie materiałów, które będą wykorzystywane przez media rosyjskojęzyczne[34]. Zespół ośrodka liczy obecnie kilkanaście osób (według jednego ze źródeł, cały personel tworzy 11 osób[35]), w tym 2 osoby specjalizują się w tematyce *fake news*[36]. Z informacji na stronie internetowej zespołu wynika, że obecnie wspiera go sieć 400 ekspertów, urzędników, dziennikarzy, przedstawicieli organizacji pozarządowych i think tanków z ponad 30 krajów. Ośrodek publikuje krótki przegląd wybranych przykładów rosyjskiej dezinformacji w postaci „Disinformation Digest" oraz cotygodniowy (publikowany w czwartki) biuletyn Disinformation Review (również ograniczający się do przeglądu rosyjskich mediów społecznościowych)[37].
2. **NATO Strategic Communications Centre of Excellence** (NATO STRATCOM) z siedzibą w Rydze (Łotwa) to jedno z 24 tzw. Centrów Doskonałości NATO. Instytucja ma status organizacji międzynarodowej; powstała 1 lipca 2014 roku w wyniku podpisania porozumienia przez Łotwę, Estonię, Niemcy, Włochy, Litwę,

Polskę i Wielką Brytanię[38]. Koncentruje się na komunikacji strategicznej. Plan głównych działań na rok 2017 obejmuje m.in.:

- Badanie ruchów ekstremistycznych jako nowego zagrożenia dla państw NATO.
- Badanie, jak NATO i jego członkowie mogą przeciwdziałać wrogim wpływom.
- Badanie rosyjskiej kampanii informacyjnej w krajach nordyckich i bałtyckich.
- Badanie rosyjskich interpretacji wydarzeń z okresu II wojny światowej.
- Analizę nowych wyzwań w środowisku informacyjnym w kontekście trollingu maszynowego[39].

Ośrodki narodowe

3. W styczniu 2017 roku rozpoczęło pracę **Centr proti terorismu a hybridním hrozbám** (Centrum Walki z Terroryzmem i Zagrożeniami Hybrydowymi) w Czechach (z siedzibą w Pradze). Ma ono początkowo zatrudniać 20 osób, zaś ich głównym celem ma być zwalczanie kampanii dezinformacyjnych, zwłaszcza w kontekście wyborów do niższej izby parlamentu jesienią 2017 roku oraz wyborów prezydenckich w roku 2018[40].

4. W roku 2015 w strukturze **armii brytyjskiej** powołano **nową brygadę (77th),** której celem ma być „podejmowanie wyzwań nowoczesnej wojny poprzez działania nie-śmiercionośne [*non-lethal*] i wykorzystanie prawomocnych środków pozamilitarnych modyfikowania zachowań sił przeciwników”[41]. Jednostka powstała z połączenia kilku innych, mniejszych jednostek; rekrutuje także rezerwistów – osoby dobrze obeznane z mediami społecznościowymi i posiadające umiejętności dziennikarskie[42]. Wśród obszarów działania, jakie wymieniono na stronie brygady, można znaleźć m.in. „analizę kręgów odbiorców i przeciwników” oraz działania medialne. Na tej ostatniej kwestii skoncentrowały się doniesienia medialne, w których pojawiły się informacje, iż ważnym obszarem działania żołnierzy będą m.in. media społecznościowe (stąd funkcjonujące w mediach określenie nowej jednostki jako „Facebook warriors”[43]).

Ośrodki, które planuje się utworzyć:

1. **Abwehrzentrum gegen Desinformation** (nazwa wstępna, po polsku: Centrum Obrony przed Dezinformacją) – koncepcja powołania została zgłoszona przez niemieckie MSW w grudniu 2016 roku[44]. Według doniesień, mogłoby ono powstać pod auspicjami biura prasowego Urzędu Kanclerskiego. Warto podkreślić, że niemieckie MSW dostrzega potrzebę powstania nowego centrum walki z dezinformacją, mimo iż biuro prasowe Urzędu już obecnie zatrudnia 500 osób, a niedawno utworzono instytucję o zbliżonych zadaniach – w 2011 MSW utworzyło Narodowe Centrum Cyberobrony (Nationale Cyber-Abwehrzentrum, w skrócie: NCAZ lub Cyber-AZ)[45]. W uzasadnieniu potrzeby powołania centrum wskazuje się na nowe zagrożenia ze strony Rosji w kontekście wyborów parlamentarnych w roku 2017[46]. Wskazuje się, że grupami szczególnie narażonymi na oddziaływanie *fake news* są Niemcy pochodzenia rosyjskiego oraz tureckiego. Niemieckie MSW promuje także międzypartyjne porozumienie w sprawie rezygnacji z wykorzystania w kampanii *fake news* oraz „botów społecznych” (programy imitujące aktywność ludzi w portalach społecznościowych).

2. Na rok 2018 zapowiedziano utworzenie kolejnego z natowskich „centrów doskonałości" – **European Center of Excellence for Countering Hybrid Threats w Helsinkach**. Utworzenie centrum mają popierać: USA, Wielka Brytania, Niemcy, Francja, Włochy, Hiszpania, Polska, Szwecja i kraje bałtyckie[47].

