RAPORT

FUNDACJI INSTYTUT BEZPIECZEŃSTWA I STRATEGII

# WYZWANIA DLA BEZPIECZEŃSTWA WSPÓŁCZESNEJ POLSKI

INSTYTUT
BEZPIECZEŃSTWA
I STRATEGII

październik 2019

Spis treści

## WSTĘP

Mam wyjątkową przyjemność i zaszczyt zaprezentować pierwsze kompleksowe opracowanie powstałego przed rokiem think tanku Fundacja Instytut Bezpieczeństwa i Strategii, stanowiące zbiór analiz i rekomendacji zmian w wybranych kluczowych dla bezpieczeństwa współczesnej Polski obszarach strategicznego zarządzania państwem.

Celem działania Instytutu jest tworzenie i promowanie optymalnych rozwiązań czyniących Polskę nowoczesną i bezpieczną, zdolną do zapewnienia przyszłym pokoleniom Polaków życia w warunkach stabilnego rozwoju i dobrobytu. Istotą działalności Instytutu jest identyfikowanie problemów o kluczowym znaczeniu dla bezpieczeństwa narodowego i poddawanie ich  wnikliwej analizie. Skupiamy naszą uwagę na problemach o charakterze systemowym i złożonej naturze, które m.in. z tego powodu nie znajdowały dotychczas należytego zainteresowania ze strony władz państwowych i elit politycznych. W oparciu o sformułowane w oparciu o ich gruntowaną analizę wnioski, przygotowujemy propozycje rozwiązań oraz rekomendacje działań, stanowiących wszechstronną odpowiedź na zidentyfikowane problemy.

Niniejszy raport porusza 7 wybranych zagadnień, dla których wspólnym mianownikiem jest znaczący potencjał dla bezpieczeństwa dzisiejszej Polski, a także pozostawanie ich poza zainteresowaniem głównego nurtu debat publicznych, wynikające z niezrozumienia lub niedoceniania ich znaczenia. Intencją twórców raportu jest zwrócenie na nie uwagi decydentów politycznych oraz liderów opinii publicznej, z zamiarem wytworzenia warunków do włączenia ich do głównej agendy politycznej. Liczymy na to, że w perspektywie zaowocuje to wdrożeniem rekomendowanych przez nas zmian.

Pomimo upływu 30 lat od pierwszych częściowo wolnych wyborów do parlamentu RP szereg wyzwań dla bezpieczeństwa Polski pozostaje nadal aktualne, m.in. z uwagi na popełnione w minionych latach błędy i zaniedbania np. w sferze budowy nowoczesnego i skutecznego systemu służb specjalnych czy demokratycznej kontroli nad nimi. Ostatnie lata, m.in. w konsekwencji gwałtownych przeobrażeń technologicznych spowodowanych rewolucją cyfrową, obfitują w liczne nieznane dotąd wyzwania, zmieniające całkowicie strategiczne otoczenie Polski. Stawienie im czoła wymaga gruntownej zmiany modelu zarządzania bezpieczeństwem narodowym, dostosowującej struktury, mechanizmy, formy i metody działania do nowej rzeczywistości. Wypracowane w ciągu minionych 30 lat systemowe rozwiązania uległy w dużej mierze dezaktualizacji i wymagają pilnych modyfikacji. Im szybciej zostaną one wypracowane i wdrożone tym lepiej Polska będzie w stanie sprostać nowym wyzwaniom. Kluczem do przebudowy państwa powinna być świadomość, że nie ma powrotu do przeszłości i stosowanych wówczas rozwiązań. Reguły gry uległy bezpowrotnym zmianom i przyszłość będzie kształtowana  w oparciu o te nowe reguły.

Wartością raportu jest nowatorskie podejście, w jakim prezentowane są zagadnienia, uznane za wyzwania dla bezpieczeństwa współczesnej Polski. Każdy z rozdziałów analizuje istotę omawianego zagadnienia i jego znaczenie dla bezpieczeństwa Polski oraz oferuje konkretne rozwiązania, które w ocenie autorów pozwolą wypracować skuteczną odpowiedź na opisywane zjawiska i rozwiązać związane z nimi problemy. Co szczególnie istotne proponowane rozwiązania odnoszą się nie tylko do zagrożeń ale także szans, jakie ze sobą niosą wyzwania współczesności. Uprzedzając ewentualne pytania należy zauważyć, że wybór obszarów omówionych w raporcie ma charakter autorski i nie stanowi wyczerpującego ani zamkniętego katalogu. Zamierzeniem Instytutu jest kontynuacja studiów nad wyzwaniami dla bezpieczeństwa współczesnej Polski i prezentacja ich rezultatów w kolejnych edycjach raportu.

