Biuletyn Ośrodka Studiów nad Wyzwaniami Cywilizacyjnymi
CBB ASzWoj
Numer 1 | luty 2017

W numerze:

1. Nowe metody marketingu politycznego mogą zadecydować o wyniku wyborów.

- W kampaniach wyborczych poprzedzających Brexit i wybory prezydenckie w USA wykorzystano innowacyjne metody wpływu na preferencje wyborców.
- Rekomendujemy objęcie monitoringiem i zweryfikowanie skuteczności tych metod szczególnie w kontekście zbliżających się wyborów w Polsce w 2018 r.

2. Komercyjne *fake news* zagrożeniem dla suwerenności informacyjnej.

- Rozprzestrzenianie fałszywych wiadomości dokonywane jest nie tylko w celach propagandowych, ale także dla zysku.
- Zalew *fake news* obniża zdolność do odróżniania prawdy od fałszu, prowadzi do umacniania się podziałów społecznych i obniża sterowność państwa.
- Rekomendujemy wspieranie przez państwo ośrodków dostarczających rzetelne informacje i analizy oraz weryfikujących fałszywe wiadomości.

3. Badacze rosyjskiej dywersji informacyjnej opracowali jej model, dzięki któremu można odróżnić ją od spontanicznego szumu w cyberprzestrzeni.

4. Należy powołać centralne biuro oceny technologii.

- Skoordynowany rozwój cywilizacyjny Polski, wymaga zinstytucjonalizowanego namysłu nad skutkami rozwoju innowacji.
- W większości państw rozwiniętych instytucje oceny technologii działają od lat 90-tych XX wieku. W Polsce ocena technologii istnieje obecnie jedynie w formie zalążkowej.
- Rekomendujemy powołanie instytucji odpowiedzialnej za systemową ocenę technologii w Polsce. Optymalną formułą, byłoby powołanie centralnego biura oceny technologii współpracującego z niezależnymi instytucjami eksperckimi.

5. Uzależnienie od infrastruktury elektronicznej zagraża bezpieczeństwu państwa.

- Decydenci, urzędnicy, wojsko i zwykli obywatele nie potrafią funkcjonować bez pośrednictwa elektroniki.
- Infrastruktura elektroniczna podatna jest na zniszczenie wskutek katastrofy naturalnej, awarii, dywersji terrorystycznej lub ataku bronią elektromagnetyczną.
- Nagła awaria elektroniki doprowadzi do natychmiastowego paraliżu instytucji państwa i dezorganizacji społecznej.
- Rekomendujemy wprowadzenie polityki „zarządzania cyfrowym wykluczeniem" – celowego utrzymywania mechanizmów zarządzania państwem i regulacji współżycia obywateli zdolnych do działania w przypadku awarii elektroniki i sieci informatycznych.

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

1. KOMUNIKAT: Modelowanie psychograficzne i mikrotargetingowy marketing – nowe metody wpływania na preferencje wyborcze

Po ogłoszeniu wyników wyborów prezydenckich w Stanach Zjednoczonych, media zachodnie i krajowe obiegła informacja, że twórcą sukcesu wyborczego Donalda Trumpa jest firma *Cambridge Analytica* (*CA*)[1]. Opinię taką miał wyrazić m.in. Frank Luntz, słynny amerykański badacz i doradca polityczny, stwierdzając, iż to działania *CA* doprowadziły Trumpa do zwycięstwa. *CA* to brytyjska firma specjalizująca się w komunikacji politycznej, działająca na pograniczu badań społecznych, *data miningu* oraz marketingu. Przypuszcza się, że metodologia zastosowana przez *CA* czerpie z dorobku naukowego analityka i psychologa polskiego pochodzenia, dra Michała Kosińskiego. Badania prowadzone przez Kosińskiego w ramach współpracy University of Cambridge i Stanford University wykazały, że modele statystyczne korzystające z danych z serwisów społecznościowych są w stanie zrekonstruować profil psychologiczny człowieka trafniej niż znające go osoby. Jak dowodzi naukowiec, „na podstawie 10 facebookowych lajków sztuczna inteligencja może ocenić osobowość człowieka trafniej niż kolega z pracy; na podstawie 70 lajków – oceni lepiej niż przyjaciel; na podstawie 150 – lepiej niż rodzice; a na podstawie 250 – lepiej niż partner życiowy (…). Na podstawie 100 do 200 lajków jesteśmy w stanie określić poglądy polityczne dowolnej osoby z paroprocentowym marginesem błędu. I to po odrzuceniu wszystkich lajków dotyczących polityki”[2]. *Cyfrowe ślady* pozostawiane przez użytkowników internetu w serwisach społecznościowych, przeglądarce internetowej, czy smartfonie, mogły z powodzeniem zostać wykorzystane do odtworzenia cech osobowości pojedynczych Amerykanów, stanowiąc punkt wyjścia do *psychograficznego mikrotargetingowego marketingu*. Istotą mikrotargetingowego marketingu jest emisja zróżnicowanych komunikatów, do możliwie małych i homogenicznych grup odbiorców, których siła perswazyjna – za sprawą precyzji oraz psychologicznej optymalizacji – jest dalece większa od efektywności tradycyjnych metod marketingowych – niuansujących przekaz na poziomie, obiektywnie heterogenicznych, wielkich grup demograficznych. Jak podaje *Das Magazin*, sztab Donalda Trumpa tylko w dniu debaty z Hillary Clinton rozesłał, m.in. za pośrednictwem portalu Facebook, ok. 175 tys. różnych wariacji haseł wyborczych i argumentów. Na swojej stronie internetowej *CA* deklaruje, iż jest w posiadaniu zbiorów danych obejmujących przeszło 5 tys. zmiennych (*data points*), charakteryzujących ponad 220 mln Amerykanów, w tym ponad 100 *punktów* wykorzystuje do budowy algorytmów umożliwiających psychograficzną segmentację obserwacji oraz predykcję zachowań i postaw obywateli.

Wnioski: korzyści płynące z modelowania psychograficznego i mikrotargetowania treści marketingowych podnoszą obie metody do rangi potencjalnych *game changerów*, mogących zredefiniować mechanizmy prowadzenia kampanii informacyjnych w Polsce (i na temat Polski). Istnieje prawdopodobieństwo zastosowania *big data* i elementów psychograficznego mikrotergetingowego

marketingu w kampaniach poprzedzających przyszłoroczne wybory samorządowe oraz późniejsze wybory prezydenckie i parlamentarne.

Rekomendacje: ze względu na realne zagrożenie dla bezpieczeństwa obywateli państwa polskiego, należy podjąć działania zmierzające do kompleksowej diagnozy zakresu gromadzonych danych i podmiotów je przetwarzających, jak również do określenia sposobów i skali wykorzystania tego typu zasobów, w szczególności dla celów modelowania psychograficznego. Rekomenduje się rozważenie ogólnopolskiej kampanii zwiększającej społeczną świadomość problemów prywatności w sieci oraz wprowadzenie regulacji prawnych, które zmniejszą ryzyko wykorzystywania osiągnięć informatyki społecznej w złej wierze – np. dla celów zniesławiania osób prywatnych i publicznych, manipulowania dużymi kategoriami społecznymi lub budowania pozycji marki, w tym marki politycznej, w oparciu o nierzetelne informacje – nie ograniczając przy tym dalszego rozwoju tej dziedziny wiedzy i jej społecznie doniosłych, pożytecznych, zastosowań. **[13]**

2. KOMUNIKAT: Komercyjne *fake news* – potencjalne konsekwencji dla Polski

Problem:

Po wyborach prezydenckich w USA w listopadzie 2016 roku globalnym tematem dyskusji stał się problem potencjalnego wpływu fałszywych informacji szerzonych za pośrednictwem mediów społecznościowych (głównie Facebooka), które przyczyniły się do zwycięstwa Donalda Trumpa[3]. Większość uwagi poświęcono potwierdzonemu oficjalnie przez CIA zaangażowaniu Rosji, przejawiającemu się próbami masowej manipulacji opinią publiczną w USA[4]. O ile praktyki takie (np. prowadzenie tzw. farm trolli, czyli zorganizowanych grup osób produkujących masowo treści propagandowe zamieszczane w Internecie, w tym w mediach społecznościowych) były znane już wcześniej, zaskoczeniem była skala oddziaływania oraz jego potencjalnie decydujący wpływ na wynik wyborów.

Osobnym problemem okazała się analogiczna działalność, prowadzona przez **grupy i jednostki działające (najprawdopodobniej) wyłącznie dla zysku**. Dziennikarskie śledztwo portalu BuzzFeed, a także innych mediów (np. amerykańskiej telewizji NBC News) pozwoliło ustalić, że grupa ok. 300 osób, głównie młodych, relatywnie wykształconych (w tym – znających dobrze angielski i obeznanych w niuansach sytuacji w USA) ludzi zamieszkujących miasto Veles w Macedonii, wykorzystała (i nadal wykorzystuje) regulacje dotyczące polityki reklamowej Google i Facebooka, zarabiając na fałszywych newsach kierujących ruch w Internecie na prowadzone przez nich strony. **Metoda** działania polega zasadniczo na kopiowaniu cudzych treści i opatrywaniu ich sensacyjnymi tytułami, a następnie upowszechnianie ich za pomocą sieci społecznościowych; rzadziej – na samodzielnym wytwarzaniu kłamliwych treści. Podobną aktywność odnotowano w Rumunii, ale także na terenie USA, gdzie działalność zaledwie jednego człowieka (Paula Hornera) doprowadziła do rozpowszechnienia wielu fałszywych informacji, które zyskały wielki rozgłos także w obiegu oficjalnym (np. były podawane przez telewizje czy Google News). Newsy te były jednoznacznie przychylne dla Trumpa, choć część ich autorów (w rozmowach z dziennikarzami) deklarowała obojętność w kwestii wyniku wyborów; wybór treści przekazu tłumaczyli większym rozgłosem (a więc perspektywą zysków), z jakim spotykały się newsy przychylne wobec DT a krytyczne wobec Clinton.

W reakcji na te doniesienia zarówno Facebook, jak i Twitter zadeklarowały wdrożenie rozwiązań mających na celu ograniczenie problemu (np. algorytmów wykrywających i blokujących kłamliwe treści), zaś w Kongresie USA zgłoszono projekt utworzenia komisji śledczej.

Wnioski:

1. W nawiązaniu m.in. do tezy P. Pomerantzeva, a także mechanizmu tzw. kaskad informacyjnych i zjawiska baniek informacyjnych[5], można wnioskować, że wzrost znaczenia sieci społecznościowych jako źródła informacji sprzyja pogłębianiu podziałów społecznych i politycznych, prowadzi do brutalizacji polityki i uwiądu kultury demokratycznej debaty, utrudnia zawieranie ponadpartyjnych koalicji i porozumień, a więc **obniża sterowność państwa**. Jest tak, gdyż algorytmy mediów społecznościowych promują (wyświetlają) treści już wcześniej preferowane przez internautę (tj. na ogół zgodne z jego poglądami). W efekcie, internauci zamykają się w kręgu ludzi podobnie myślących. Różnice poglądów wydają się coraz większe, podziały głębsze, poglądy przeciwników coraz bardziej odrażające i niezrozumiałe.
2. W krótkim i średnim okresie zjawisko „fałszowania newsów dla zysku" może **grozić destabilizacją sceny politycznej** w krajach demokratycznych, w tym także w Polsce. Daje niewidocznym i/lub dotychczas nieliczącym się aktorom (np. grupom czy wręcz jednostkom z krajów i/lub środowisk peryferyjnych) potężne narzędzia wpływu **poza kontrolą istniejących mechanizmów prawnych i politycznych**.
3. Można zauważyć **proces upodabniania się mediów tradycyjnych** głównego nurtu (np. prasy) do logiki, która generuje *fake news*. Jako niedawny przykład tego procesu można wskazać artykuł na łamach tygodnika „Der Spiegel" z dn. 12.12.2016, dotyczący populizmu, który zilustrowano zdjęciem plakatu trzymanego przez jednego z uczestników pewnej demonstracji, na którym N. Farage, J. Kaczyński, M. Le Pen i V. Orban pokazani są w mundurach ze swastykami; choć formalnie zdjęcie było tylko ilustracją, w rzeczywistości stanowiło *clickbait* – przynętę dla czytelnika gazety; strategia ta niewiele różni się od strategii wytwórców *fake news*.
4. W dłuższej perspektywie problem *fake news* grozi dewaluacją dążenia do prawdy oraz demontażem podstawowych zasad demokracji i wartości cywilizacji Zachodu. Zdaniem części analityków (np. P. Pomerantzeva) sytuacja taka jest **zbieżna ze strategicznymi celami Rosji:** zgodne z koncepcją tzw. zarządzania refleksyjnego, podważenie wiarygodności wszelkich przekazów utrudnia przeciwnikowi rozpoznanie własnej sytuacji i podejmowanie decyzji.