Ośrodki pozarządowe

1. **StopFake Ukraine** (www.Stopfake.org) – inicjatywa Wydziału Dziennikarstwa Uniwersytetu Narodowego „Akademia Kijowsko-Mohylańska", który sprawuje nadzór merytoryczny nad programem i zapewnia studio telewizyjne. Program zapoczątkowano w roku 2014; obecnie zatrudnia 26 osób, zaś grono współpracowników z kraju i zagranicy jest znacznie szersze. Ze strony internetowej projektu wynika, iż weryfikowane, redagowane i propagowane są informacje w 10 językach: rosyjskim, angielskim, hiszpańskim, rumuńskim, bułgarskim, francuskim, włoskim, holenderskim, czeskim i niemieckim[48]. W ramach programu przygotowywany jest program telewizyjny dostępny w ok. 30 ukraińskich stacjach telewizyjnych[49]. Organizacja deklaruje programową niezależność od władz ukraińskich, wśród źródeł finansowania wymienia m.in. czeskie MSZ, ambasadę brytyjską w Kijowie, Renaissance Foundation, oraz Sigrid Rausing Trust.
2. Program „**Kremlin Watch**" prowadzony jest przez czeski think tank Evropské hodnoty (ang. European Values; szef: Jakub Janda[50]) powstały w roku 2005. Ośrodek publikuje cotygodniowy biuletyn „Kremlin Watch Monitor"; na stronie internetowej dostępnych jest też 17 bardziej obszernych analiz (część tylko w j. czeskim, część w j. angielskim), poświęconych m.in. analizie konkretnych przypadków dezinformacji, a także kwestiom metodologicznym[51]. Ze strony internetowej organizacji wynika, iż jej zespół liczy 7 osób.
3. Czeska organizacja pozarządowa **East European Information Centre** (zarejestrowana w sierpniu 2015 roku właśnie pod tą anglojęzyczną nazwą) stawia sobie za cel „walkę z propagandą Kremla przeciwko społeczeństwom zachodnim"[52]; organizacja utrzymuje jedynie profil na Facebooku[53].

Wnioski:

1. W okresie ostatnich dwóch lat w krajach UE/NATO powstały co najmniej dwie ponadnarodowe i co najmniej dwa narodowe ośrodki walki z dezinformacją; w najbliższym czasie planowane jest utworzenie co najmniej jednego ośrodka ponadnarodowego oraz jednego – narodowego; oprócz tego, powstaje wiele inicjatyw pozarządowych, które mają na celu przeciwstawienie się zalewowi *fake news* – zwłaszcza w kontekście wyborów parlamentarnych i prezydenckich.
2. Istniejące ośrodki walki z dezinformacją działają według różnych modeli: zasadna byłaby pogłębiona analiza porównawcza ich metodologii oraz skuteczności, pod kątem ewentualnego powołania analogicznego ośrodka w Polsce.
3. Mimo rosnącej świadomości problemu dezinformacji, zasoby inwestowane przez kraje UE/NATO do walki z dezinformacją są znikome w porównaniu z projektami rosyjskimi[54].
4. W Polsce jak dotąd nie istnieje żaden ośrodek systematycznej walki z dezinformacją. Zadania te są wykonywane przez podmioty prywatne, często

jednak sprofilowane na kwestie wewnętrzne (np. uczciwość polityków – jak serwis Demagog.pl), lub przez „hobbystów" (aktywnych głównie w mediach społecznościowych).

5. Planując powołanie takiego ośrodka, trzeba wziąć m.in. pod uwagę fakt, iż część osób współpracujących z takimi ośrodkami deklaruje, iż z tego tytułu spotykały ich rozmaite nieprzyjemności, a nawet były adresatami gróźb śmierci. Być może rozwiązaniem tego problemu byłoby powołanie odpowiedniej struktury przy polskim wojsku na wzór brytyjski.

Prognoza: czego się spodziewać?

1. Prawdopodobne jest nasilenie rosyjskich kampanii dezinformacyjnych w kontekście tegorocznych wyborów prezydenckich we Francji i parlamentarnych w Niemczech. W tym drugim kraju narasta przekonanie, że Rosja już zebrała materiały użyteczne w kampanii dezinformacyjnej, które zapewne zostaną wykorzystane późną wiosną lub w sezonie wakacyjnym, być może za pośrednictwem portalu Wikileaks[55].
2. Prawdopodobne jest, że w najbliższym czasie w kolejnych krajach powstaną – zarówno na poziomie ponadnarodowym, jak i krajowym – kolejne ośrodki walki z dezinformacją.

Rekomendacje:

5. Wskazane jest monitorowanie działalności ośrodków walki z (głównie rosyjską) dezinformacją i wspieranie prac (na tym etapie: koncepcyjnych) nad stworzeniem krajowego ośrodka tego typu.
6. Warto pamiętać o odpowiednim zabezpieczeniu personelu ośrodka na wypadek decyzji o jego utworzeniu; zasadne może być jego umiejscowienie w strukturach armii lub resortu obrony.
7. Należy zachęcić partie polityczne do stałego usprawniania swoich systemów zabezpieczeń w sieci, gdyż w szeregu państw zachodnich padały one ostatnio ofiarą poważnych ataków hakerów pracujących dla Rosji.
8. Dotychczasowe inicjatywy zdają się koncentrować na zwalczaniu fałszywych informacji. Warto rozważyć doświadczenia Finlandii w tym zakresie. Prowadzą one do wniosku, że wykazywanie kłamstwa jest odpowiedzią nieadekwatną do skali zagrożenia, zaś kluczowe znaczenie ma zdolność do tworzenia i propagowania własnej narracji[56]. **[5/8]**

System Windows 10 ma samoodblokowujący się keylogger.