Prezentowane rekomendacje bazują na najlepszych wzorach i praktykach oferowanych przez współczesną naukę, ale także wypracowanych przez państwa, uznawane za wiodące w dziedzinach doskonalenia swoich systemów bezpieczeństwa narodowego oraz twórców trendów rozwojowych w dziedzinie wykorzystania najnowszych technologii. W wielu aspektach stanowią przełom w podejściu i sposobie myślenia o zagadnieniach, będących przedmiotem analizy. Intencją twórców raportu jest nadanie całkiem nowej perspektywy widzenia omawianych zagadnień i skierowanie uwagi decydentów politycznych i liderów opinii na rozwiązania pozostające często poza ich świadomością, będące jednocześnie fundamentem paradygmatu działania państw uznawanych za wiodące. Liczymy na to, że zaproponowane przez autorów rozwiązania spotkają się z zainteresowaniem odbiorców oraz znajdą praktyczne zastosowanie w praktyce zarządzania bezpieczeństwem narodowym RP.

Grzegorz Małecki
Prezes Zarządu Fundacji
Instytut Bezpieczeństwa i Strategii

**dr. M. Jones**

# Technologia cyfrowa jako kluczowy czynnik niepewności strategicznej

## Wstęp i metodologia[1]

Każda analiza strategicznej niepewności w Polsce i na świecie, która nie zaczyna się od próby zrozumienia wpływu wykorzystywanych technologii na społeczeństwa, kultury oraz profile psychologiczne poszczególnych jednostek, zawsze w sposób chybiony opisze charakter tego zjawiska we współczesnym świecie. W Polsce, tak jak w każdym innym miejscu na świecie, toczy się właśnie rewolucja informatyczna, zaś jej zrozumienie jest niezbędne do prawidłowej analizy strategicznego kontekstu kraju.

Struktura niniejszej pracy nawiązuje do proponowanych przeze mnie Ram Reakcji Strategicznej, obejmujących trzy podstawowe osądy bądź pytania: osąd rzeczywistości (co się dzieje?) osąd wartości (co to znaczy?) i osąd działania (jak powinniśmy reagować?). Pod wieloma względami niniejszy tekst stanowi esej w klasycznym sensie tego słowa – jest testem idei.

## Osąd rzeczywistości – co się dzieje?

Dla każdego, kto choć pobieżnie interesuje się polityką, świat stał się ostatnio naprawdę dziwnym miejscem. Nie chodzi tu tylko o coraz większy zasięg zjawiska zwanego „populizmem" czy załamanie tradycyjnych kategorii lewicy i prawicy. Przy okazji upadło też bardzo wiele założeń, na których kiedyś budowaliśmy swoje wizje przyszłości. Dlaczego tak się stało? Jestem przekonany, że podstawową przyczyną tej transformacji i płynącej w ślad za nią niepewności strategicznej w Polsce i na świecie jest przejście od geopolityki w warunkach analogowych/elektrycznych do geopolityki w warunkach cyfrowych.

Od przedwestfalskiej epoki pisma ręcznego do druku (ok. 1450 r.), który pomógł zbudować porządek westfalski, przez kody przesyłane elektrycznie (ok. 1850 r.), aż do transmisji dźwięku i obrazu (poprzez radio i telewizję), społeczeństwo i geopolityka przechodzą gwałtowne przemiany pod wpływem zmieniających się technologii komunikacyjnych[2]. Dziś nasze środowisko strategiczne znów ulega przeobrażeniom, tym razem za pomocą pamięci przechowywanych cyfrowo. Kiedyś cyfry reprezentowały zjawiska; w elektronicznym świecie je tworzą, a fakt ten niesie ze sobą ogromne reperkusje. Innymi słowy, obecnie technologie cyfrowe kształtują i napędzają niepewność strategiczną na wszystkich płaszczyznach i w przewidywalnej przyszłości będą to robić w coraz szybszym tempie. A zatem technologie te stanowią to, co Arystoteles określał „przyczyną formalną", tj. czynnik kształtujący nasze wybory i strukturę myślenia.
Jak pamiętamy, Arystoteles postulował cztery przyczyny bytu, tj. przyczyny istnienia rzeczy. Na samej górze są „przyczyny finalne" (gr. telos), w sposób dosłowny teleologiczne, definiujące sam cel istnienia rzeczy. Dalej są „przyczyny materialne" (gr. hylé): wypływające z natury materiałów, jak drewna czy żelaza. Po nich następują „przyczyny efektywne" (gr. kinoun), które mają bezpośrednie skutki, jak ruch rozpoczynający lub kończący jakąś akcję; nie kształtują one systemów czy ludzkich wyborów. To właśnie o nich myślimy, gdy używamy terminu „przyczyna i skutek".