Prognoza: czego się spodziewać?

1. Rosnące „oswojenie" opinii publicznej z nieprawdopodobnymi scenariuszami, wydarzeniami, opiniami będzie sprzyjać **wzrostowi wpływu ugrupowań/polityków o skrajnych poglądach**;
2. Pojawi się możliwość przekierowywania przez podmioty zagraniczne (lub krajowe) opinii publicznej w określonym kierunku w celu **wpłynięcia**

na wynik wyborów zgodnie z własnymi preferencjami (lub w sposób przypadkowy);

3. Podjęte zostaną próby (najprawdopodobniej selektywnego i kontrowersyjnego) filtrowania treści, oceny wiarygodności, rzetelności, stopnia radykalizmu treści krążących w mediach społecznościowych, rodzące pokusę i **ryzyko cenzury** tych mediów – współcześnie jednego z kluczowych źródeł informacji ludzi o świecie; FB i Google mają swe polityczne preferencje (światopogląd liberalny, generalnie wsparły Demokratów) i już dziś pojawiają się sygnały o postulowaniu przez nie konieczności eliminacji treści uznawanych za „radykalnie prawicowe";
4. Zapowiadane środki zaradcze zapewne okażą się jedynie połowicznie skuteczne; należy się spodziewać, że dezinformatorzy znajdą alternatywne sposoby kontynuowania swego modelu biznesowego. Dodatkowo, motywację koncernów informacyjnych do walki z nadużyciami obniża sytuacja **konfliktu interesów**, w jakim się znajdują – *fake news* również zwiększają ich „oglądalność".

Rekomendacje:

1. Rozważyć zasadność prawnego uregulowania odpowiedzialności autorów fałszywych newsów;
2. Opracować mechanizmy wsparcia przez państwo (najlepiej ponadpartyjnie) ośrodków generujących rzetelne analizy i publikujących sprawdzone informacje; np. wzmocnienie Polskiej Agencji Prasowej jako jednego z kluczowych rozsadników rzetelnej informacji;
3. Oszacować stopień narażenia Polski na opisane manipulacje poprzez analizę wielkości krajowego rynku reklamowego w sieciach społecznościowych (Google AdSense, Facebook); przyjąć założenie, że im większy w skali globalnej ten rynek, tym bardziej prawdopodobne jest wystąpienie zjawiska w Polsce;
4. Wspierać proces powstawania ośrodków (w tym NGO) skoncentrowanych na weryfikacji prawdziwości informacji (kluczowy zasób – dziennikarze), istotny w kontekście kryzysu prasy w Polsce, a także dominacji kapitału zagranicznego na polskim rynku medialnym;
5. Monitorować i przeciwdziałać próbom zastosowania opisanych powyżej instrumentów w celu wpływania na przebieg wyborów samorządowych w Polsce w roku 2018
6. W kontekście krajowym pamiętać o tzw. **youtuberach**, czyli osobach zarabiających poważne pieniądze na generowaniu „zaraźliwych" (często obraźliwych, wulgarnych lub przynajmniej prowokujących) treści na portalu Youtube. Czołowi youtuberzy w Polsce, często osoby bardzo młode, gromadzą nawet do 3 mln regularnych odbiorców (tzw. subskrybentów). O ile obecnie generowane przez nich treści nie mają na ogół charakteru politycznego (zazwyczaj są „jedynie" ogłupiające), należy monitorować aktywność najbardziej wpływowych w celu wykrycia ewentualnego „wychylenia" politycznego, szczególnie w zakresie stosunku do Rosji. **[5]**

3. ANALIZA: Infowojna czy infozgiełk? Kryteria odróżniania na przykładzie doświadczeń z konfliktu ukraińskiego[i]

Streszczenie

Jednym z celów „wojny informacyjnej" jest wywołanie **stanu powszechnej dezorientacji** w obrębie danej zbiorowości. Esencją takich działań jest doprowadzenie do sytuacji, w której odróżnienie elementów spontanicznych od zorganizowanych staje się niemożliwe. Dlatego tego rodzaju praktyki w znacznej części przypadków są trudne do wykrycia.

Wnioski i rekomendacje

W związku z tym rekomendujemy **regularne monitorowanie przekazów informacyjnych (dobieranych celowo bądź losowo)** z uwzględnieniem kryteriów pozwalających odróżnić spontaniczne akty komunikacyjne od zaplanowanych przedsięwzięć; te ostatnie wyróżniają następujące cechy:

1. masowość i wielokanałowość;
2. szybkość, ciągłość i powtarzalność;
3. brak wymogu związku z obiektywną rzeczywistością;
4. brak wymogu spójności wewnętrznej (w przypadku pochodzenia z tego samego źródła informacji);
5. wykorzystywanie „trolli" (i botów).

Ponadto, rekomendujemy następujące działania nakierowane na wykrywanie wrogich ataków na elementy infrastruktury krytycznej:

- rozpowszechnianie informacji o takich atakach;
- stałe badanie ewentualnej korelacji pojawiania się przekazów informacyjnych o powyżej wymienionych cechach z danymi o rzeczywistych atakach na infrastrukturę krytyczną.

Analizę prowadzoną za pomocą powyższych wskaźników warto uzupełnić o poszukiwanie ewentualnych podwykonawców komercyjnych. Strategia prywatyzacji działań wojennych odnosi się również do wojen informacyjnych. Dlatego ważne jest prowadzenie stałego monitoringu oferty i działań agencji PR oraz think tanków oferujących takie usługi. Należy również rozwijać analizy studiów przypadków wykrytych wojen informacyjnych.

W praktyce, wyżej naszkicowany monitoring mógłby wyglądać następująco (zakładając, że opieramy się wyłącznie na danych jawnych, publicznie dostępnych):

[i] Fragment wykorzystano w raporcie OSWC „Formalne i nieformalne, wewnętrzne i zagraniczne grupy interesów jako ograniczenie potencjału rozwojowego Polski" przygotowanym przez zespół dr. Macieja Gurtowskiego.

1. Wylosowanie bądź celowy dobór monitorowanych mediów.
2. Identyfikacja (na początku ręczna, po jakimś czasie zautomatyzowana) informacji na podstawie wymienionych powyżej kryteriów.
3. Śledzenie: komentarzy internautów na stronach serwisów informacyjnych, schematów rozprzestrzeniania się informacji w mediach społecznościowych, wykrywanie modyfikacji informacji w trakcie rozprzestrzeniania się.
4. Przypisywanie autorstwa poszczególnych informacji konkretnym grupom interesu.
5. Identyfikacja powtarzających się osób, instytucji bądź wzorców w kontekście rozpowszechniania informacji.

Osobno następowałoby rejestrowanie informacji medialnych dotyczących wszelkich zakłóceń funkcjonowania infrastruktury krytycznej, w tym: informacji o atakach hakerskich na instytucje publiczne, nagłych przerwach w funkcjonowaniu systemów bankowości elektronicznej, problemach w funkcjonowaniu sieci telefonii komórkowej, paraliżach komunikacyjnych na kolei itp. Rejestracja tego rodzaju informacji wymagałaby przygotowania zautomatyzowanych narzędzi.

Po wdrożeniu takiego systemu (obejmującym opracowanie narzędzi, dobór obserwowanych mediów itp.), część pracy miałaby charakter zautomatyzowany, niemniej działanie takie wymagałoby ciągłej pracy zespołu przynajmniej kilkuosobowego zajmującego się bezpośrednio monitoringiem mediów, wspieranego przez przynajmniej jednego informatyka-statystyka. System mógłby stanowić zaplecze dla aktywnego przeciwdziałania atakom informacyjnym i wojnie informacyjnej.

Analiza

W złożonych układach społecznych problem odróżniania elementów spontanicznych i zorganizowanych jest zagadnieniem kluczowym. Im bardziej złożone jest społeczeństwo, im większy wolumen informacji znajduje się w obiegu, tym trudniej oddzielić działania przypadkowe od intencjonalnych działań.

Chcąc ustalić, czym wyróżniają się zorganizowane działania informacyjne lub szerzej – intencjonalne działania rozmaitych grup – w przestrzeni społecznej, warto wyjść od przypadku, który jest dość dobrze opisany i może stanowić model tego rodzaju aktywności. Chodzi tutaj o działania Federacji Rosyjskiej, które określane są mianem „wojny informacyjnej" (aczkolwiek w obiegu są też takie spokrewnione, choć nietożsame pojęcia jak „walka informacyjna", „wojna sieciowa", „zarządzanie refleksyjne", „sterowanie refleksyjne" i inne; bliskie jest też pojęcie „wojny hybrydowej"). Istnieje wiele opracowań pokazujących, na czym polega specyfika tak rozumianej wojny informacyjnej[6]. Najprościej rzecz ujmując, chodzi tu o systemowe i

intencjonalne oddziaływanie na masową świadomość w trakcie rywalizacji między państwami (i cywilizacjami), także podmiotami pozapaństwowymi. Oddziaływanie takie ma miejsce w przestrzeni informacyjnej (zawierającej w sobie zarówno mass-media tradycyjne, jak i media społecznościowe), a „bronią" są rozmaite sposoby kontroli i wykorzystania informacji[7]. Należy podkreślić, że Rosja rozwija ten sposób działania od wielu lat nakładem poważnych sił i środków. Można powiedzieć, że problematyka wojen informacyjnych jest obecnie w Rosji silnie zinstytucjonalizowaną nauką praktyczną, której uczeni są dyplomaci, żołnierze czy studenci kierunków humanistyczno-społecznych[8]. Krótka charakterystyka typowych elementów działań podejmowanych w ramach „walki informacyjnej" może uwrażliwić nas na to, jak odróżnić elementy intencjonalne od spontanicznego szumu informacyjnego.

Amerykańscy psychologowie współpracujący ze znanym think tankiem RAND Corporation, Christopher Paul i Miriam Matthews, wyróżnili następujące cechy charakteryzujące działania **czysto informacyjne** (propagandowe) w rosyjskim modelu wojny informacyjnej:

- są masowe i wielokanałowe;
- są szybkie, ciągłe i powtarzalne;
- nie wymagają związku z obiektywną rzeczywistością;
- nie wymagają spójności wewnętrznej[9].

Dobrym przykładem empirycznym **masowości** i **wielokanałowości** jest przypadek działań komunikacyjnych towarzyszących interwencji rosyjskiej na Ukrainie. Jak pisze Jolanta Darczewska: „W bezprecedensowej pod względem skali kampanii dezinformacji na temat sytuacji na Ukrainie uruchomiono wszystkie federalne kanały telewizyjne, radiowe, gazety, mnóstwo zasobów internetowych. Front informacyjny wsparli dyplomaci, politycy, politolodzy, eksperci, elita nauki i kultury. Front ten został rozwinięty wiele lat wcześniej. Na początku kryzysu ukraińskiego (Euromajdan) sprzężono go z dywersją ideologiczną, polityczną, socjokulturową, prowokacją, aktywnością dyplomacji"[10]. **Wskaźnikiem intencjonalności jest w takim przypadku masowość i wielokanałowość przekazu**. Można założyć, że jeśli dany przekaz informacyjny jest wieloźródłowy i zarazem masowy, zapewne jest związany z działaniem jakiejś zorganizowanej grupy.