KOMUNIKAT

25 marca 2017. Od kilku dni użytkownicy systemu operacyjnego Windows 10 informują[57], że w ich komputerach system ten poza kontrolą użytkownika przywraca funkcję rejestrowania sekwencji klawiszy naciskanych przez użytkownika i wysyłania danych na ten temat na serwery producenta oprogramowania. Stanowi to zagrożenie dla prywatności i bezpieczeństwa danych użytkownika. Zapisywanie i przekazywanie informacji o naciskanych klawiszach to tzw. keylogger. Jest to standardowa technika wykradania haseł dostępu i innych cennych informacji (np. danych osobowych). System Windows 10 w ustawieniach domyślnych posiada wbudowany taki keylogger. Program uzasadnia jego istnienie troską o optymalizowanie i doskonalenie procesu rozpoznawania wprowadzanego tekstu. Funkcję tę użytkownik pozornie może wyłączyć. W ostatnich dniach użytkownicy z różnych stron świata potwierdzili, że system Windows 10 samodzielnie odblokowuje funkcję keyloggera. Już wcześniej ostrzegano (np. polski GIODO i UOKiK[58], francuski CNIL[59]), że system Windows 10 szpieguje użytkowników[60]. Nowością jest informacja, że poza monitorowaniem aktywności użytkownika online czy przeglądania zawartości pamięci komputera, ten system operacyjny poza wiedzą i zgodą użytkownika zbiera także treści wprowadzane za pomocą klawiatury.

Rekomendacje:

1. Należy przeprowadzić audyt w instytucjach państwa w celu sprawdzenia skali wykorzystywania w nich systemu Windows 10.

2. Należy rozważyć powszechną wymianę w instytucjach państwowych systemu operacyjnego z Windowsa 10 na którąś z dystrybucji systemu Linux, np. Ubuntu, która posiada podobne funkcjonalności jak Windows. **[3/5]**

Francuski wywiad ostrzega przed intensyfikacją działań rosyjskich służb w cyberprzestrzeni w okresie przedwyborczym

KOMUNIKAT

17 marca 2017. Dyrekcja Generalna Bezpieczeństwa Zewnętrznego (DGSE), francuska służba wywiadowcza, poinformowała, iż intensyfikowane są działania rosyjskich służb specjalnych w sferze cybernetycznej w związku z kampanią prezydencką we Francji. W kontekście omawianego zagrożenia, które jest przedmiotem szerokiej debaty publicznej we Francji, urządzenia elektroniczne nie będą wykorzystywane w procesie głosowania w nadchodzących wyborach. W sposób znaczący ogranicza to możliwości rosyjskich służb specjalnych, które skoncentrowane są na atakowaniu stron internetowych kandydatów, nie zaś samej infrastruktury wykorzystywanej w organizacji wyborów oraz przeprowadzaniu operacji wpływu politycznego tradycyjnymi środkami. Przykładem mogą być niedawne ataki na serwery internetowe E. Macrona, potencjalnego przeciwnika M. Le Pen w drugiej turze. Istotnym jest fakt, iż DGSE jako służba zewnętrzna skupiona głównie na zwalczaniu terroryzmu, teraz w sposób bezprecedensowy włącza się w ochronę procesów wyborczych, m.in. instruując sztaby kandydatów w zakresie cyberbezpieczeństwa.

Ocenia się, że rosyjskie służby specjalne (w szczególności FSB oraz GRU) rozwijają znaczne zdolności cybernetyczne, które są wykorzystywane w ramach dotychczasowej praktyki prowadzenia operacji wpływu politycznego przez rosyjskie służby specjalne. Ponadto, należy ocenić, iż w obecnej sytuacji nie ma istotnego zagrożenia bezpośredniego wpływu na wynik wyborów we Francji.

Rekomendacja:

Należy przeprowadzić testy, które odpowiedzą na pytanie, jaki wpływ na polski proces wyborczy miałyby techniki zastosowane przez Rosję w innych krajach. **[2]**

Big data wsparciem w walce z terroryzmem

KOMUNIKAT

9 marca 2017. *Big data* to sformułowanie odnoszące się do gromadzenia i przetwarzania danych ilościowych o ogromnej skali. Zakres przedmiotowy *Big data* określa koncepcja *3V – Volume Velocity Variety* – określająca zbiory informacji o dużej objętości, dużej zmienności czy dużej różnorodności, których opracowanie wymaga zastosowania odpowiedniej infrastruktury oraz użycia zaawansowanych narzędzi informatycznych i analitycznych. Termin *big data* w ostatnich latach cieszy się niesłabnącą popularnością. Obserwowany trend wzrostowy, a nawet swoista *moda na Big data*, ma bez wątpienia źródło w postępującym procesie *cyfryzacji*. To bowiem *cyfrowe ślady*, coraz liczniej pozostawiane przez użytkowników Internetu i nabywców usług elektronicznych, są w wielkich bazach podstawowym źródłem danych i decydują o ich stale rosnącym potencjale. Oprócz licznych zastosowań biznesowych, technologie *Big data* mogą dostarczać odpowiedzi na aktualne problemy cywilizacyjne i przyczyniać się do lepszego objaśniania współczesnego świata. Na początku marca br. portal Engineering.com zamieścił notatkę opisującą jedną z najnowszych prób wykorzystania *Big data* do modelowania zagrożeń terrorystycznych. Algorytm *Networked Pattern Recognition (NEPAR)* został opracowany w Nowym Jorku przez badaczy z Binghamton University. Do konstrukcji modelu wykorzystano informacje na temat ponad 150 tys. ataków z lat 1970-2015. Przeprowadzone analizy pozwoliły określić wzory aktów terroryzmu, ustalić relacje pomiędzy atakami, a także wskazać miejsca szczególnie narażone na ich wystąpienie. Intencją autorów było wsparcie władz Stanów Zjednoczonych w lepszym rozumieniu zjawiska terroryzmu, nakreślaniu scenariuszy przyszłych zdarzeń i im zapobieganiu.