„Przyczyny formalne" (gr. eidos lub morphos) są zapewne najtrudniejsze do konceptualizacji[3]. Musimy jednak je pojąć, jeśli chcemy zrozumieć naturę geopolityki w warunkach świata cyfrowego. W przeciwieństwie do przyczyn

---

[1] Praca ta oparta jest w dużej mierze na mojej prelekcji pt." Niepewność strategiczna, technologia cyfrowa i przyczyna formalna" wygłoszonej w Instytucie im. Samuela Neamana w Technion w Izraelu dnia 26 czerwca 2018 r., a także na odczycie wygłoszonym dla FIBiS dnia 6 marca 2019 r. w Warszawie.

[2] zob. Mark Stahlman, The Digital Sphere, Order and Chaos, raport sporządzony dla Biura Oceny Sieci Departamentu Obrony USA, 2016.

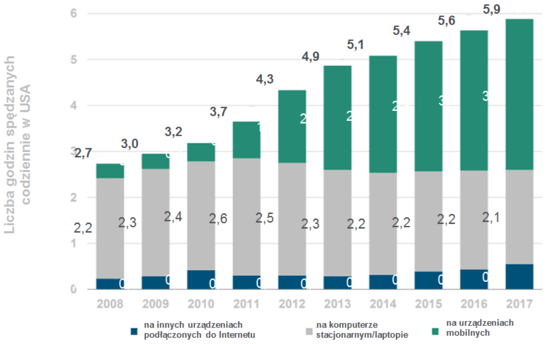
[3] Trudność, z jaką konceptualizujemy przyczyny formalne wynika ni mniej ni więcej jak tylko z „przyczyny formalnej" uruchomionej przez maszynę drukarską.

efektywnych, przyczyny formalne nie mają „skutków” w codziennym rozumieniu tego słowa. Zamiast tego aktywnie tworzą i zmieniają struktury. Dzięki nim z materii lub struktur powstają poszczególne kategorie rzeczy. Innymi słowy, „przyczyny formalne są przyczyną nowych form”, tak jak technologie cyfrowe tworzą nowe formy polityczne, społeczne i gospodarcze w środowisku strategicznym Polski.

Potraktowanie technologii cyfrowych jako przyczyny formalnej obala wiele z dzisiejszych analitycznych i społeczno-naukowych założeń. Oznacza ono, że technologie te nie są neutralne; przeciwnie, ich kulturowe, psychologiczne i socjologiczne konsekwencje wygaszają wiele z poprzednich możliwości i kreują nowe.

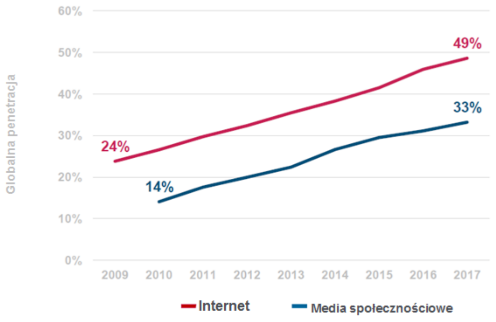
W tym miejscu można postawić pytanie „czy narzędzie to naprawdę kształtuje Polskę i świat w sposób tak gruntowny? Czy świat rzeczywiście jest aż tak ucyfrowiony?” Aby przedstawić choć garść danych z raportu[4] „Internet Trends” opublikowanego przez inwestorkę Mary Meeker w 2018 r., liczba godzin spędzanych codziennie przez dorosłych Amerykanów w mediach cyfrowych wzrosła z 2,7 w 2008 r. do 5,9 w 2016 r. Ponad połowa tego czasu przypada na urządzenia mobilne.

**Godziny spędzane codziennie w mediach cyfrowych przez dorosłych użytkowników**



Czy skala tego zjawiska dotyczy wyłącznie USA? Nie, globalna penetracja Internetu wzrosła z 24% światowej populacji w 2009 r. do ok. 49% w 2017 r. W tym czasie globalna penetracja mediów społecznościowych wzrosła z 14% światowej populacji w 2009 r. do ok. 33% w 2017 r.

**Internet + media społecznościowe — globalna penetracja**



Nikt nie spodziewa się, by za dekadę technologie informatyczne gdziekolwiek straciły na znaczeniu. Urządzenia cyfrowe kształtują realne życie coraz większej liczby ludzi, a zjawisko to będzie się tylko pogłębiało. Podsumowując, w rozważaniach na temat przyszłości, analitycy strategiczni powinni rozpatrywać pojęcie „rzeczywistości wirtualnego świata”[5] – wszystkich implikacji płynących z przejścia do nowych, cyfrowych form w Polsce i wokół niej.

## Nowa rola „mediów”?

Wpływ technologii na ludzkie wybory, struktury i treści w sposób najbardziej oczywisty widać na przykładzie mediów. Wspomnijmy tekst znany wielu analitykom strategicznym, „Mowa pogrzebowa Peryklesa”. Stanowi on perełkę dobrze skonstruowanej retoryki: ok. 2800 świetnie dobranych, przemyślanych i wyważonych słów. To m.in.