Szybkość odnosi się do rozpowszechniania informacji jak najprędzej, bez żadnej weryfikacji, wyłącznie w celu wywarcia pierwszego wrażenia na odbiorcy. Dlatego, zgodnie z doktryną rosyjską, pierwsze pojawienie się danego przekazu informacyjnego powinno być szybkie i wyraźnie dostrzegalne. Z kolei **ciągłość** i **powtarzalność** mają prowadzić do oswojenia się przez odbiorców z informacją, a następnie do jej akceptacji[11].

Wyjaśniając dlaczego **brak związku z obiektywną rzeczywistością** jest istotną cechą wojny informacyjnej ponownie można odwołać się do przykładu propagandy

podczas wojny na Ukrainie: „Po wojskowym zajęciu i inkorporacji Krymu do Rosji mechanizmy dezinformacji miały uwiarygodnić intencje Moskwy i ukryć braki w argumentacji co do działań wojskowych oraz samego wcielenia Krymu. Argumentacja ta była absurdalna: obawiano się <<wtargnięcia banderowców na Krym>>, <<zajęcia baz Floty Czarnomorskiej przez NATO>>, <<derusyfikacji obywateli Ukrainy>> itd., itp."[12]. W połączeniu z masowością przekazu prowadziło to do sytuacji, w której trudno odróżnić stwierdzenia prawdziwe od fałszywych. Dodatkowo, jak zauważają Christopher Paul i Miriam Matthews, „Dane stwierdzenia są łatwiejsze do zaakceptowania, jeśli są oparte na dowodach, nawet jeśli dowody są fałszywe"[13]. Zatem **wskaźnikiem działań intencjonalnych jest stałe podawanie nieprawdziwych stwierdzeń, przy jednoczesnym popieraniu ich dowodami empirycznymi**.

Brak spójności wewnętrznej oznacza, że w trakcie konkretnej wojny informacyjnej mogą występować obok siebie przekazy zupełnie ze sobą sprzeczne. Przykład to zaprzeczanie w jednym przekazie, że na Krymie są jacyś rosyjscy żołnierze, i jednoczesne potwierdzanie tego w innym. Efektem jest brak jasności i zamieszanie wśród części odbiorców; inni z kolei nie dostrzegają tych sprzeczności bądź skupiają się na szukaniu ich racjonalnego wytłumaczenia[14]. Należy zatem zwracać uwagę na sytuacje, w których jednocześnie z – jak się wydaje – jednego źródła wysyłane są sprzeczne informacje.

Wskazuje się, że na potrzeby wojen informacyjnych w Rosji funkcjonują specjalne „farmy trolli"[15], w których pracują ludzie zadaniowani do walki informacyjnej. Ich celem jest rozpowszechnianie danych przekazów informacyjnych oraz włączanie do takiej aktywności innych osób aktywnych w Internecie, które – zupełnie nieświadomie i z bardzo różnych powodów – mogą wspierać ich aktywność. Identyfikacja tego rodzaju aktywności jest dość trudna. W przypadku rosyjskich trolli może pomóc analiza błędów językowych i szukanie (również zautomatyzowane) obecności rusycyzmów. Niemniej, w miarę profesjonalizacji tego rodzaju działań (i doskonalenia automatycznych translatorów), ten wskaźnik będzie tracił na znaczeniu. W przypadku outsourcingu tego rodzaju działań (np. zlecania ich agencjom PR), kryterium językowe może nie mieć charakteru wskaźnikowego, podobnie zresztą w przypadku działania krajowych grup interesu. Coraz istotniejszą kwestią są boty – proste programy, które udają użytkowników Internetu. Całe ich grupy są nadzorowane przez trolli nadzorujących kontrolujących pracę botów. Dzięki temu siła „farm trolli" może ulec zwielokrotnieniu.

Cechą specyficzną wojny informacyjnej jest to, że obejmuje ona działania, które same w sobie często trudno uznać za akty wrogości. To znaczy, medialnej manipulacji i perswazji nie da się łatwo oddzielić od działań bardziej agresywnych, np. ataków hakerskich. Jak zauważa Keir Giles, ataki hakerskie typu DDoS[16], jak i działalność stacji telewizyjnej RT (dawniej Russia Today) są powiązanymi ze sobą narzędziami wojny informacyjnej[17]. Z tego względu **osobne diagnozowanie zagrożeń technicznych** (cyberataki) **oraz informacyjnych** (propaganda,

perswazja) **jest błędem**. Dodatkowo, należy pamiętać, że cyberataki mogą nie mieć na celu wyrządzenia szkód materialnych, a jedynie wywołanie paniki w społeczeństwie czy też podważenie kompetencji władz[18].

W fazie przejściowej między wojną informacyjną a wojną hybrydową (granica jest tu dość płynna), coraz ważniejsze staje się **współwystępowanie działalności propagandowej z atakami na infrastrukturę krytyczną**, czyli „rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa" (…). Infrastruktura krytyczna obejmuje systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych"[19]. Monitorowanie częstotliwości awarii (i rozpoznawanych ataków) elementów infrastruktury krytycznej, a także łączenie tego rodzaju wydarzeń z wojną informacyjną jest niezbędnym działaniem pozwalającym wykrywać intencjonalne działania silnych grup interesu **[8]**

4. ANALIZA: Izolacja cyfrowa jako zasób strategiczny państwa w kontekście zagrożeń związanych ze zniszczeniem infrastruktury elektronicznej

Streszczenie

1. Mamy do czynieniu z **postępującym uzależnieniem** wielu dziedzin życia społecznego (w tym – infrastruktury krytycznej państwa) **od technologii informacyjno-komunikacyjnych** (ICT).

2. Istnieje poważne zagrożenie związane katastrofą naturalną, awarią, sabotażem lub atakiem z użyciem **broni** wykorzystującej **impuls EMP** (broni elektromagnetycznej, tzw. „E-bomby"[20]) które mogą zniszczyć i zakłócić działanie urządzeń elektronicznych na terenie państwa. Broń oparta na impulsie EMP **niszcząca infrastrukturę elektroniczną** jest względnie tania, działa z prędkością światła, jest precyzyjna, nie zostawia ofiar śmiertelnych, jest cicha, może przenikać przez ściany budynków i niektóre przeszkody naturalne. Co czyni ją właściwą dla działań z zakresu **wojny hybrydowej**, gdyż jej użycie raczej początkowo będzie identyfikowane jako awaria, nie jako atak.

3. Rekomendujemy:

- opracowania programu **polityki zarządzania wykluczeniem cyfrowym**, czyli zaplanowanego izolowania określonych obszarów państwa od uzależnienia od technologii **informacyjno-komunikacyjnych**. W przypadku zniszczeń infrastruktury elektronicznej na skutek ataku EMP lub katastrofy naturalnej, zdolność do zorganizowanego funkcjonowania instytucji państwa i poszczególnych grup ludności będzie kluczowym zasobem strategicznym rozstrzygającym o fizycznym przetrwaniu.
- rozważenie wykonania **technologicznego „kroku w bok"** w niektórych dziedzinach infrastruktury krytycznej państwa, poprzez szersze wprowadzenie technologii mechanicznych, optycznych i być może także elektronicznych wykorzystujących technologie lampowe jako mniej podatnych na zniszczenia impulsem EMP.
- zdecydowane **zintensyfikowanie prac badawczo-rozwojowych** nad własnymi technologiami wykorzystującymi impuls EMP, jako skutecznej i „humanitarnej broni", mającej zastosowanie zarówno militarne, jak i antyterrorystyczne, ofensywne i defensywne. Istnieje pilna potrzeba rozwoju technologii **wykrywania** samej obecności broni EMP w pobliżu infrastruktury krytycznej państwa oraz wczesnego wykrywania przypadków użycia tejże broni.
- niezwłoczne wprowadzenie rozbudowanego **systemu zabezpieczeń** wybranych elementów infrastruktury krytycznej państwa przed oddziaływaniem E-broni.
- przeprowadzenie szeroko zakrojonych **działań kontrwywiadowczych** mających za zadanie rozpoznanie czy i w jakim stopniu na terenie naszego kraju oraz w pobliżu np. polskich placówek zagranicznych już ulokowano urządzenia i instalacje, które zdolne są do generowania efektów właściwych dla broni EMP.

Analiza

Postępujące uzależnienie od elektroniki zagrożeniem dla bezpieczeństwa

Ważną cechą społeczeństw współczesnych jest powszechne wykorzystywanie technologii telekomunikacyjnych i informatycznych. Nie są one jedynie udogodnieniem, czy narzędziem wspierającym funkcjonowanie systemów społecznych. Są one fundamentem infrastruktury tego typu społeczeństw. Technologie te pośredniczą powszechnie w relacjach między ludźmi i ci ostatni w coraz mniejszym stopniu chcą i potrafią funkcjonować bez tego technologicznego pośrednictwa.

Kolejne dziedziny życia społecznego: praca, nauka, kultura, rozrywka, opieka zdrowotna i dostęp do nich, w tym także zaspokajanie podstawowych potrzeb życiowych, uzależnione są od zaawansowanych (skomputeryzowanych) urządzeń elektronicznych. **Coraz częściej dostęp ten jest bezalternatywny**. Przykładowo: brak karty kredytowej czy konta na popularnym portalu społecznościowym może podnieść cenę lub nawet uniemożliwić nabycie określonego towaru czy usługi, czasem także usługi publicznej o podstawowym charakterze. Brak dostępu do nowych mediów czy też brak umiejętności posługiwania się nimi w coraz większym stopniu oznacza także brak możliwości uczestniczenia w życiu społecznym. Osoby z jakiegoś powodu nie korzystające z technologii elektronicznych, w sytuacji, gdy społeczeństwo przenosi coraz bardziej swoje funkcjonowanie do sieci, pozbawiane bywają możliwości partycypacji w nim. To zjawisko nazywane jest „cyfrowym wykluczeniem" i ma ono wyraźnie pejoratywny wydźwięk.

Badacze zajmujący się problematyką „cyfrowego wykluczenia" powszechnie przyjmują założenie, że osoby podlegające temu zjawisku, muszą przełamać bariery odpowiedzialne za trudności z korzystaniem z mediów elektronicznych i dołączyć do reszty społeczeństwa uzależnionej od urządzeń elektronicznych. Zazwyczaj, za „wykluczone cyfrowo" uważa się osoby starsze wiekiem, niewykształcone, niezamożne i mieszkające na wsi, a czasem także niepełnosprawne[21]. Receptą na to mają być np. programy edukacyjne zachęcające ludzi w wieku dojrzałym do nauki korzystania z komputera czy też polityka dostarczania dostępu do Internetu w różne oddalone od dużych ośrodków miejskich rejony. W skali globalnej w ten trend wpisują się inicjatywy korporacji Facebook na polu rozwoju technologii „dronów solarnych" i innych nowych technik dostarczania dostępu do sieci bezprzewodowej (np. satelity).

Badacze we współpracy z ekspertami opracowującymi założenia do polityki społecznej postulują działania z zakresu e-Integracji[22], czyli konieczności motywowanego etycznie włączenia osób wykluczonych cyfrowo w grono osób zaspokajających swoje potrzeby za pośrednictwem urządzeń elektronicznych. Tego rodzaju dążenie do uzależnienia kolejnych grup społecznych

od nowoczesnych technologii – jeśli realizowane w sposób bezrefleksyjny – jest polityką nietrafną. **Postulujemy działanie odwrotne – aby rozważyć zjawisko cyfrowego wykluczenia jako istotny strategiczny zasób państwa**, nie zaś jedynie jako przejaw zacofania. Powód jest następujący: grupy, czy też całe konteksty społeczne, które są w stanie funkcjonować bez pośrednictwa urządzeń i mediów elektronicznych, posiadają wyższą zdolność sprawnego funkcjonowania w warunkach awarii, katastrofy naturalnej, dywersji terrorystycznej czy ataku bronią wykorzystującą impuls niszczący elektronikę (broń elektromagnetyczna, broń EMP, E-bomba[23]).

Katastrofa naturalna może uszkodzić infrastrukturę elektroniczną

We wrześniu 1859 roku w wielu miejscach na świecie zaobserwowano anomalie w funkcjonowaniu urządzeń wykorzystujących prąd elektryczny[24]. Dotyczyły one nie tylko zakłóceń ich poprawnego funkcjonowania – zaobserwowano także, że telegrafy odłączone od zasilania były w stanie nadawać sygnał. Współcześnie interpretuje się to zdarzenie jako efekt tzw. „słonecznej burzy magnetycznej", czyli kosmicznej anomalii pogodowej skutkującej uwolnieniem znacznej ilości plazmy ze Słońca w kierunku Ziemi, czemu towarzyszą poważne zakłócenia w polu elektromagnetycznym.