Wnioski: coraz bardziej efektywne modelowanie wielkich zbiorów danych będzie wspierać organy państwa w rozwiązywaniu istotnych problemów społecznych. **[13/7]**

Wybrane źródła:

Douglas Laney, *The Importance of Big Data: A Definition*, Gartner (https://www.gartner.com/login/loginInitAction.do?method=initialize&TARGET=http%253A%252F%252Fwww.gartner.com%252Fdocument%252F2057415)

The Engineer, marzec 2017, *Big Data Predicts Terrorist Attacks with More Than 90% Accuracy*, Engineering.com (http://www.engineering.com/DesignerEdge/DesignerEdgeArticles/ArticleID/14426/Big-Data-Predicts-Terrorist-Attacks-with-More-Than-90-Accuracy.aspx)

Tutun Salih, Khasawneh Mohammad T., Zhuang Jun, *New framework that uses patterns and relations to understand terrorist behaviors*, Expert Systems with Applications, volume 78, 2017, s. 358-375 (http://www.sciencedirect.com/science/article/pii/S0957417417301161)

Zaprezentowano robot bojowy, który wkrótce może zmienić sytuację na polu walki

SYGNAŁ

15 marca 2017. Amerykańska spółka Boston Dynamics, która należy do korporacji Google Inc., zademonstrowała **nowatorski model robota przemieszczającego się na dwóch nogach** („Handle")[61]. Roboty tego typu mają funkcjonować w takich samych sytuacjach jak ludzie i np. korzystać z takich samych urządzeń technicznych lub narzędzi, a nawet uzbrojenia. W przeciwieństwie do innych projektów budowy półautonomicznych robotów zastępujących człowieka[62] rozwiązanie zaproponowane przez Boston Dynamics wyróżnia się tym, że **nogi robota kończą się kółkami**. Dzięki temu dochodzi do fuzji ewolucyjnych osiągnięć *Homo sapiens* z rozwiązaniami charakterystycznymi dla maszyn.

Nowatorskość w porównaniu do dotychczasowych robotów wiąże się z dłuższą pracą na jednym załadowaniu baterii, większą szybkością, zwrotnością, lepszym pokonywaniem wybranych przeszkód. „Handle" ma mieć znaczną przewagę na drogach, w budynkach i innych płaskich powierzchniach nad robotami, których nogi są pozbawione kółek; w takich sytuacjach „Handle" ma przewagę również nad ludźmi.

Rekomendacja: warto nie tylko monitorować projekty Boston Dynamics i innych podobnych podmiotów, ale również na podstawie oceny osiągów i potencjału rozwiązań takich jak robot „Handle" prowadzić prace nad wykorzystywaniem własnych modeli oraz nad technikami przeciwdziałania robotom na polu walki. **[4/8]**

Barometr Ryzyka Nadużyć w Zamówieniach Publicznych: nowe narzędzie do analizy patologii gospodarczych

KOMUNIKAT

20 marca 2017. Pod koniec lutego br. Fundacja im. Stefana Batorego (wspólnie z portalem Zamówienia 2.0 i węgierską organizacją Government Transparency Institute) upubliczniła – na stronie www.barometrryzyka.pl – Barometr Ryzyka Nadużyć w Zamówieniach Publicznych. Barometr jest indeksem zbudowanym z dziewięciu wskaźników, które pomagają oszacować ryzyko wystąpienia nieprawidłowości w konkretnym postępowaniu o zamówienie. Wskaźniki te to:

„(1) tryb zamówienia,
(2) szczegółowość (długość) opisu przedmiotu zamówienia,
(3) opis (długość) kryteriów kwalifikowalności,
(4) liczba wymaganych poświadczeń i certyfikatów,
(5) wysokość wadium,
(6) waga kryteriów pozacenowych,
(7) czas od ogłoszenia do zamknięcia naboru ofert,
(8) czas od zamknięcia naboru ofert do podjęcia decyzji o wyborze wykonawcy,
(9) sytuacja, gdy w postępowaniu wystąpił tylko jeden oferent”[63].

Autorzy narzędzia szczegółowo omawiają konstrukcję indeksu, a także algorytm obliczania końcowego wyniku, który przyjmuje postać liczby od 0 do 1[64]. Poszczególnym wskaźnikom przypisano wagi; za najważniejszy wskaźnik uznano „pojedynczego oferenta”.

Autorzy prezentują także pierwsze ustalenia, poczynione przy użyciu nowego narzędzia oraz kilkadziesiąt szczegółowych rekomendacji. Wskazują, że np. polski rynek zamówień poniżej progów unijnych jest niekonkurencyjny (odsetek postępowań, w których pojawił się tylko jeden oferent, przekracza 40%), zaś obszary szczególnie wysokiego ryzyka obejmują: zamówienia inicjowane w dwóch ostatnich i dwóch pierwszych miesiącach roku kalendarzowego, zamówienia, w których oferentami są spółki, których właścicielami są instytucje publiczne oraz organizacje społeczne (te zależne od lokalnych władz, jak np. OSP, kluby sportowe czy koła łowieckie)[65].