---

McLuhan objaśnia przemiany świadomości pod wpływem drukowanej książki w książce z 1962 r. pt. Galaktyka Gutenberga. Tworzenie człowieka druku.

[4] Dane i wykresy nt. korzystania z internetu zaczerpnąłem z raportu: https://www.kleinerperkins.com/perspectives/internet-trends-report-2018

[5] za Slavojem Zizkiem: Manufacturing Reality: lavoj Zizek and the Reality of the Virtual, dostępne pod adresem https://www.youtube.com/watch?v=YUTgcYxX-IZA

pod ich wpływem zaciągnąłem się do Korpusu Piechoty Morskiej. Choć z początku była to mowa pogrzebowa, słowa Peryklesa zostały uwiecznione w tekście Tukidydesa „Wojna peloponeska". Aby zrozumieć najbardziej podstawowy wpływ mediów, zadajmy sobie pytanie, czy ten sam przekaz mógłby do nas trafić za pomocą sygnałów dymnych i jaką miałby wtedy siłę rażenia? Dość oczywiste jest, że wybór medium (tekstu czy dymu) kształtuje charakter przesyłanej wiadomości.

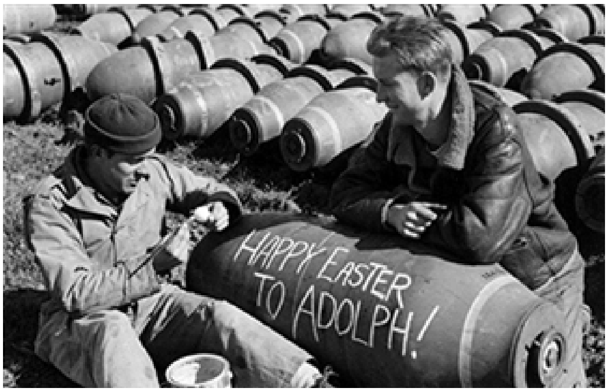
Spójrzmy na bliższy nam przykład. Według niektórych relacji, prezydent Abraham Lincoln świadomie użył mniej niż 300 słów w swej Przemowie gettysburskiej, gdyż rozumiał naturę nowego środka przekazu swoich czasów, czyli telegrafu. W Białym Domu często obserwował pracę telegrafistów i zdawał sobie sprawę, jak nowy wynalazek będzie kształtował rynek medialny. Jeśli Lincoln chciał przedstawić obywatelom cele wojenne w sposób bezpośredni i błyskawiczny, jego przemowa musiała być krótka, aby dziennikarze mogli ją przepisać oraz przekazać od razu i dosłownie. Możemy myśleć o tym wystąpieniu jako o dziewiętnastowiecznym tweecie, za pomocą którego Prezydent komunikował się bezpośrednio z obywatelami.

Z kolei w latach dwudziestych radio zmieniło tekstualne środowisko gazet i przywróciło nam formę medialną. Wynalazek ten świetnie opanowali Mussolini, Hitler, Roosevelt i Churchill. W latach pięćdziesiątych przyszła kolej na rewolucję telewizyjną. Niektórzy dowodzą, że wizualne elementy przekazu telewizyjnego pozwoliły „stworzyć" Ronalda Reagana, zaś obrazy niezmiennie drewnianego (a raz nawet zaślinionego) Breżniewa przyczyniły się do upadku ZSRR. Co ważne dla naszego wywodu, na każdym kroku tego technologicznego rozwoju zwiększał się ładunek emocjonalny przekazywanej wiadomości, zaś jej struktura logiczna stawała się mniej tekstowa i bardziej fragmentaryczna (lub co najmniej mniej liniowa).

Dziś już coraz większa część naszej komunikacji jest post-piśmienna. Ktoś zamieszcza zdjęcie rannego lub martwego dziecka na Facebooku lub Instagramie, a inni komentują za pomocą gniewnych lub smutnych „emotikonek". Środek przekazu ogranicza i kształtuje wiadomość. Narracja jest implikowana, lecz raczej nieobecna w nieprzyjaznym jej cyfrowym medium smartfona.

Czytelnicy zaznajomieni z teorią mediów zapewne wspomnieli teraz sławne i może trochę niejasne powiedzenie Marshalla McLuhana, „środek przekazu jest przekazem". Autor chciał przez to powiedzieć, że środek przekazu wpływa zarówno na dobór przesyłanych wiadomości, jak i ich odbiór. Według niego ukryte, podświadome efekty środka przekazu są ważniejsze od jego treści. To dlatego właśnie każda analiza strategicznej niepewności, która nie zaczyna się od próby zrozumienia wpływu wykorzystywanych technologii na naszą podświadomość (która z kolei kształtuje nasze przekonania i działania), skazana jest na niezrozumienie kultury i szerszego świata[6].