Podczas prób nuklearnych na Pacyfiku w 1962 roku zaobserwowano[25], że eksplozji bomby towarzyszą zniszczenia elektroniki znajdującej się daleko poza obszarem rażenia oraz zakłócenia działania urządzeń elektrycznych nawet znacznie (nawet 1445 km) oddalonych od epicentrum wybuchu. Zintensyfikowano badania nad nowym typem broni, której efektywność miała sprowadzać się do jej niszczycielskiego działania na elektronikę.

Broń elektromagnetyczna

Istnieją doniesienia medialne na temat zaobserwowania efektów zbliżonych do użycia tego typu broni podczas konfliktu w Kosowie[26] i Iraku[27]. Według względnie aktualnych (listopad 2015 rok) doniesień Amerykanie i Chińczycy dysponują mobilnymi stacjami zdolnymi do rażenia impulsem elektromagnetycznym, które można instalować na samochodach; zasięg ich oddziaływania szacuje się na kilkadziesiąt metrów[28].

Brakuje publicznie dostępnej wiedzy, jakie dokładnie zniszczenia i na jakim obszarze dokona uderzenie dużą E-bombą wywołującą impuls EMP[29]. Przyjmuje się, że w przypadku impulsu EMP towarzyszącemu naziemnej eksplozji nuklearnej o mocy 10 kT niszczące dla urządzeń elektronicznych działanie obejmie obszar o średnicy 6–16 km[30]. Niszczący zasięg oddziaływania może być większy niż samo pole objęte impulsem ze względu na zjawisko określane mianem „source-region EMP", któremu towarzyszy rozprzestrzenianie się impulsu poprzez materiały przewodzące: rury, kable. Brakuje dokładniejszych oszacowań, jak daleko może sięgać ten efekt. Natomiast zwiększa się podatność kolejnych obszarów na tego typu atak z powodu rosnącego wykorzystywania, zwłaszcza w układach sterujących,

instalacji elektronicznych zawierających elementy półprzewodnikowe, dla których niszczące są nawet niewielkie skoki napięcia. Należy zaznaczyć, że sprzęt elektroniczny wniesiony do strefy działania EMP po ustaniu impulsu będzie funkcjonował normalnie z tym zastrzeżeniem, że np. telefony nie będą mogły dokonywać połączeń za pośrednictwem lokalnych stacji bazowych, które zostały uszkodzone.

Osobnym problemem jest kwestia wpływu oddziaływania impulsu EMP na życie i zdrowie człowieka[31]. Przyjmuje się, że jest to broń nie-zabójcza (*non-lethal*), ale twierdzenie o jej humanitarnym charakterze może być mylące, ponieważ wpływ pola magnetycznego na ludzki organizm nie jest obojętny i w pewnych warunkach morze być szkodliwy[32]. Rażenie ciała bronią wykorzystującej mikrofale może skutkować bólem i poparzeniami[33]. Pośrednio także zniszczenie infrastruktury np. szpitala doprowadzić może do śmierci wielu osób. Nie wiadomo, jakie mogą być następstwa indukowania się napięcia np. na metalowych protezach, szynach usztywniających złamania. Będzie to zależało od odległości od źródła impulsu.

Rekomendacje

Rekomendujemy zdecydowane zintensyfikowanie prac badawczo-rozwojowych nad własnymi technologiami broni elektromagnetycznej, jako skutecznej i „humanitarnej broni", mającej zastosowanie zarówno militarne, jak i antyterrorystyczne, ofensywne i defensywne. W tym ostatnim wypadku impuls elektromagnetyczny jawi się jako skuteczne narzędzie do zwalczania zagrożenia w postaci dronów.

Istnieje także pilna potrzeba rozwoju technologii wykrywania samej obecności broni EMP w pobliżu infrastruktury krytycznej państwa oraz wczesnego wykrywania przypadków użycia tejże broni. Urządzenia zdolne do rażenia elektromagnetycznego mogą być maskowane i przypominać wyglądem urządzenia cywilne i pod taką legendą mogą być lokowane przez np. przedsiębiorstwa w pobliżu elementów infrastruktury krytycznej państwa.

Kluczową rekomendacją, którą proponujemy poddać głębszemu namysłowi, jest rozważenie wprowadzenia polityki intencjonalnego zarządzania wykluczeniem cyfrowym. Miałaby ona polegać na zerwaniu z naiwnym i pewnym sensie przymusowym włączaniem kolejnych obszarów funkcjonowania państwa, gospodarki i życia obywateli w sieć infrastruktury zarządzanej przez urządzenia elektryczne. W szczególności idzie o narastający trend tzw. Internetu Rzeczy (czy nawet Internetu Wszystkiego).

Sednem problemu nie jest **zakwestionowanie sensu postępu technologicznego, ale jego demonopolizacja**. Składające się na system Internetu Rzeczy sieci teleinformatyczne i urządzenia elektroniczne nie powinny mieć wyłączności na regulowanie współdziałania obywateli, urzędników i instytucji. Zwłaszcza w niektórych obszarach instytucjonalnych należy przywrócić urządzeniom tym rolę wspomagającą, a nie silnie definiującą funkcjonowanie społeczeństwa.

W praktyce polityka ta miałaby sprowadzać się do równoczesnego prowadzenia dotychczasowych prac na rzecz wdrażania zaawansowanych technologii teleinformatycznych z równoczesnym zachowaniem, przywracaniem i rozwijaniem niezapośredniczonych elektrycznie alternatywnych kanałów komunikacji i procedur ważnych dla bezpieczeństwa państwa.

W kontekście rywalizacji ekonomicznej i politycznej dalsze korzystanie i rozwijanie technologii teleinformatycznych wydaje się być koniecznością. Zagrożenie związane z podatnością tych technologii na ataki bronią elektromagnetyczną nakazują bezzwłoczne wprowadzenie kompleksowego systemu zabezpieczeń (zob. informacje na temat prowadzonego projektu NCBIR[34]). Wybitny znawca problematyki broni EMP Carlo Kopp[35] postuluje, by zabezpieczanie całej infrastruktury krytycznej państwa przed atakiem EMP było wymuszone prawnie, tak jak to jest obecnie z zabezpieczeniami przeciwpożarowymi. Kopp zwraca także uwagę, że istotnie taniej jest tworzyć zabezpieczone systemy od nowa, np. stawiać nowe budynki, czy budować pomieszczenia niż przerabiać już istniejące[36].

Zalecamy też wykonanie swoistego audytu sprawdzającego, czy i w jakim stopniu ukryte głęboko pod ziemią bunkry przeciwatomowe z grubymi ścianami ze zbrojonego betonu są podatne na atak EMP.

Należy przygotować odpowiednio zabezpieczone magazyny zawierające zapasowy, zdolny do autonomicznego funkcjonowania przez dłuższy czas sprzęt elektroniczny, który mógłby przetrwać np. spowodowaną czynnikami naturalnymi burzę magnetyczną.

Rekomendujemy rozważenie szerszego korzystania z technologii nieopartych o urządzenia elektryczne podatne na zniszczenie bronią elektromagnetyczną. Impuls EMP niszczy przede wszystkim urządzenia, w których napięcia są niewielkie, np. procesory. Zwiększenie napięcia nawet o tylko 1 V może prowadzić do nieodwracalnych uszkodzeń. Kłopot w tym, że wykorzystywanie układów opartych o procesory staje się powszechne nawet w miejscach i urządzeniach, które tradycyjnie nie wymagały tego rodzaju elektronicznego nadzoru (np. samochody).

Należy rozważyć, czy w niektórych typach urządzeń i instalacji kluczowych dla bezpieczeństwa państwa warto by wrócić do technologii wykorzystujących lampy elektronowe, które są mniej podatne na zniszczenia bronią elektromagnetyczną, ponieważ znoszą duże zmiany napięcia. Elektronika lampowa, mimo ograniczeń dotyczących jej wydajności, może zostać wykorzystana np. do konstrukcji prostych urządzeń sterujących lub komunikacyjnych, które mogłyby zostać wykorzystane w przypadku awarii innych systemów łączności.

Przykładem tego typu swoistego „technologicznego kroku w tył" są testy możliwości wykorzystania ptaków drapieżnych do zwalczania dronów[37]. Na podobnej zasadzie można rozważyć opracowanie na wypadek kryzysu systemu komunikacji wykorzystującego tradycyjne środki przekazu informacji w postaci gońców, czy wyszkolenie „trenerów" gołębi pocztowych. Te ostatnie bywają współcześnie

wykorzystywane przez zorganizowaną przestępczość jako „bezpieczny" kanał komunikacji[38].

Priorytetowo rekomendujemy niezwłoczne przeprowadzenie szeroko zakrojonych zadań kontrwywiadowczych, których celem będzie wytypowanie lokalizacji sąsiadujących z elementami infrastruktury krytycznej państwa podatnymi na atak bronią elektromagnetyczną i skontrolowanie ich otoczenia pod kątem wykrycia ewentualnych przypadków ulokowania tam urządzeń zdolnych do rażenia impulsem EMP. Umieszczenie takich instalacji może odbyć się np. pod pozorem prowadzenia działalności gospodarczej.

Rekomendujemy rozważenie działań zmierzających do celowego rozpraszania geograficznego elementów infrastruktury krytycznej państwa, które ograniczyłoby zakres zniszczeń spowodowanych serią impulsów EMP

Rekomendujemy wprowadzenie systemu regularnych, cyklicznych ćwiczeń dla instytucji mających znaczenie dla bezpieczeństwa państwa sprawdzających ich zdolność do funkcjonowania w przypadku uszkodzenia wszystkich urządzeń zasilanych prądem elektrycznym lub uszkodzenia tych z nich, które nie były odpowiednio zabezpieczone. Zakładamy, że czymś oczywistym i pożądanym jest szkolenie i ćwiczebne testowanie pododdziałów wojsk różnych typów w warunkach utrudniających lub kompletnie uniemożliwiających stosowanie nowoczesnych technologii. Szczególny nacisk powinien zostać położony na testowanie możliwości koordynacji współpracy różnych jednostek w takich warunkach **[3]**.

5. ANALIZA: Potrzeba systemowej oceny technologii[ii]

Streszczenie

1. System oceny technologii (ang. *technology assessment* – dalej: TA) jest istotnym elementem zarządzania innowacjami technologicznymi. Jego zadaniem jest **oparta na nauce ocena skutków i oddziaływań nowych rozwiązań technologicznych na społeczeństwo, kulturę, politykę, gospodarkę i środowisko**. Stanowiąc system wczesnego ostrzegania przed potencjalnymi niebezpieczeństwami związanymi z określonymi technologiami, stanowi istotny element szeroko pojmowanego bezpieczeństwa narodowego.

2. **Instytucje oceny technologii działają od lat 90-tych XX wieku w większości państw rozwiniętych**. Ocena technologii obejmuje zarówno wąskie, specjalistyczne zagadnienia związane z bezpieczeństwem określonych produktów (np. leków czy substancji wykorzystywanych w przemyśle), aż po **wzbudzające kontrowersje społeczne nowe trendy rozwojowe**, takie jak rozpowszechnianie się Internetu Rzeczy, zagrożenia z zakresu cyberbezpieczeństwa, rozwój neuronauki czy sztucznej inteligencji.

3. Odpowiedzialny rozwój Polski, na który składa się zapewnienie odpowiednich relacji między rozwojem technologicznym a rozwojem społecznym, nie może obyć się bez jakiejś formy zinstytucjonalizowanego **namysłu nad kierunkiem i charakterem rozwoju innowacji, umożliwiającym zarządzanie procesami społeczno-technologicznymi.** Zinstytucjonalizowana ocena technologii pozwala w systematyczny i oparty na nauce sposób identyfikować, rozpatrywać i dokonywać wyboru odpowiednich opcji rozwojowych. Ponadto, **ogranicza nieformalne, quasi-lobbystyczne wpływy grup interesu** powiązanych z określonymi opcjami technologicznymi, które w sposób niejawny mogą oddziaływać na procesy rozwojowe.