Uruchomiony przez partnerów projektu portal internetowy stwarza możliwość wykorzystania narzędzia do własnych analiz, m.in. dzięki wyszukiwarce, która pozwala przeglądać wszystkie postępowania o zamówienia publiczne z lat 2010-2015 pod kątem słów kluczowych. Autorzy narzędzia podkreślają, że udostępniają szczegółową metodologię narzędzia po to, by było ono rozwijane i adaptowane do monitorowania innych obszarów życia społeczno-gospodarczego.

Rekomendacje:

1. Należy przeanalizować doświadczenia i wnioski twórców Barometru pod kątem opracowania analogicznego narzędzia detekcji nieprawidłowości w innych obszarach życia społeczno-gospodarczego. Jak się wydaje, do obszarów i zjawisk możliwych do zbadania zaproponowaną metodą należą m.in.:
   - tryb zatrudniania w instytucjach publicznych;

- zjawisko nepotyzmu w instytucjach publicznych[66];
- sektor przedsiębiorstw państwowych.

2. Warto zbadać możliwości wykorzystania Barometru do analizy działalności pasożytniczych grup interesów, w tym np. poprzez rozbudowanie istniejącego narzędzia na zasadzie uwzględnienia dodatkowych kryteriów. Autorzy dokonali wyboru 9 wskaźników spośród co najmniej 64, o których istnieje dostępna wiedza; wykorzystanie części z nich jest możliwe, choć wymagałoby dodatkowych obliczeń[67].
3. Należy rozważyć ryzyko i konsekwencje wykorzystywania informacji agregowanych za pomocą Barometru do celów walki politycznej przez którąkolwiek ze stron sporu. **[5/6]**

Przypisy

[1] https://www.facebook.com/notes/mark-zuckerberg/building-global-community/10154544292806634.

[2] Zuckerberg podaje jako przykład trudności automatycznego rozróżnieniu postów informacyjnych od postów rekrutacyjnych związanymi z działaniami terrorystów.

[3] Ta funkcjonalność już jest zaimplementowana w algorytmach sterujących publikacją informacji na news feed. Zaakceptowanie wiadomości do publikacji zależny m.in. od następującej heurystyki: „jeśli użytkownik przekazuje wiadomość do znajomych po 'długim' czytaniu, to jest większe prawdopodobieństwo, że wiadomość jest wartościowa".

[4] Omawiany dokument jest nawet mocniejszy w przekazie: „keep improving our tools to help more people register and **vote**".

[5] Katarzyna Kwiatkowska, *Zuckerberg z Sankt Petersburga*, „wyborcza.pl" 7 grudnia 2012.

[6] Mark Scott, *Mail.ru Takes Full Ownership of VKontakte, Russia's Largest Social Network*, „dealbook.nytimes.com" 16 września 2014. Dostępne na: https://dealbook.nytimes.com/2014/09/16/mail-ru-takes-full-ownership-of-vkontakte-russias-largest-social-network/ (data odczytu 15 marca 2017).

[7] https://br-analytics.ru/statistics/author?hub_id=3&date=201702&country_id=0&period_type=month () – twórcy postów.

[8] Eric Eldon, *Attack of the Facebook clones: Russia's Vkontakte*, http://venturebeat.com 5 września 2007. Dostępne na: http://venturebeat.com/2007/09/05/attack-of-the-facebook-clones-russias-vkontakte/ (data odczytu: 17 marca 2017). Taylor Buley, *Facebook's Russian Frenemy With Benefits*, "Forbes" 13 lipca 2009. Dostępne na: https://www.forbes.com/2009/07/13/facebook-vkontakte-russia-technology-internet-facebook.html (data odczytu: 17 marca 2017).

[9] Zakładka „About" na stronie VK. Dostępna na: https://vk.com/about (data odczytu: 15 marca 2017).

[10] Np. z powodu zarzutów producentów muzycznych przez półtora roku na VK nie była dostępna muzyka w formie streamingowej.

[11] Vladimir Kozlov, *Again Labeled 'Notorious,' Russia's VKontakte Vows to Keep Fighting Piracy in 2017*, „Billboard" 23 grudnia 2016. Dostępne na: http://www.billboard.com/articles/business/7633166/russia-vkontakte-piracy-2017-licensing-content (data odczytu 17 marca 2017).

[12] *Zasady* działania VK. Dostępne na: https://vk.com/terms (data odczytu 17 marca 2017).

[13] *Polityka prywatności VK*. Dostępna na: https://vk.com/privacy (data odczytu 17 marca 2017).

[14] Pkt. 4.2.1. *Polityki Prywatności VK*.

[15] Pkt. 4.2.5. *Polityki Prywatności VK*.

[16] Pkt. 5.1.5. *Polityki Prywatności VK*.

[17] Zakładka „About" na stronie VK. Dostępna na: https://vk.com/about (data odczytu: 15 marca 2017).

[18] „Alexa.com" [22 lutego 2017].

[19] 2. „Youtube.com", 4. „Google.com", 5. „Allegro.pl", 6. „Onet.pl", 7. „Wp.pl", 8. „Wikipedia.org", 9. „Olx.pl".