Dobrą metaforą ujęcia proponowanego przez McLuhana są stare zdjęcia z II Wojny Światowej, na których alianccy żołnierze malowali wiadomości na bombach przeznaczonych do zrzucenia na państwa Osi[7]:



---

[6] Mark Stahlman, The Digital Sphere, Order and Chaos, raport sporządzony dla Biura Oceny Sieci Departamentu Obrony USA, 2016

[7] zdjęcie z https://www.dailymail.co.uk/news/article-4571244/London-Bridge-attack-revenge-RAF-s-airstrike.html

Aby zrozumieć znaczenie środka przekazu, McLuhan radzi nam zignorować „treść" zapisaną na bombie i pomyśleć o skutku samej bomby! Konwencjonalna analiza zwykle ignoruje wybuchowość środka przekazu i skupia się na „treści" wiadomości[8].

Siła tezy McLuhana zwiększa się dramatycznie, jeśli zrozumiemy, że używał on słów „środki przekazu" na określenie całego „środowiska technologicznego", tj. matrycy technologii i jej efektów strukturalnych[9]. Np. w jednej ze swych najważniejszych prac „Zrozumieć media: Przedłużenia człowieka" (wyd. 1964, wersja polska 2004), analizuje społeczne i psychologiczne skutki takich „środków przekazu" jak lokomotywy, żarówki, maszyny do pisania czy nawet ubranie!

Jak już wspomnieliśmy, w cyfrowym świecie liczby nie tylko reprezentują zjawiska, ale i je tworzą. Dlatego gdy myślimy o technologiach cyfrowych, nie powinniśmy skupiać się jedynie na Facebooku czy Whatsappie, lecz spojrzeć na pełen pejzaż wynalazków ogólnego zastosowania, które tworzyć będą nowe formy i kształtować strategiczne, polityczno-społeczne, a nawet psychologiczne środowisko polskiego kraju. Po angielsku możemy je zapamiętać dzięki akronimowi 3-GRAIN:

- 3-D Printing (Druk 3-D)
- Genetics (Genetyka)
- Robotics (Robotyka – automatyzacja)
- Artificial Intelligence (Sztuczna Inteligencja – AI)
- Internet of Things (Internet rzeczy lub „big data")
- Nanotechnology (Nanotechnologia)

Każda z tych dziedzin jest pośrednio lub bezpośrednio związana z postępem cyfrowym. Nawet osobno są brzemienne w skutkach, lecz oprócz tego uzupełniają się wzajemnie i napędzają w wieloraki sposób. Powtórzmy sobie zatem: W świecie analogowym cyfry oznaczają lub symbolizują zjawiska, w świecie cyfrowym je tworzą. Technologie 3-GRAIN mogą wywrócić do góry nogami całe gałęzie przemysłu, obniżyć koszty technik podwójnego zastosowania lub podważyć oświeceniowe idee o podstawowej równości wszystkich ludzi. Dlatego też dyskusja na temat współczesnego świata musi wyjść poza ciasne ramy postulatów w stylu „naprawmy Facebooka" czy „walczmy z fake newsami".

## Osąd wartości – co to znaczy?

Jeśli więc to technologie cyfrowe zmieniają zarówno globalną politykę, jak i całe środowisko strategiczne Polski, jak możemy poradzić sobie z ich skutkami i co to właściwie oznacza?

Raz jeszcze możemy wrócić do McLuhana. W książce „Laws of Media" (1988), McLuhan podsumował swoje koncepcje w ramach „tetrady efektów środków przekazu"[10]. Jego analiza skutków technologii jest subtelna i nie ma wiele wspólnego ze stanowiskami zbywanymi jako „determinizm technologiczny".

Przy korzystaniu z tej tetrady możemy odnośnie do każdego środka przekazu czy technologii postawić pytanie, jaką ludzką funkcję ona rozwija. W procesie takiego rozwoju, technologia ta wypiera swoją poprzedniczkę, która spełniała dotychczas tę samą funkcję. Co jednak bywa ironiczne, nowy środek przekazu lub technologia często odwraca lub przekształca się w komplementarną (lub wręcz przeciwstawną) formę. Zwykle też przy tym przywraca jakieś starsze formy z bardziej odległej przeszłości cywilizacji.

---

[8] zob. wywiad z Marshallem McLuhanem dla Playboya, marzec 1969 r.

[9] McLuhan próbował wprowadzić termin „ekologii mediów", w nawiązaniu do modnego w latach sześćdziesiątych motywu „środowiska". Chciał w ten sposób zwrócić uwagę, że otaczający nas świat nie stanowi „natury", lecz jest stworzony przez człowieka.