4. **W Polsce ocena technologii istnieje obecnie jedynie w formie zalążkowej.** Proponowaną formą instytucjonalną dla systemu TA w Polsce jest połączenie pracy biura oceny technologii z niezależnymi instytucjami, dedykowanymi do wykonywania różnego rodzaju prac badawczych w obszarze TA. Pozwoliłoby to wykorzystać zalety jednego i drugiego rozwiązania: bliskość decydentów z elastycznością i niezależnością działania.

Analiza

Cele i funkcje oceny technologii

Ocena technologii (ang. *Technology Assessment* – dalej: TA) jest zinstytucjonalizowaną procedurą naukowej oceny procesów powstawania, rozwoju,

[ii] Rozszerzona wersja niniejszej analizy znajduje się w raporcie OSWC „Nowe technologie w kontekście interesu narodowego RP. Przegląd problemów i rekomendacje" przygotowanym przez zespół prof. Jerzego Surmy.

wdrażania, rozprzestrzeniania i oddziaływania innowacji naukowo-technologicznych na społeczeństwo, gospodarkę i środowisko. Analiza TA ukierunkowana jest na dostarczanie wiedzy pomocnej przy podejmowaniu decyzji politycznych; jednocześnie ma za zadanie wczesne sygnalizowanie i ostrzeganie przed możliwymi zagrożeniami, tworzenie społecznej świadomości w zakresie różnych aspektów rozwoju naukowo-technologicznego, stymulowanie debaty publicznej, kształtowanie postaw i opinii w stosunku do nowych technologii. Skrótowo rzecz ujmując, TA to **rodzaj opartego na wiedzy doradztwa politycznego w zakresie rozwoju naukowo-technologicznego**.

Strategiczna ocena technologii ma za zadanie dostarczać wiedzy pomagającej w kształtowaniu strategii rozwoju technologii nie tylko przez decydentów politycznych, ale także przez podmioty prywatne zaangażowane w tworzenie innowacji. Naczelnym celem jest kształtowanie kierunków rozwoju naukowo-technologicznego w pożądanym społecznie kierunku. By móc zapewnić zgodność między rozwojem innowacji a rozwojem społecznym, TA poszerzyła swój obszar działania o podejście partycypacyjne, umożliwiające włączanie w procesy tworzenia wiedzy różnych interesariuszy.

Potrzeba oceny technologii wiąże się z pojawianiem się nowych wyzwań cywilizacyjnych. Problemem nie jest już tylko to, czy dana technologia może okazać się szkodliwa dla środowiska, zdrowia ludzkiego czy mieć niekorzystny wpływ na warunki życia części społeczeństwa. W obliczu takich zjawisk jak konieczność wypracowania nowych sposobów zapewnienia stabilnych źródeł energii, konsekwencji zmian klimatycznych, perspektyw rozwoju sztucznej inteligencji, Internetu Rzeczy i robotyzacji sfery komunikacji, konieczna jest całościowa i wielowymiarowa wiedza wyprzedzająca bieg zjawisk.

Dominujący obecnie (choć wciąż nie jedyny) kształt oceny technologii, mającej ambicję bycia „strategiczną", tym zatem różni się od poprzednich, iż nie ogranicza się tylko do reagowania na powstające innowacje i poddawania ich ocenie na zamówienie decydentów, lecz „proaktywnie" poddaje refleksji możliwe kierunki przyszłego rozwoju naukowo-technologicznego, w celu jego **współkształtowania.** Głównym zadaniem TA stało się wspieranie strategicznych decyzji w obszarze innowacji naukowo-technologicznych, w zgodzie z dynamiką rozwoju gospodarczo-społecznego. Ocena technologii przestaje być zatem tylko „systemem wczesnego ostrzegania" przed zagrożeniami związanymi z wykorzystywaniem określonych technologii, który blokuje rozwój technologii (stąd nieprzychylne określanie klasycznego TA w kręgach przemysłu jako *technology arrestment*), a staje się systemem rozpoznawania potencjału i kształtowania trendów rozwoju technologicznego. Jak to ujął jeden z badaczy oceny technologii Ruud Smits „TA przestaje pełnić rolę *watchdoga* (psa stróża), a staje się *trackerdogiem* (psem tropiącym)"[39].

Można wymienić następujące funkcje TA:

- przygotowanie i wspieranie decyzji politycznych dotyczących technologii;
- wczesne ostrzeganie przed ryzykami i zagrożeniami, a także wczesne rozpoznawanie szans i potencjału nowych technologii;
- zapobieganie i łagodzenie konfliktów na tle technologicznym (zarówno przy pomocy mediacji między skonfliktowanymi stronami, jak i poprzez kształtowanie określonych rozwiązań technologicznych w taki sposób, by były one akceptowalne społecznie);
- wspieranie społecznych procesów uczenia się wykorzystywania nowych technologii.

Zarysowana ewolucja TA oznacza również zmianę w oczekiwanych efektach TA. Nie musi to być już tylko wiedza prowadząca bezpośrednio do zmian prawnych lub dająca się zaimplementować w procesach politycznych.

Niemieccy badacze skutków innowacji technologicznych Danielle Bütschi i Michael Nentwich[40] zanalizowali różne **oczekiwania i zadania stawiane współcześnie przed oceną technologii – różnią się** one przede wszystkim **stopniem oddziaływania na proces polityczny**. Rola TA w procesie kształtowania polityki technologicznej może uwidocznić się w kilku obszarach[41]:

1. **Działania pozbawione bezpośredniego politycznego oddziaływania na procesy decyzyjne**. Tutaj należy wymienić takie „miękkie" funkcje TA, jak promowanie komunikacji i współpracy między nauką i opinią publiczną, stymulowanie debaty publicznej w sprawach nauki i techniki, kształtowanie świadomości społecznej w zakresie nowych technologii, zwiększanie zainteresowania i uczestnictwa obywateli w dyskusjach dotyczących rozwoju technologicznego. Ten wymiar funkcjonowania TA znacznie odbiega od pierwotnych, klasycznych celów stawianych przed oceną technologii, rozumianą jako doradztwo polityczne realizowane przez ekspertów na rzecz decydentów. Tutaj wyraźnie uwidacznia się zwrot w stronę opinii publicznej i jej udziału (nawet jeśli nie bezpośredniego) w wypracowywaniu polityk względem nowych technologii.
2. **Ustalanie hierarchii problemów *(agenda setting)* i wprowadzanie do niej nowych zagadnień**. Również w tym przypadku widać rolę TA we wzmacnianiu „strony społecznej" i jej głosu w dyskusji nad rozwojem technologicznym. Funkcja ustanawiania agendy pozwala już nie tylko na dokonywanie analizy tematów podejmowanych przez instytucje państwowe, ale także na wskazywanie, co powinno stać się przedmiotem zainteresowania tych instytucji.
3. **Określanie celów rozwojowo-strategicznych**. Ocena technologii jest tutaj rozumiana jako przestrzeń do dialogu i rozpoznawania różnych możliwych ścieżek rozwoju technologii w oparciu o określone wartości, cele i interesy, których realizację umożliwiają. Taka dyskusja pozwala na sformułowanie

alternatywnych scenariuszy przyszłości i określenie preferencji dla każdej z nich przez różnych aktorów społecznych.

4. **Wybór rozwiązań.** Po sformułowaniu (niekoniecznie w trybie TA) możliwych wariantów działań politycznych, ocena technologii może pomóc w wyborze najbardziej pożądanej spośród dostępnych alternatyw.
5. Przełamywanie impasu przy silnych protestach społecznych, **zarządzanie konfliktami społecznymi na tle technologicznym**.
6. **Implementacja i ewaluacja innowacji technologicznych**. Tutaj w grę wchodzi pełnienie przez TA funkcji związanych z kontrolą i monitoringiem procesu implementacji danej technologii.

Rodzaje instytucji oceny technologii

W państwach europejskich ocena technologii prowadzona jest głównie przy parlamentach (wyjątek stanowią jednostki ulokowane przy akademiach nauk, jak np. w Czechach). **Parlamentarna ocena technologii** przybiera zazwyczaj jedną z trzech form:

1. **Jednostki parlamentu** (komisji, biura, komórki badawczej), ze względu na swą formułę ściśle powiązanej z pracami parlamentu. Takie rozwiązanie można znaleźć w Grecji, Francji, Finlandii i we Włoszech. Na przykład we Francji taką instytucją jest Parlamentarne Biuro ds. Oceny Nauki i Technologii (OPECST, *L'Office Parlementaire d'Évaluation des Choix Scientifiques et Technologiques*), w którego skład wchodzi 18 członków Zgromadzenia Narodowego oraz 18 senatorów. Z kolei w Finlandii instytucją zajmującą się oceną społecznych skutków rozwoju technologii jest jedna z komisji parlamentu – Komisja ds. Przyszłości, utworzona w 1993 r., od 2000 r. mająca status komisji stałej i składająca się z 17 członków reprezentujących wszystkie partie obecne w parlamencie. Głównym celem działania takiej jednostki jest wspieranie decydentów w prowadzeniu polityki w obszarze naukowo-technologicznym; funkcje „zewnętrzne" – takie jak np. dialog ze społeczeństwem – mają charakter poboczny. Zaletą takiego rozwiązania jest aktywne i stałe zaangażowanie parlamentarzystów w działalność instytucji TA, co pozwala zapewnić lepsze dostosowanie analiz do potrzeb i oczekiwań odbiorców. Jednostki przyparlamentarne cechują się relatywnie niewielkim składem osobowym (opierają się na zlecaniu większości prac zewnętrznym zespołom eksperckim) i prostą strukturą organizacyjną (bez zarządu, rad programowych itp.).
2. Kolejna formuła działania to **biuro oceny technologii,** któremu parlament zleca wykonywanie prac z zakresu TA. Biuro może być częścią struktur parlamentu (tak jest w Wielkiej Brytanii, Szwecji, Katalonii i Parlamencie Europejskim), jak również działać na zasadach kontraktu z parlamentem (Niemcy). W Wielkiej Brytanii taką instytucją jest utworzony w 1989 r. POST

(*Parliamentary Office of Science and Technology*). Podobną rolę w Parlamencie Europejskim odgrywa biuro STOA (*Scientific and Technological Options Assessment*), nadzorowane przez panel składający się z europarlamentarzystów i będące obecnie jednostką organizacyjną EPRS (*European Parliament Reseach Service*). W Niemczech tą instytucją jest powołane do życia w 1990 r. TAB (*Büro für Technikfolgenabschätzung*), które co pięć lat wyłania w konkursie zewnętrznego wykonawcę praz z zakresu TA. Od początku tę funkcję pełni jedna instytucja: *Institut für Technikfolgenabschätzung und Systemanalyse* (ITAS) z Karlsruhe. Budżet TAB wynosi 2 miliony euro rocznie. Biura oceny technologii, choć wciąż funkcjonują bezpośrednio przy parlamentach i pełnią podobną funkcję jak parlamentarne jednostki TA, charakteryzują się pewną autonomią: zatrudniają na stałych etatach również ekspertów, którzy w pewnym sensie „równoważą" polityczny charakter tych instytucji. Istnienie zarządów i/lub rad naukowych pozwala na ustalanie planów pracy w odniesieniu do zapotrzebowania zgłaszanego przez parlament, ale nieograniczonych do niego. O ile jednostki parlamentarne realizują prace zlecone przez parlamentarzystów, to biura oceny technologii prowadzą też własne działania badawcze według ustalanych wcześniej priorytetów.