[20] Próba stworzenia reklamy została podjęta w marcu 2017 roku.

[21] Por. Piotr Celej, *Myślałeś, że polski Facebook to dno i hejt? Na rosyjskim VKontakte jest inny stan umysłu...*, „natemat.pl" 30 grudnia 2015. Dostępne na: http://natemat.pl/166715,myslales-ze-polski-facebook-to-dno-i-hejt-na-rosyjskim-vkontakte-jest-inny-stan-umyslu (data odczytu: 15 marca 2017).

[22] T. Romm, Silicon Valley leaders organizing against Trump, 02.03.2017, http://www.politico.com/story/2017/02/silicon-valley-against-trump-234579 [odczyt: 17.03.2017].

[23] M. Isaac, Uber C.E.O. to Leave Trump Advisory Council After Criticism, 02.02. 2017. https://www.nytimes.com/2017/02/02/technology/uber-ceo-travis-kalanick-trump-advisory-council.html [odczyt: 17.03.2017].

[24] *China invents the digital totalitarian state*, "Economist", 17.12.2016, http://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian (data odczytu: 03.03.2017).

[25] Dokument w chińskim oryginale oraz angielskim tłumaczeniu Rogiera Creemersa, badacza z Uniwersytetu w Oxfordzie, zob. *Planning Outline for the Construction of a Social Credit System,* GF No. (2014)21 (2014-2020), https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/ data publikacji: 14 czerwca 2014 [data modyfikacji: 25.04.2015; data odczytu: 03.03.2017]. Omówienie dokumentu oraz praktycznych aspektów pilotażowych wdrożeń znaleźć można w artykule R. Creemersa, Petera Mattisa, Samanthy Hoffman i Pameli Kyle Crossley pt. *What Could China's 'Social Credit System' Mean for its Citizens*? "Foreign Policy", 15.08.2016, http://foreignpolicy.com/2016/08/15/what-could-chinas-social-credit-system-mean-for-its-citizens/ (data odczytu: 03.03.2017).

[26] Celia Hatton, *China 'social credit': Beijing sets up huge system*, 26.10.2015, http://www.bbc.com/news/world-asia-china-34592186. Choć dominują głosy podkreślające zagrożenia, niektórzy komentatorzy wskazują na analogiczne mechanizmy, które już funkcjonują w państwach zachodnich. Przykładowo, Pamela Kyle Crossley, professor historii z Dartmouth College (USA) wskazuje, że już teraz wykorzystywany w USA rating kredytowy FICO wpływa na to, jak szybko wchodzi się na pokład samolotu, zaś ratingi z mediów społecznościowych oraz platform handlowych miewają wpływ na zatrudnienie lub awans pracowników; zob. http://foreignpolicy.com/2016/08/15/what-could-chinas-social-credit-system-mean-for-its-citizens/ (data odczytu: 03.03.2017). *China invents the digital totalitarian state*, Economist, 17.12.2016, http://www.economist.com/news/briefing/21711902-worrying-implications-its-social-credit-project-china-invents-digital-totalitarian (data odczytu: 03.03.2017).

[27] Catherine Shu, *Data From Alibaba's E-Commerce Sites Is Now Powering A Credit-Scoring Service*, 27.01.2015 https://techcrunch.com/2015/01/27/data-from-alibabas-e-commerce-sites-is-now-powering-a-credit-scoring-service/ (data odczytu: 03.03.2017).

[28] *Ant Financial Unveils China's First Credit-Scoring System Using Online Data*, 27.01.2015, http://www.marketwatch.com/story/ant-financial-unveils-chinas-first-credit-scoring-system-using-online-data-2015-01-27 (data odczytu: 03.03.2017). Co ciekawe, istnieje anglojęzyczna strona usługi, https://www.creditsesame.com/, na której podano wysoce niejasne informacje nt. sposobu funkcjonowania systemu. Jak się wydaje, na stronie tej zaprezentowano wersję systemu dla klienta amerykańskiego, z funkcjonalnością ograniczoną do oceny zdolności kredytowej.

[29] Przykład z miejscowości Hangzhou; co ciekawe, punktacja jest ustalana przy pomocy skanera twarzy; zob. *Face-scanning assists borrowing in Hangzhou community*(1/4), 2017-03-02, http://www.ecns.cn/visual/hd/2017/03-02/122731.shtml (data odczytu: 03.03.2017).

[30] *Just spend*, "Economist" z dn. 17.11.2016, http://www.economist.com/news/finance-and-economics/21710292-chinas-consumer-credit-rating-culture-evolving-fastand-unconventionally-just (data odczytu: 03.03.2017). Hal Hodson, *Inside China's plan to give every citizen a character score*, 14.10.2015, https://www.newscientist.com/article/mg22830432-100-inside-chinas-plan-to-give-every-citizen-a-character-score/ (data odczytu: 03.03.2017).

[31] *Propaganda Games: Sesame Credit - The True Danger of Gamification - Extra Credits*, 16.12.2015, https://www.youtube.com/watch?v=lHcTKWiZ8sI (data odczytu: 03.03.2017).

[32] Wypowiedź R. Creemersa, zob. *Inside China's plan…*.

[33] *Questions and Answers about the East StratCom Task Force*, 26/11/2015, https://eeas.europa.eu/headquarters/headquarters-homepage_en/2116/%20Questions%20and%20Answers%20about%20the%20East%20StratCom%20Task%20Force (data odczytu: 13.03.2017).