[10] Wyraźny związek między tetradą mediów a przyczyną formalną jest przedstawiony w książce opracowanej i współtworzonej przez jego syna Eryka: Marshall McLuhan and Eric McLuhan, Media and Formal Cause, NeoPoiesis Press, LLC, 2011.

Tetrada efektów środków przekazu

McLuhan (1988)

Nie mamy tutaj miejsca na omówienie całej tetrady cyfrowej i jej skutków dla Polski, warto jednak zauważyć, że jedną z główną ludzkich funkcji, jaką rozwijają nowe technologie, jest pamięć. Systemy elektroniczne stanowią przedłużenie naszej pamięci. Za chwilę przejdziemy do konsekwencji uwiecznienia wspomnień i przyjrzymy się tym aspektom z naszej przeszłości, które możemy odzyskać dzięki cyfrowym technologiom. Chciałbym jednak w tym miejscu zwrócić czytelnikom uwagę, że to między innymi zapominanie pozwala nam nie popaść w szaleństwo, zaś jeśli współczesne struktury wydają się pękać czy wręcz „wariować”, dzieje się tak dlatego, że nasze społeczeństwo straciło zdolność zapominania. Zapisujemy i przechowujemy coraz więcej „wspomnień”. To właśnie o to rozbija się np. debata na temat prywatności.

## Osąd działania – co teraz robimy?

Nakreśliwszy obecne i przyszłe skutki technologii cyfrowej, chciałbym podsumować mój wywód kilkoma rozważaniami na temat przyszłości Polski, Europy i świata. Nawiązując do jednego z elementów tetrady McLuhana – przywracania – stawiałbym tezę, że pod wieloma względami „cyfrowy świat przywraca świat średniowieczny” pamiętany z polskiej historii.

Wielu ekspertów dowodzi, że towarzysząca nam współcześnie niepewność strategiczna to skutek dobrze zrozumianych czynników cyklicznych. Ponadto nowe technologie są „neutralne”, czyli w żargonie ekonomistów stanowią „efekty zewnętrzne” (externalities). Analitycy strategiczni stojący na tym stanowisku są przekonani, że ostatni wysyp prawicowych i lewicowych partii populistycznych w Europie (i gdzie indziej) to pokłosie kryzysu ekonomicznego z 2008 r. Gdy wzrost gospodarczy powróci, „populizm” zniknie wraz z niepewnością strategiczną. „Poczekajmy chwilę, a wszystko wróci do normy”.

Ja natomiast twierdzę, że nie ma już do czego wracać. Pozostajemy wciąż na etapie „wozu bez koni[11]”, czyli rozumienia i stosowania nowych technologii przez pryzmat starych. Tymczasem zrozumienie wszystkich implikacji zachodzących przemian wymaga ogromnej wyobraźni. Stwierdzając leniwie, że „to już kiedyś było”, zamykamy sobie drogę do strategicznej analizy.

Cały system międzynarodowy składa się z narodów i państw powstałych w innym środowisku medialno-technologicznym. Nasz świat zorganizowany jest wokół jednostek – państw narodowych i ponadnarodowych struktur jak ONZ – utworzonych w epoce druku i elektryczności (radio i TV). Jak te podmioty zachowają się w warunkach cyfrowych, w którym wracamy od systemu westfalskiego do czegoś na kształt średniowiecza?

---

[11] Pierwsze samochody w Ameryce nazywano właśnie „wozami bez koni”.

Pozwolę sobie zaprezentować być może trącące groteską paralele między średniowieczem a naszą epoką. Czy udaje się nam zauważyć:

- rozrost ponadnarodowej arystokracji, tzn. „elit" dysponujących ogromnym majątkiem, niejasną tożsamością narodową i elastycznym systemem sojuszy?

- międzynarodowy klimat, w którym państwa utraciły już monopol na przemoc, a pozapaństwowi aktorzy są w stanie rzucić im wyzwanie? Np. Al-Kaida lub Hezbollah, ale też Google czy Facebook.

- zwrot do tożsamości lokalnych, plemiennych lub religijnych? Zastanówmy się, jakie zjawiska noszą teraz łatkę „populizmu" albo spójrzmy na powrót średniowiecznego islamu w wydaniu ISIS. Niektórzy mówią o Turcji neoosmańskiej lub nawet Imperium Perskim w kontekście asertywnej polityki Iranu.

- nowe branże i technologie podważające status „gildii" dyplomowanych profesjonalistów? Choćby Uber kontra taksówkarze. A przecież czekają nas samochody bez kierowców. Czy to nie dziwne, że co najmniej jedna nowa struktura handlowa nie przyjmuje formy dwudziestowiecznych umów o wolnym handlu, lecz ma wyraźnie średniowieczny wydźwięk? Chiński projekt jednego pasa i jednej drogi jest przecież fetowany jako nowy „jedwabny szlak"!