3. Ostatni typ instytucji składających się na parlamentarną ocenę technologii to **niezależny instytut**, dla którego parlament pozostaje głównym odbiorcą i zleceniodawcą prac z zakresu TA. Wykraczają one w swej działalności poza doradztwo polityczne i aktywnie uczestniczą w dyskursie publicznym poświęconym rozwojowi nauki i technologii. Model ten występuje w takich krajach jak Dania, Holandia, Norwegia, Szwajcaria i Flandria. Przykładem tego rodzaju instytucji są: w Danii – *Danish Board of Technology Foundation* (*Teknologirådet*), w Holandii – *Rathenau Instituut*, w Szwajcarii – *Center for Technology Assessment* (TA-SWISS), w Norwegii – *Norwegian Board of Technology* (*Teknologirådet*). Takie instytuty charakteryzują się większą autonomią, a co za tym idzie swobodą w wyborze tematów, ale także większym dystansem wobec polityków i decydentów, co często utrudnia dotarcie z rezultatami prac do tych środowisk. Stąd też bardziej niż poprzednie rodzaje instytucji TA pełnią one funkcje wykraczające poza dostarczanie wiedzy decydentom: swoją rolę postrzegają w stymulowaniu debat publicznych, kształtowaniu świadomości społecznej i postaw w odniesieniu do nowych rodzajów technologii, wypracowywaniu ocen przy udziale interesariuszy i opinii publicznej.

Procedura i metody oceny technologii

Zróżnicowane style uprawiania TA oraz różnorodność form instytucjonalnych zaowocowały również szerokim repertuarem metod i procedur badawczych wykorzystywanych przy analizie zjawisk technologicznych. W pewnym uproszczeniu

można powiedzieć, że rozpościerają się one na osi klasyczna (ekspercka)–partycypacyjna ocena technologii. Ta pierwsza typowa jest dla wczesnego etapu rozwoju TA oraz przyparlamentarnych jednostek TA, ukierunkowanych głównie na dostarczanie eksperckiej, naukowej wiedzy decydentom. Z kolei partycypacyjna TA, włączająca w procesy oceny technologii interesariuszy i opinię publiczną, pojawiła się w Europie na przełomie lat 80-tych i 90-tych za sprawą zewnętrznych instytucji oceny technologii. Nastąpiło to w wyniku ich doświadczeń ze współpracą z szerokimi kręgami społeczeństwa zaangażowanymi w debatę o rozwoju technologicznym. Oczywiście ten podział nie jest bezwyjątkowy: zarówno w działaniach zewnętrznych instytucji TA eksperci mają istotną rolę do odegrania, jak również jednostki parlamentarne prowadzą działania dialogowe, wychodzące ku społeczeństwu, takie jak warsztaty, seminaria, wysłuchania publiczne. Dlatego też błędem byłoby proste utożsamianie podejścia eksperckiego z konkretną formą organizacji instytucji TA czy też tym bardziej z minioną już pierwszą fazą jej rozwoju. Bardziej adekwatna wydaje się być klasyfikacja różnych rodzajów oceny technologii pod kątem udziału zewnętrznych interesariuszy i opinii publicznej ze względu na charakter analizowanych problemów. Zaproponował ją holenderski badacz Wiebe E. Bijker[42]. Wyróżnił on trzy typy TA:

1. Pierwszy z nich to właśnie **klasyczna TA**, w którą włączeni są jedynie badacze i eksperci, a jej efektem ma być neutralny, odnoszący się do faktów raport stanowiący wkład w proces podejmowania decyzji. To podejście ma zastosowanie w sytuacji, gdy skutki danej technologii są rozpoznane i zidentyfikowane oraz panuje zgoda co do ich występowania – jak np. w przypadku azbestu czy radioaktywności.
2. Drugie podejście wykracza poza model klasyczny i opiera się na włączaniu wybranych przedstawicieli zewnętrznych interesariuszy i ich ekspertów. To podejście, które nazywane jest **oceną z udziałem interesariuszy**, zasadne jest wówczas, gdy konsekwencje stosowania przedmiotowej technologii nie są jasno określone i konieczne jest znalezienie równowagi między szansami i zagrożeniami generowanymi przez nową technologię w różnych wymiarach życia społecznego (przykładem może być rozwój nanotechnologii).
3. Trzeci typ TA, czyli **publiczną ocenę technologii**, stosuje się w przypadku istnienia znacznych różnic w ocenie technologii, gdy brakuje społecznego konsensu odnośnie do pożądanego kierunku rozwoju i gotowości do zaakceptowania pewnych rodzajów ryzyka. Jest to model szerokiej partycypacji publicznej, stosowany przy szczególnie kontrowersyjnych zagadnieniach, dotyczących ogółu społeczeństwa. Oprócz ekspertów i przedstawicieli interesariuszy uczestniczą w nim „zwykli" obywatele, by poprzez debatę publiczną wypracować spójne rozwiązanie w takich kwestiach jak np. polityka energetyczna, walka ze zmianami klimatycznymi czy bardziej wybiegające w przyszłość – neurobiologia i zastosowanie

technologii do zwiększania możliwości ludzkiego mózgu (*human enhancement*)[43].

4. We wszystkich trzech perspektywach wykorzystywane jest podejście naukowe, różnica dotyczy stopnia wykorzystania rozwiązań partycypacyjnych. Błędem byłoby jednak utożsamianie metod naukowych wyłącznie z klasyczną TA, zaś partycypacyjnych z optyką publiczną. W tej ostatniej również korzysta się z wiedzy i procedur nauki, które jednak uzupełniane są o społeczną ocenę dostarczaną przez uczestniczących w badaniu przedstawicieli różnych grup i środowisk społecznych[44]. Metody naukowe, wykorzystywane w ocenie technologii, to: wywiad ekspercki, dyskusja ekspercka, modelowanie, symulacja, analiza systemowa, analiza ryzyka, ekstrapolacja trendów, metoda delficka, techniki scenariuszowe, analiza dyskursu, analiza drzewa wartości itp.[45]
5. Z kolei podejście partycypacyjne oparte jest na procedurze dialogu publicznego, umożliwiającego włączenie w analizę nowych technologii wiedzy (zwłaszcza tej nie-eksperckiej), doświadczeń, perspektyw, wartości i interesów różnych interesariuszy. Odchodzimy tu zatem od analizy wyłącznie w kategoriach obiektywnych, naukowych „faktów" w stronę szerokiej refleksji społecznej, uwzględniającej różne preferowane i realizowane style życia odnoszące się do różnych horyzontów światopoglądowych. Do metod ułatwiających włączanie nie-ekspertów w dialog o nowych technologiach należą konferencje konsensualne (stworzone i wykorzystywane głównie przez *Danish Board of Technology*), wysłuchania publiczne, grupy fokusowe, panele obywatelskie, warsztaty scenariuszowe, komórki planowania[46].
6. Stopniowe wychodzenie procedury TA poza wąskie, eksperckie podejście związane było z opisanym wcześniej poszerzaniem obszaru tematycznego: od oceny poszczególnych technologii i ich (możliwych) oddziaływań na otoczenie po nastawioną na przyszłość strategiczną analizę i współkształtowanie trendów cywilizacyjnych. Tak szeroko zakrojony obszar działań z zakresu TA wymagał wyjścia poza instytucje naukowe i zintegrowania prowadzonego namysłu z debatą publiczną. Ta zmiana znalazła swoje odzwierciedlenie w kształcie polityki naukowej Unii Europejskiej. Za przykłady mogą posłużyć przygotowane na zlecenie KE raporty i opracowania, takie jak *Science Technology and Governance in Europe: Challenges of Public Engagement*[47], *From Science and Society to Science in Society*[48] czy *Science and Governance. Taking European Knowledge Society Seriously*[49]. Wszystkie one postulowały silniejsze włączenie w namysł nad rozwojem technologicznym zainteresowanych grup społecznych, zgodnie z modelem „współzarządzania technologią" (ang. *technology governance)*[50].
7. Zmiana w relacjach między nauką, technologią i społeczeństwem daje się zaobserwować także w wytycznych i priorytetach unijnych Programów

Ramowych, czego wyrazem jest ewolucja nazw kolejnych obszarów tematycznych. W ramach 6 Programu Ramowego obszar tematyczny dotyczący relacji między nauką a społeczeństwem nosił nazwę „Nauka i społeczeństwo", by w 7 Programie Ramowym zostać zastąpionym przez „Naukę w społeczeństwie", a w aktualnym, Horyzoncie 2020 przez „Naukę z udziałem społeczeństwa i dla społeczeństwa". Pokazuje to dość dobrze przechodzenie od postrzegania nauki i społeczeństwa jako względnie odrębnych sfer (6 PR: „Nauka i społeczeństwo" jako dwa odrębne obszary), przez dostrzeżenie społecznego umiejscowienia nauki (7 PR: „Nauka w społeczeństwie"), aż po zwrócenie się ku udziałowi społeczeństwa w tworzeniu nauki i społecznym powinnościom i zobowiązaniom tej instytucji.

8. Obecnie jednym z naczelnych postulatów wyznaczających charakter namysłu nad rozwojem technologicznym jest „odpowiedzialne prowadzenie badań i innowacji" (*Responsible Research and Innovation, RRI*), obecne chociażby w programie badawczym Horyzont 2020. Zdobyło sobie ono sporą popularność w ciągu ostatnich kilku lat, owocując licznymi publikacjami oraz projektami badawczymi. RRI definiowane jest jako „transparentny, interaktywny proces, w którym aktorzy społeczni i innowatorzy stają się wzajemnie odpowiedzialni przed sobą pod względem (etycznej) akceptowalności, przestrzegania zasad zrównoważonego rozwoju i dopasowania procesu innowacyjnego oraz jego produktów do społecznych potrzeb w celu właściwego wdrożenia osiągnięć nauki i technologii w społeczeństwie"[51].

Stan obecny

Bez wątpienia w Polsce istnieje **luka w zakresie efektywnego systemu oceny technologii**. Istnienie tej luki generuje określone negatywne konsekwencje dla rozwoju państwa, wynikające zarówno z warunków zewnętrznych, w jakich funkcjonuje nasz kraj, jak i realizowanych przezeń działań. Do tych pierwszych należy zaliczyć oddziaływanie powstających poza granicami Polski (a przez to pozostającymi w dużym stopniu poza możliwościami skutecznego wpływania na ich kształt) innowacji naukowo-technologicznych, takich jak przechwytywanie głównych strumieni komunikacji, automatyzacja i robotyzacja procesów komunikacji społecznej (vide Facebook i Google), rozwój sztucznej inteligencji, Internet Rzeczy, *human enhancement,* wdrażanie ustaleń neuronauk wspieranych przez biotechnologię, informatykę i nanotechnologię (NBIC). Z drugiej strony państwo polskie podejmuje szereg działań i decyzji dotyczących sfery technologicznej: np. w obszarze energetyki (poszukiwanie gazu łupkowego, budowa elektrowni atomowych, utrzymywanie sektora węglowego), polityki klimatycznej, cyfryzacji (np. projekt elektronicznego dowodu osobistego), zarządzania dużymi zbiorami danych typu *Big Data* (np. integracja systemów PESEL i ZUS).

Ta sytuacja wskazuje na **potrzebę instytucjonalizacji oceny technologii, jako części strategicznych procesów decyzyjnych**. Pozwoliłoby to w systematyczny i oparty na wiedzy sposób identyfikować, rozpatrywać i dokonywać wyboru odpowiednich opcji rozwojowych, minimalizując w ten sposób niepewność i arbitralność podejmowanych wyborów. Ponadto, instytucjonalizacja TA umożliwiłaby poddanie w pewnym stopniu kontroli i monitoringowi głównych kierunków rozwoju technologicznego w celu lepszego dopasowania go do przyjętych kierunków rozwoju społecznego. Po trzecie wreszcie, ocena technologii istniejąca w formie odpowiedniej instytucji ogranicza nieformalne, quasi-lobbystyczne wpływy grup interesu powiązanych z określonymi opcjami technologicznymi, które oddziałują obecnie na proces stanowienia prawa kanałami nieformalnymi bądź pod postacią „niezależnych ekspertów", pełniących funkcje doradców przy procesach podejmowania decyzji.

Potencjał dla instytucjonalizacji TA. Kluczowym elementem każdego systemu oceny technologii jest zaplecze badawcze: sprawne instytucje, będące w stanie dostarczyć użytecznej wiedzy na potrzeby podejmowania decyzji oraz stymulowania debaty publicznej oraz kadra badawcza dysponująca zarówno wąskimi, specjalistycznymi kompetencjami eksperckimi, jak i doświadczeniem w interdyscyplinarnej, wieloaspektowej analizie społecznych aspektów rozwoju naukowo technologicznego.