[34] *Tamże.*

[35] Mark Scott, Melissa Eddy, *Europe Combats a New Foe of Political Stability: Fake News*, 20.02.2017, https://www.nytimes.com/2017/02/20/world/europe/europe-combats-a-new-foe-of-political-stability-fake-news.html (data odczytu: 13.03.2017).

[36] M. Boni, *Chcecie wyplenić fałszywe wiadomości? Uczcie ludzi, jak korzystać z mediów*, „Gazeta Wyborcza" z dn. 8 marca 2017.

[37] Przykładowy numer biuletynu nt. *Polski: Focus on Poland*, nr 48 - 22 listopada 2016, http://us11.campaign-archive1.com/?u=cd23226ada1699a77000eb60b&id=62d2998c9e (data odczytu: 13.03.2017).

[38] http://www.atlanticcouncil.org/blogs/natosource/seven-allies-establish-nato-s-strategic-communications-center-of-excellence-in-latvia (data odczytu: 13.03.2017).

[39] http://www.stratcomcoe.org/about-us (data odczytu: 13.03.2017).

[40] Anthony Faiola, *As Cold War turns to Information War, a new fake news police combats disinformation*, 22.01.2017. https://www.washingtonpost.com/world/europe/as-cold-war-turns-to-information-war-a-new-fake-news-police/2017/01/18/9bf49ff6-d80e-11e6-a0e6-d502d6751bc8_story.html?utm_term=.f9f2e15890af (data odczytu: 13.03.2017).

[41] http://www.army.mod.uk/structure/39492.aspx (data odczytu: 13.03.2017).

[42] Ewan MacAskill, *British army creates team of Facebook warriors*, "The Guardian", 31 stycznia 2015, https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade (data odczytu: 13.03.2017).

[43] Tamże. Zob. też: *Army sets up new brigade 'for information age'*, http://www.bbc.com/news/uk-31070114, 31.01.2015 (data odczytu: 13.03.2017).

[44] *Germany plans creation of 'center of defense' against fake news, report says*, http://www.dw.com/en/germany-plans-creation-of-center-of-defense-against-fake-news-report-says/a-36887455. (data odczytu: 13.03.2017).

[45] Bundespresseamt will Fake News strafrechtlich nicht bewerten, http://www.faz.net/aktuell/politik/inland/kein-zentrum-gegen-desinformationen-im-bundespresseamt-14652042.html 15.01.2017 (data odczytu: 13.03.2017).

[46] *Germany plans creation of 'center of defense' against fake news, report says*, http://www.dw.com/en/germany-plans-creation-of-center-of-defense-against-fake-news-report-says/a-36887455. (data odczytu: 13.03.2017).

[47] *Finland plans to set up center to counter 'hybrid' threats*, 21.11.2016, http://www.reuters.com/article/us-eu-defence-finland-hybrid-idUSKBN13G1F8 (data odczytu: 13.03.2017).

[48] http://www.stopfake.org/en/about-us/ (data odczytu: 13.03.2017).

[49] Andrew E. Kramerfeb, *To Battle Fake News, Ukrainian Show Features Nothing but Lies,* 26.02.2017, https://www.nytimes.com/2017/02/26/world/europe/ukraine-kiev-fake-news.html?_r=0 (data odczytu: 13.03.2017).

[50] http://www.europeanvalues.net/kremlinwatch/ Kremlin Watch. (data odczytu: 13.03.2017).

[51] Zob. J. Janda, O. Kunda, *Mechanisms of Influence of the Russian Federation into Internal Affairs of the Czech Republic*, 04.09.2016, http://www.europeanvalues.net/wp-content/uploads/2016/09/Mechanisms-Of-Influence-Of-The-Russian-Federation-Into-Internal-Affairs-Of-The-Czech-Republic.pdf (data odczytu: 13.03.2017).

[52] Michael Colborne, *Meet the Czechs fighting back against Russia's (dis)information war,* "The Sydney Morning Herald", 19.12.2016, http://www.smh.com.au/world/meet-the-czechs-fighting-back-against-russias-disinformation-war-20161215-gtcbh5.html (data odczytu: 13.03.2017).

[53] https://www.facebook.com/pg/EEICzs/about/?ref=page_internal.

[54] Budżet samej telewizji RT (dawniej: Russia Today) wynosi ok 300 mln USD rocznie; unijny East StratCom Task Force nie posiada nawet wydzielonego budżetu, niedawno w Parlamencie Europejskim odrzucono wniosek o dodatkowe 800 tys. EUR na potrzeby zespołu. W dn. 22.02.2017 rosyjski Minister Obrony Siergiej Szojgu ogłosił oficjalnie, że Rosja utworzyła jednostki do prowadzenia walki informacyjnej, zob. Russia sets up information warfare units - defence minister, 22.02.2017, http://www.reuters.com/article/russia-military-propaganda-idUSL8N1G753J (data odczytu: 14.03.2017).

[55] Rachel Stern, *Germany's plan to fight fake news*, 09.01.2017, http://www.csmonitor.com/World/Passcode/2017/0109/Germany-s-plan-to-fight-fake-news (data odczytu: 13.03.2017).

[56] R. Standish, *Why is Finland better at fending off Russian-linked fake news*? "The Star", 1.03.2017, https://www.thestar.com/news/world/2017/03/01/why-is-finland-better-at-fending-off-russian-linked-fake-news.html (data odczytu: 13.03.2017).