- kolejne plagi i zarazy? Ptasia grypa czy Ebola. Pomyślmy o Theodorze Kaczynskim, tzw. Unabomberze. A jeśli kolejny zamachowiec nie będzie matematykiem, lecz genetykiem? W przyszłości może on „zbawiać" świat za pomocą zmodyfikowanego wirusa HIV roznoszonego przez komary.

- masowe migracje? Technologie cyfrowe pozwalają znaleźć emigrantom nowe miejsca pobytu i trasy wędrówki, skontaktować się z przemytnikami lub zagwarantować płatność ze strony rodzin po wysłaniu selfie jako „dowodu, że żyję". Co więcej, wystawiają oni przemytnikom oceny w podobny sposób, jak my oceniamy kierowców Ubera[12].

- Te podobieństwa są spekulatywne, uproszczone i przejaskrawione. Chciałbym jednak uczulić na nie analityków strategicznych. Korzystam ze średniowiecznych analogii, by wzbudzić pewne emocje:

- Czy państwa narodowe flirtują z „baronami", potężnymi niepaństwowymi aktorami? Dania zatrudnia obecnie „ambasadora technologicznego" ze stałymi placówkami w trzech miejscach: Kopenhadze, Pekinie i Dolinie Krzemowej[13]. Uwagę Unii Europejskiej zaprząta obecnie zarówno niepaństwowy terroryzm, jak i presja ze strony Rosji, cofniętej do swych szesnastowiecznych granic.

- Czy widzimy powrót murów, fos i zamków? Jak zauważył niedawno David Betz w artykule w Infinity Journal, „World of Wallcraft: The Contemporary Resurgence of Fortification Strategies[14]", stałe umocnienia i fortyfikacje wracają do łask. Można sobie nawet wyobrazić, że budowa murów stałaby się osią skutecznej kampanii politycznej. Donald Trump? Victor Orban?

- Robert Kaplan postulował niedawno określenie strategicznego kontekstu Ameryki mianem „powrotu świata czasów Marco Polo [15]". W dwudziestym pierwszym wieku! Jak już wspominaliśmy, chińską inicjatywę „Jednego pasa i jednej drogi" można rozumieć jako renesans szlaku jedwabnego dynastii Tang. Pekin wprost nawiązuje do tej tradycji.

---

[12] z prywatnej rozmowy z pracownikiem FRONTEX-u.

[13] zob. http://techamb.um.dk/

[14] David Betz, World of Wallcraft: The Contemporary Resurgence of Fortification Strategies, Infinity Journal. Volume 6, Issue 1, Winter 2018.

[15] Robert D Kaplan. The Return of Marco Polo's World: War, Strategy, and American Interests in the Twenty-first Century. Random House, 2018.

- Czy Unia Europejska po Brexicie nie przypomina neośredniowiecznego Świętego Cesarstwa Rzymskiego? Charakteryzuje ją trzon francusko-niemiecki, niedoskonałe kompromisy, niejasne kompetencje wobec państw narodowych wchodzących w jej skład, a także stolica w Brukseli (zamiast Akwizgranu, stolicy Cesarstwa).

Na miejscu polskich analityków strategicznych zadałbym sobie pytanie:

- Czy w dwudziestym pierwszym wieku nie pobrzmiewa echo Polski średniowiecznej? Tak można odbierać Inicjatywę Trójmorza, zaś rozmowy z krajami skandynawskimi czy bałtyckimi przywodzą na myśl jakiś rodzaj Hanzy. Lepsi ode mnie eksperci w dziedzinie Polski średniowiecznej zwracali już uwagę na te podobieństwa, próbując lepiej zrozumieć nasze czasy. Czy to wszystko nie czyni z UE nowego Świętego Cesarstwa Rzymskiego (z jego wieloma dysfunkcjami)?

- Pozwolę sobie przypomnieć, że jedną z silnych stron Polski średniowiecznej była jej różnorodność kulturowa i wyznaniowa, co nie w smak wielu współczesnym komentatorom mówiącym o obronie Polski i „Zachodu” w czasach zwiększonej niepewności strategicznej. Obecna jednorodność etniczna, religijna i językowa tego kraju jest w miarę świeża i nie jest skutkiem pobożności, lecz dziełem Adolfa Hitlera i Józefa Stalina. Czy ta potworna spuścizna to najlepszy pomysł na zabezpieczenie przyszłości Polski? Twierdziłbym, że jest dokładnie na odwrót. Z organicznej tradycji różnorodności i tolerancji Polska może czerpać bardzo dużo siły.