W Polsce ocena technologii rozwijała się do tej pory głównie na poziomie teoretycznym i popularyzatorskim. Pierwsze prace z tego zakresu, próbujące przeszczepić na polski grunt podejście *technology assessment* pochodzą z lat 70. Ich autorem jest Lech W. Zacher, dziś profesor Akademii Leona Koźmińskiego, który od lat promuje idee poddawania systematycznemu namysłowi kierunków rozwoju naukowo-technologicznego i przewidywania jego konsekwencji. Z lat dwutysięcznych pochodzą prace m.in. Andrzeja Kiepasa z Uniwersytetu Śląskiego. W 2015 roku powstało Polskie Towarzystwo Oceny Technologii, skupiające badaczy z różnych dyscyplin – zarówno społecznych, humanistycznych, jak i przyrodoznawczych; jednak do tej pory jego działalność jest znikoma i ogranicza się do wewnątrzśrodowiskowych aktywności.

Jedyną instytucją publiczną pełniącą zbliżone funkcje do oceny technologii jest Biuro Analiz Sejmowych, będące członkiem stowarzyszonym Europejskiej Sieci Parlamentarnej Oceny Technologii EPTA i uczestniczące w niedawno zakończonym projekcie europejskim PACITA (*Parliaments and Civil Society in Technology Assessment*), którego zadaniem było wzmacnianie roli parlamentarnej oceny technologii w krajach uczestniczących w projekcie. Nakładem Biura Analiz Sejmowych ukazał się również numer tematyczny czasopisma Studia BAS, pod tytułem *Technology Assessment. Problematyka oceny technologii*[52].

Kondycja polskiej nauki pozwala zakładać, że możliwe jest stworzenie w przeciągu kilku lat sieci profesjonalnych ośrodków analitycznych, będącej w stanie dostarczać

analiz na potrzeby procedury TA. Potencjał w obszarze klasycznych, eksperckich analiz technologii bezsprzecznie istnieje na wyższych uczelniach technicznych i w państwowych instytutach badawczych. Również społeczne badania nad rozwojem naukowo-technologicznym rozwijają się w Polsce w ostatnich latach, choć jak na razie jedynie rzadko wychodzą poza refleksję teoretyczną lub rekapitulację namysłu prowadzonego w innych krajach.

Istnieje również podglebie instytucjonalne w obszarze prowadzonych przez agencje wspierające badania naukowe programów badawczych. Już sam Krajowy Program Badań podkreśla znaczenie interdyscyplinarnych badań, wykorzystujących nauki społeczne i humanistyczne w tworzeniu innowacji pozwalających domknąć lukę cywilizacyjną między Polską a Europą Zachodnią. Dostrzeżenie roli nauk społecznych i humanistycznych w tym procesie można potraktować jako potencjalny punkt wyjścia dla analiz z zakresu szeroko zakrojonej oceny technologii. Z kolei w założeniach do jednego ze strategicznych programów badawczych, opartych na wytycznych KPB, o nazwie „Gospostrateg: Społeczny i gospodarczy rozwój Polski w warunkach globalizujących się rynków", znalazły się wytyczne dotyczące wspierania tworzenia „modeli umożliwiających przewidywanie skutków, wykorzystania szans i zapobieganie ryzykom wynikających z rozwoju technologicznego na szczeblu makroekonomicznym, jak też na szczeblach regionalnych i lokalnych w Polsce oraz doskonalenia metod ewaluacji wpływu nowych technologii na polityki publiczne"[53].

Stan pożądany i rekomendacje

Spośród omówionych wcześniej rozwiązań instytucjonalnych najbardziej właściwą wydaje się być forma hybrydowa: **połączenie pracy biura oceny technologii, istniejącego przy parlamencie lub władzy wykonawczej, z zewnętrznymi, niezależnymi instytucjami**.

Jak podkreślają Enzing i in., jednostki parlamentu i biura oceny technologii korzystają ze swobodnego dostępu do parlamentarzystów i realizują przede wszystkim funkcję informacyjną wobec decydentów[54]; z kolei niezależne instytuty TA mogą w większym stopniu wykraczać poza zlecany im zakres tematyczny, by wspólnie z przedstawicielami otoczenia społeczno-gospodarczego identyfikować wymagające analizy tematy, poddawać je ocenie i w ten sposób wpływać na agendę polityczną.

Odnosząc te odmienne sposoby funkcjonowania instytucji TA do często używanej typologii efektów oceny technologii o nazwie TAMI[55], można zauważyć istotne różnice w rodzajach konsekwencji działań poszczególnych typów instytucji TA. Decker i Ladikas wyszczególniają trzy typy efektów, do których może prowadzić ocena technologii:

- zwiększanie wiedzy,
- kształtowanie opinii i postaw,
- inicjowanie działań.

Instytucje TA typu pierwszego i drugiego (jednostki parlamentarne i biura oceny technologii) wypracowują – jak wynika z ich analizy przeprowadzonej przez Deckera i Ladikasa – głównie pierwszy rodzaj efektów, tj. zwiększanie wiedzy decydentów. Działając przede wszystkim na zamówienie wychodzące od parlamentarzystów, mają oni ograniczone możliwości inicjowania działań,w znaczeniu sygnalizowania nowych obszarów problemowych i wyboru tematów do analizy. To z kolei możliwe jest właśnie – jak o tym była wcześniej mowa – przez zewnętrzne instytucje TA.

Czysto przyparlamentarne sposoby organizacji oceny technologii – przy wszystkich swoich zaletach – wydają się być zatem niewystarczające: ze względu na swój „reaktywny" charakter, grozi im pozostawanie zawsze krok z tyłu za bieżącymi trendami rozwojowymi. Ograniczenie się do dostarczania wiedzy nie pozwala im na aktywne uczestnictwo w procesach powstawania i kształtowania innowacji, tak jak mogą to czynić podmioty zewnętrzne. Te zaś, pozostając o oddaleniu od instytucji politycznych, mogą korzystać z bliższych relacji z podmiotami przemysłowymi, technologicznymi, a także reprezentującymi społeczeństwo obywatelskie. To daje im większą elastyczność, pozwalając na sprawniejsze rozpoznawanie nowych trendów i sygnalizowanie obszarów zjawisk wymagających namysłu i refleksji.

Należy jednak pamiętać, że bliska współpraca z decydentami jest podstawowym warunkiem prowadzenia oceny technologii i konieczna jest począwszy od pierwszych etapów działań (tj. identyfikacji i formułowania problemów, dyskutowania możliwych rozwiązań itd.). Sytuacja, w której decydenci są jedynie finalnymi odbiorcami powstających na zewnętrz produktów TA grozi niedopasowaniem prac do potrzeb decydentów, zarówno co do treści, jak i formy.

Połączenie formuły biura oceny technologii (które może działać zarówno przy parlamencie, jak i rządzie) z działalnością zewnętrznych ośrodków badawczych, dedykowanych do wykonywania różnego rodzaju prac badawczych w obszarze TA, pozwoliłoby na wykorzystanie zalet jednego i drugiego rozwiązania: bliskości decydentów z elastycznością i niezależnością działania.

Rekomendacje

Stworzenie instytucji oceny technologii w Polsce musi być z konieczności procesem wieloetapowym. Powinny na niego składać się takie działania, jak:

- wprowadzenie wymogu uwzględniania interdyscyplinarnej oceny technologii w programach rozwojowych i wdrożeniowych finansowanych ze środków publicznych. Pozwoliłoby to z jednej strony na nabranie doświadczenia w realizacji TA przez polskich badaczy, a z drugiej ugruntowało pozycję TA jako nieodłącznego elementu polityki innowacyjnej;
- wspieranie rozwoju *know-how* w zakresie oceny technologii poprzez interdyscyplinarne programy badawcze nakierowane na realizację badań nad rozwojem naukowo-technologicznym w paradygmacie TA;

- wyselekcjonowanie potencjalnych partnerów (ośrodków i osób), którzy mogliby być zainteresowani tworzeniem w przyszłości instytucji TA w Polsce i zainicjowanie konsolidacji środowiska oceny technologii w Polsce;
- czerpanie z doświadczeń innych krajów poprzez udział w programach studyjnych, wymianach badaczy, zatrudnianie w polskich instytucjach naukowych badaczy z doświadczeniem w TA itp.;
- wypracowanie różnorodnych, interaktywnych kanałów stałej komunikacji między środowiskiem badaczy z obszaru TA i decydentów (wspólnie organizowane seminaria, dyskusje, stały przepływ informacji);
- wykorzystywanie realizowanych reform w obszarze organizacji nauki i polityki naukowo-technologicznej do wprowadzania procedury TA – dla przykładu, zapowiadane przez Ministerstwo Nauki i Szkolnictwa Wyższego powołanie Narodowego Instytutu Technologicznego w miejsce dotychczasowych państwowych instytutów badawczych powinno uwzględniać stworzenie w nim interdyscyplinarnej komórki oceny technologii[56].

W oparciu o realizację powyższych kroków w perspektywie kilku lat możliwe powinno stać się powołanie sprawnie funkcjonujących instytucji oceny technologii, składających się z biura oceny technologii, koordynującego prace współpracujących z nim ośrodków analitycznych, umieszczonych w różnych obszarach problemowych **[11]**.

Przypisy

[1] Wybrane źródła informacji:
Informacja dostarczona przez Cambridge Analytica, *Cambridge Analytica The Data Gurus Who Anticipated the Election Result*, „PR Newswire" 11 listopada 2016. Dostępne na: http://www.prnewswire.com/news-releases/cambridge-analytica-the-data-gurus-who-anticipated-the-election-result-300361599.html); T. Cheshire, *Behind the scenes at Donald Trump's UK digital war room*, „Sky News" 21 października 2016. Dostępne na: http://news.sky.com/story/behind-the-scenes-at-donald-trumps-uk-digital-war-room-10626155 (data odczytu: 29 lutego 2017). M. Krogerus i H. Grassegger, *Ich habe nur gezeigt, dass es die Bombe gibt*, „Das Magazin" 3 grudnia 2016. Dostępne na: https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/ (data odczytu: 29 lutego 2017). A. Turek, *Komputer lepiej oceni charakter niż znajomi. Współautor badań dr Kosiński: Maszyny mogą poznać nas lepiej niż sądzimy*, „INN Poland" styczeń 2015. Dostępne na: http://innpoland.pl/114781,dr-michal-kosinski-maszyny-moga-poznac-nas-lepiej-niz-sadzilismy-powinnismy-sie-cieszyc-ze-korporacje-zbieraja-nasze-dane (data odczytu: 29 lutego 2017). W. Youyou, M. Kosinski, D. Stillwell, *Computer-based personality judgments are more accurate than those made by humans*, „Proceedings of the National Academy of Sciences", 2015. Strona internetowa spółki Cambridge Analytica. Dostępne na: https://cambridgeanalytica.org/ (data odczytu: 29 lutego 2017). Marek Szymaniak, *Polak odkrył polityczną bombę atomową. To koniec demokracji jaką znamy?,* „Magazyn TVN24", 22 stycznia 2017. http://www.tvn24.pl/magazyn-tvn24/polak-odkryl-polityczna-bombe-atomowa-to-koniec-demokracji-jaka-znamy,79,1628 (data odczytu: 29 lutego 2017)

[2] M. Kosiński, , *Internetowy Frankenstein*, rozmawiał J. Żakowski, „Polityka", 3/2017, s. 25-27.

[3] Zob. np. A. Smith, V. Banic, *Fake News: How a Partying Macedonian Teen Earns Thousands Publishing Lies*, 9.12.2016. Dostępne na: http://www.nbcnews.com/news/world/fake-news-how-partying-macedonian-teen-earns-thousands-publishing-lies-n692451 (data odczytu 13.12.2016); C. Silverman, L. Alexander, *How Teens In The Balkans Are Duping Trump Supporters With Fake News*, https://www.buzzfeed.com/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo?utm_term=.unl3DA5vQ7#.kuYKlVzYw3 (data odczytu: 13.12.2016).

[4] M. Mazzetti, E. Lichtblau, *C.I.A. Judgment on Russia Built on Swell of Evidence*, 11.12.2016. Dostępne na: http://www.nytimes.com/2016/12/11/us/politics/cia-judgment-intelligence-russia-hacking-evidence.html (data odczytu: 14.12.2016).