[57] J.W. Aldershoff, Massive uproar on alleged Windows 10 built-in 'keylogger' feature, 23.03.2017, http://www.myce.com/news/massive-uproar-alleged-windows-10-built-keylogger-feature-81685/ [odczyt: 27.03.2017].

[58] J.Styczyński i P. Słowik, UOKiK i GIODO idą na wojnę z Microsoftem. Poszło o Windows 10, 22.08.2016, http://technologia.dziennik.pl/aktualnosci/artykuly/529246,uokik-i-giodo-ida-na-wojne-z-microsoftem-poszlo-o-windows-10.html [odczyt 27.03.2017].

[59] D.Długosz, CNIL: Windows 10 jest niebezpieczny, 24.07.2016, http://www.komputerswiat.pl/nowosci/programy/2016/30/cnil-windows-10-jest-niebezpieczny.aspx [odczyt 27.03.2017].

[60] A.Kalia. With Windows 10, Microsoft Blatantly Disregards User Choice and Privacy: A Deep Dive, 17.03.2017, https://www.eff.org/deeplinks/2016/08/windows-10-microsoft-blatantly-disregards-user-choice-and-privacy-deep-dive [odczyt 27.03.2017].

[61] Robert Hackett, *Leaked Video Reveals 'Nightmare Inducing' Google Robot*, „fortune.com" 2 lutego 2017. Dostępne na: http://fortune.com/2017/02/02/boston-dynamics-robot-video/; Erico Guizzo i Evan Ackerman, *Boston Dynamics Officially Unveils Its Wheel-Leg Robot: 'Best of Both Worlds'*, „IEEE Spectrum" 27 lutego 2017. Dostępne na: http://spectrum.ieee.org/automaton/robotics/humanoids/boston-dynamics-handle-robot; Kelly Hodgkins, *Boston Dynamics shows off first official video of its new wheel-footed robot*, „digitaltrends.com" 27 lutego 2017 r. Dostępne na: http://www.digitaltrends.com/cool-tech/boston-dynamics-handle-robot-nightmare/#ixzz4auvr1gtG; Lucinda Shen, *Boston Dynamics Reveals New 'Nightmare-Inducing' Robot*, „fortune.com" 28 lutego 2017 r. Dostępne na: http://fortune.com/2017/02/28/boston-dynamics-robot-jobs-handle/; Matt Simon, *Boston Dynamics' New Rolling, Leaping Robot Is an Evolutionary Marvel*, „wired.com" 1 marca 2017. Dostępne na: https://www.wired.com/2017/03/boston-dynamics-new-rolling-leaping-robot-evolutionary-marvel/ (data odczytu odnośników z przypisu: 10 marca 2017 r.).

[62] Uczestniczących np. w „DARPA Robotics Challenge" zorganizowanym przez amerykańską rządową Defence Advanced Research Projects Agency w latach 2012-2015.

[63] Grzegorz Makowski, *Jak ograniczyć ryzyko nadużyć w zamówieniach publicznych? Najważniejsze ustalenia i postulaty na podstawie Barometru Ryzyka Nadużyć w Zamówieniach Publicznych,* http://barometrryzyka.pl/dokumenty/0_zamowienia_policy_brief.pdf [dostęp: 20.03.2017]. Autor ten przypomina, że „wartość polskiego rynku zamówień publicznych wynosi co roku około 115–150 miliardów złotych (około 6–10% PKB)" (tamże).

[64] W konstrukcji narzędzia posiłkowano się doświadczeniami z pracy nad podobnym narzędziem na Węgrzech; zob. Mihály Fazekas, *'Red flags' of institutionalised grand corruption in EU-regulated Polish public procurement*, 26.02.2016, http://barometrryzyka.pl/dokumenty/Fazekas_TEDPL_CRI_description_ENG_160226_form.pdf [dostęp: 20.03.2017]. Autor ten zauważa, że istnienie układu korupcyjnego wymaga, by pewien krąg podmiotów

regularnie otrzymywał zamówienia publiczne; skalę korupcji można pośrednio szacować analizując wykorzystanie przez te podmioty technik ograniczania konkurencji (np. skracanie czasu na przygotowanie oferty); zob. tamże, s. 2. Zob. też, M. Fazekas, *Pomiar ryzyka nadużyć w zamówieniach publicznych. Na podstawie danych z polskiego Biuletynu Zamówień Publicznych*, Budapeszt, grudzień 2015; http://barometrryzyka.pl/dokumenty/metodologia_BRN.pdf [dostęp: 20.03.2017].

[65] Grzegorz Makowski, *Jak ograniczyć ryzyko nadużyć…?* s. 3-5. Zob. też G. Makowski, *Skala i charakter ryzyka nadużyć na rodzimym rynku zamówień publicznych. Mapa zagrożeń i węzłowe problemy*, Warszawa, luty 2017.

[66] Jako jeden z bardziej wyrazistych przykładów zjawiska nepotyzmu wśród polskich instytucji publicznych w ostatnich latach wskazywano Polską Agencję Żeglugi Powietrznej; zob. W. Gadomski, *Agencja rodzinna, czyli kto pracuje w Polskiej Agencji Żeglugi Powietrznej*, 07.06.2011, http://wyborcza.pl/1,76842,9736930,Agencja_rodzinna__czyli_kto_pracuje_w_Polskiej_Agencji.html [dostęp: 20.03.2017].

[67] http://barometrryzyka.pl/metodologia/ [dostęp: 20.03.2017].