[5] Na temat kaskad informacyjnych zob. S. Bikhchandani, D. Hirshleifer, I. Welch, *A theory of fads, fashion, custom, and cultural change as informational cascades*, „Journal of Political Economy" 1992, Vol. 100; nt. baniek informacyjnych zob. E. Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, 2011; zob. także P. Pomerantzev, *Nothing Is True and Everything Is Possible: The Surreal Heart of the New Russia,* 2014.

[6] Przykładowo: J. Darczewska, *Anatomia rosyjskiej wojny informacyjnej: Operacja krymska – studium przypadku*, „Punkt widzenia" nr 42, Ośrodek Studiów Wschodnich, Warszawa 2014. Dostępne na: https://www.osw.waw.pl/sites/default/files/anatomia_rosyjskiej_wojny_informacyjnej.pdf (data odczytu: 31 grudnia 2016); J. Darczewska, *Diabeł tkwi w szczegółach: wojna informacyjna w świetle doktryny wojennej Rosji*, „Punkt widzenia" nr 50, Ośrodek Studiów Wschodnich, Warszawa 2015. Dostępne na: https://www.osw.waw.pl/pl/publikacje/punkt-widzenia/2015-05-19/diabel-tkwi-w-szczegolach-wojna-informacyjna-w-swietle-doktryny (data odczytu: 31 grudnia 2016); J. Darczewska, *Wojna informacyjna Rosji z Zachodem. Nowe wyzwanie?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015 (Wojna hybrydowa – wydanie specjalne), s. 59-73. Dostępne na: http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-4/1213,Przeglad-Bezpieczenstwa-Wewnetrznego-WYDANIE-SPECJALNE.html (data odczytu: 31 grudnia 2016); K. Giles, *Handbook of Russian Information Warfare*, Rome: NATO Defense College

„NDC Fellowship Monograph Series", Fellowship Monograph 9, 2016. Dostępne na: http://www.ndc.nato.int/news/news.php?icode=995 (data odczytu: 31 grudnia 2016); C. Paul, M. Matthews, *The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It*, RAND Corporation, Santa Monica, CA 2016. Dostępne na: http://www.rand.org/pubs/perspectives/PE198.html (data odczytu: 31 grudnia 2016); M. Wojnowski, *'Zarządzanie refleksyjne' jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 11-36. Dostępne na: http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstwa-3/1180,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-12-7-2015.html (data odczytu: 31 grudnia 2016).

7 W syntetycznym ujęciu Jolanty Darczewskiej, rekonstruującej rosyjskie ujęcia tego fenomenu, wojna informacyjna to „oddziaływanie na masową świadomość w międzypaństwowej rywalizacji systemów cywilizacyjnych w przestrzeni informacyjnej, wykorzystujące szczególne sposoby kontroli nad zasobami informacyjnymi, a używane w charakterze 'broni informacyjnej'", cyt. za J. Darczewska, *Anatomia rosyjskiej*…, s. 12.

8 Tamże, s. 10.

9 C. Paul, M. Matthews, dz. cyt., s. 2.

10 J. Darczewska, *Anatomia rosyjskiej…*, s. 5.

11 C. Paul, M. Matthews, dz. cyt., s. 5.

12 J. Darczewska, *Anatomia rosyjskiej…*, s. 5.

13 C. Paul, M. Matthews, dz. cyt., s. 7.

14 Tamże, s. 8.

15 K. Giles, dz. cyt., s. 54-56.

16 Atak DDoS (*distributed denial of service*) to atak przeprowadzany równocześnie z wielu komputerów na dany komputer (w praktyce najczęściej system komputerowy albo usługę sieciową danej instytucji). Celem ataku jest paraliż funkcjonalności systemu poprzez zablokowanie wolnych zasobów. Często taki atak jest przeprowadzany za pomocą komputerów, nad którymi bez wiedzy ich użytkowników przejęto kontrolę (przy użyciu specjalnego oprogramowania). Komputery uczestniczące w ataku jednocześnie zaczynają kontaktować się z atakowanym systemem, wywołując go, próbując skorzystać z danych usług etc. Atakowany system musi wykorzystać część swoich zasobów do kontaktu z łączącym się komputerem, co przy olbrzymiej liczbie żądań może doprowadzić do wyczerpania dostępnych zasobów i braku funkcjonalności systemu.

17 K. Giles, dz. cyt., s. 13.

18 Tamże, s. 51.

19 *Infrastruktura krytyczna,* Rządowe Centrum Bezpieczeństwa, brak daty opublikowania strony. Dostępne na: http://rcb.gov.pl/infrastruktura-krytyczna (data odczytu: 31 grudnia 2016).

20 Termin ukuty w 1996 roku przez Carlo Koppa

21 S. Watling, *Digital exclusion: coming out from behind closed doors*, „Disability & Society" nr 4(26), 2011.

22 Dostępne na: http://www.umic.pt/images/stories/publicacoes/kaplan_report_einclusion _final_version.pdf (data odczytu: 29 lutego 2017).

23 Zob. T. Szubrycht i T. Szymański, *Broń elektromagnetyczna jako nowy środek walki w erze informacyjnej*, „Zeszyty Naukowe Akademii Marynarki Wojennej" nr 46, 2005, s. 122.

24 G. Tsurutani i W. D. Lakhina, G. S. Alex, *The extreme magnetic storm of 1–2 September 1859*, „Journal of Geophysical Research: Space Physics" nr 108(A7), 2003.

25 N. Chopra i E. V. K. Kamboj, *E-Bomb*, „International Journal of All Research Education and Scientific Methods" nr 1(1), 2013.

26 C.N. Ghosh, *EMP weapons*, „Strategic Analysis" Vol. 24 , Iss. 7, 2000, s. 1333.

27 Dostępne na: http://www.cbsnews.com/news/us-drops-e-bomb-on-iraqi-tv/ (data odczytu: 29 lutego 2017).

[28] J.F. Kołodziejski i I. Kubiak, J. Łysko, *Narażenia sprzętu elektronicznego promieniowaniem elektromagnetycznym–sposoby generacji i metody ochrony*, „Przegląd Elektrotechniczny" nr 91(11), 2015, s. 38.

[29] C.N Ghosh, *EMP weapons…, s.* 1333.

[30] U.S. Department of Homeland Security, *Planning Guidance for a Response to a Nuclear Detonation*, 2010, s. 36. Dostępne na: https://www.fema.gov/media-library/assets/documents/24879 (data odczytu: 29 lutego 2017).

[31] J. Sobiech i J. Kieliszek, *Czy broń elektromagnetyczna zagraża zdrowiu człowieka?*, „Przegląd Elektrotechniczny" nr 85, 2009.

[32] R. Kubacki i M. Wnuk, *Oddziaływanie biofizyczne wysokomocowych impulsów broni elektromagnetycznej*, „Przegląd Elektrotechniczny" nr 89, 2013.

[33] J.F. Kołodziejski i Kubiak I., Łysko J., *Narażenia sprzętu…*

[34] NCBIR, Projekt budowy zabezpieczeń infrastruktury krytycznej w zakresie przetwarzania, magazynowania i przesyłu danych odpornego na działanie wysoko energetycznego promieniowania elektromagnetycznego, 2013. Dostępne na: http://www.ncbr.gov.pl/gfx/ncbir/userfiles/_public/obronnosc/4_2013/temat_nr_16.pdf (data odczytu: 29 lutego 2017).

[35] Dostępne na: http://www.ausairpower.net/E-Bomb-FAQ.html (data odczytu: 29 lutego 2017).

[36] K. Bechta, *Broń elektromagnetyczna–istota działania i znaczenie broni przyszłości*, „Spektrum", nr 5-6, 2011.

[37] Dostępne na: http://www.livescience.com/53586-raptors-disable-dutch-drones.html (data odczytu: 29 lutego 2017).

[38] Dostępne na: http://www.dailymail.co.uk/news/article-2402403/Drug-dealing-gang-used-carrier-pigeons-distribute-cannabis-Argentina-arrested.html (data odczytu: 29 lutego 2017).

[39] A. Grunwald, 2002, *Technikfolgenabschätzung: eine Einführung*, Berlin: 60.

[40] D., Bütchi, M. Nentwich, 2000, *The Role of PTA In the Policy-Making process*, [w:] L. Klüver, M. Nentwich, W. Peissl, H. Torgersen, F. Gloede, L. Hennen, J. van Eijndhoven, R. van Est, S, Joss, S. Bellucci, D. Butchi, (red). *EUROPTA. European Participatory Technology Assessment. Participatory Methods in Technology Assessment and Technology Decision-Making*, Copenhagen.

[41] Tamże: 137-139.

[42] W.E. Bijker, 2014, *Technology Assessment: The State of Play. Towards a Hybrid and Pluriform Process of Governance of Science and Technology.* [w:] T. Michalek i in. (red). *Technology Assessment and Policy Areas of Great Transitions,* Praga.

[43] L. Klüver, M. Nentwich, W. Peissl, H. Torgersen, F. Gloede, L. Hennen, J. van Eijndhoven, R. van Est, S, Joss, S. Bellucci, D. Butchi, (red). *EUROPTA. European Participatory Technology Assessment. Participatory Methods in Technology Assessment and Technology Decision-Making*, Copenhagen. Por. A. Zybertowicz, M. Gurtowski, K. Tamborska, M. Trawiński, J. Waszewski, 2015, *Samobójstwo oświecenia? Jak neuronauka i nowe technologie pustoszą ludzki świat*, Kraków.

[44] Więcej na temat różnic między klasyczną a partycypacyjną oceną technologii można znaleźć w: P. Stankiewicz, 2015a. *Klasyczna i partycypacyjna ocena technologii*. „Studia BAS", vol. 43, no. 3.

[45] C. Enzing, J. Deuten, M. Rijnders-Nagle, J. van Til, 2012, *Technology across Borders. Exploring perspectives for pan-European Parliamentary Technology Assessment*, Brussels.

[46] Inną typologię metod TA proponuje w swoim przeglądowym tekście Krzysztof Michalski, który podzielił je na metody strukturalizujące, prognostyczne, heurystyczne i ewaluacyjne (K. Michalski, 2015, *Przegląd metod i procedur wykorzystywanych w ocenie technologii*. „Studia BAS", vol. 43, no. 3). Zob. także Tran, T.A. i Daim, T., 2008, *A taxonomic review of methods and tools applied in technology assessment*, „Technological Forecasting and Social Change", vol. 75, no. 9.

[47] R. Hagendijk, P. Healey, M. Horst i A. Irwin, 2005, *Science, Technology and Governance in Europe: Challenges of Public Engagement*, STAGE Final Report.

[48] A. Stirling, 2006. *From Science and Society to Science in Society: Towards A Framework for „Co-Operative Research",* Report of a European Commission Workshop, Brussels.

[49] U. Felt, B. Wynne, 2007, *Taking European Knowledge Society Seriously*, Brussels.

[50] P. Stankiewicz, 2015b. *Współzarządzanie nauką i technologią.* „INFOS: Zagadnienia Społeczno-Gospodarcze", vol. 200, no. 7.

[51] R. von Schomberg, 2013, *A Vision of Responsible Innovation*. [w:] R. Owen, M. Heintz, i J. Bessant., (red.) *Responsible Innovation*, London.

[52] M. Gwiazdowicz, P. Stankiewicz (red.), 2015, *Technology Assessment. Problematyka oceny technologii*, Warszawa.

[53] Tamże, s. 3.

[54] C. Enzing, J. Deuten, M. Rijnders-Nagle, J. van Til, 2012, *Technology across Borders. Exploring perspectives for pan-European Parliamentary Technology Assessment*, Brussels, s. 15.

[55] M. Ladikas, M. Decker, 2004, *Assessing the Impact of Future-Oriented Technology Assessment*, [w:] *EU-US Seminar: New Technology Foresight, Forecasting & Assessment Methods,* Seville.

[56] *Strategia na rzecz doskonałości naukowej, nowoczesnego szkolnictwa wyższego, partnerstwa z biznesem i społecznej odpowiedzialności nauki,* 2016. Ministerstwo Nauki i Szkolnictwa Wyższego.