## Podsumowanie

Niniejszy esej stanowi balon próbny, test pewnych idei. Mam nadzieję, że może inspirować pewne przemyślenia. Nakłaniałbym polskich i europejskich analityków strategicznych do rozważenia co najmniej tych koncepcji:

- czy technologie cyfrowe naprawdę są „neutralne” pod względem psychologicznym, kulturowym czy socjologicznym, jak tego chciałyby konwencjonalne nauki społeczne?

- czy stać nas na ignorowanie nowej matrycy czynników sprawczych, które te technologie przynoszą – nowych struktur naszych ludzkich wyborów?

- czy paradygmat „jednego świata” lub „porządku światowego” w przyszłych relacjach międzynarodowych, czy choćby kontynuacja systemu westfalskiego, raczej traci czy zyskuje na znaczeniu? czy nie był owocem nieistniejących już warunków medialnych?

- Mówiąc krótko, czy nie należy zacząć myśleć o przyszłości Polski i niepewności strategicznej w kontekście „środowiska cyfrowego”?

## dr A. Kozłowski

## Implikacje wdrażania technologii 5G dla organizacji systemu cyberbezpieczeństwa państwa

### Wstęp

Proces wdrożenia sieci 5G w Polsce rozpocznie się niebawem i jednym z problemów z nim związanych jest kwestia bezpieczeństwa sprzętu i usług, które będą oferowane w ramach nowej sieci. Bezpieczeństwo łańcucha dostaw dla technologii 5G staje się coraz bardziej istotnym zagadnieniem dla bezpieczeństwa państwa i wyzwaniem dla systemu cyberbezpieczeństwa, który dopiero się w Polsce formuje. Technologia 5G nie będzie pierwszą, która będzie wdrażana w Polsce i która budzi obawy o bezpieczeństwo, dlatego tak istotne jest zbudowanie kompleksowego systemu oceny ryzyka w łańcuchu dostaw. Obecna sytuacja związana z siecią 5G stanowi dobry bodziec do omówienia tej kwestii i wdrożenia tego elementu do systemu cyberbezpieczeńtwa. Mechanizmy i systemy certyfikacji wypracowane podczas oceny bezpieczeństwa produktów 5G będą mogły być wykorzystane jako podstawa do stworzenia kompleksowego systemu ochrony łańcucha dostaw sprzętu i oprogramowania IT.

### Czym jest sieć 5G i jakie wyzwania niesie?

Technologia mobilna piątej generacji (5G) to nowy standard sieci komórkowej, który stanowi ewolucję w stosunku do sieci 3G i 4G, dlatego też nie powinna być postrzegana w oderwaniu od istniejącej infrastruktury telekomunikacyjnej. Obecnie istniejąca infrastruktura stanie się punktem wyjścia dla budowy sieci piątej generacji. Sieć 5G stanowi również rewolucję w porównaniu do poprzednich standardów sieci komórkowych, ponieważ niesie możliwość olbrzymich zmian dla społeczeństwa, sektorów gospodarki, administracji państwowej oraz sił zbrojnych.

Sieć 5G dzięki możliwości przesyłania olbrzymich ilości danych, bez opóźnienia, otworzy drzwi dla masowej ilości systemów tzw. inteligentnych miast, inteligentnego przemysłu czy inteligentnych domów. Autonomiczne samochody czy pociągi, regulowane komputerowo oświetlenie w miastach, tele-medycyna, regulowanie ruchu czy znaczne ułatwienia dla mieszkańców to tylko niektóre z zalet. Przykładowo sensory anty-kolizyjne autonomicznych samochodów będą musiały mieć ciągły i niezakłócony dostęp do danych. 5G wygeneruje oszczędności, zmieni rynek pracy oraz wspomoże innowacyjność i rozwój gospodarczy państwa. Stanie się kręgosłupem nowoczesnego kraju. Będzie miała również znaczenie dla wojska usprawniając komunikację na polu bitwy czy umożliwiając każdemu żołnierzowi dostęp do ogromnej ilości informacji, co poprawi jego świadomość sytuacyjną. Umożliwi również zastosowanie większej liczby autonomicznych pojazdów. Państwa nie będą miały wyboru, jeśli chcą się rozwijać to będą zmuszone zaadaptować technologie sieci 5G, w inny wypadku zostaną daleko w tyle. Raport GSMA z 2018 roku szacuje, że światowa gospodarka może powiększyć się o ponad pół biliona dolarów w związku z rozwojem sieci 5G. Ministerstwo Inwestycji i Rozwoju przewiduje, ze wdrożenie 5G może przełożyć się na wzrost polskiego PKB nawet o 13-20 %.

Ze względu na zmianę, którą wnosi 5G pojawiają się obawy o bezpieczeństwo produktów, które będą w nich używane. Niektórzy wręcz straszą przerażającymi skutkami, jak np. ambasador Stanów Zjednoczonych przy Unii Europejskiej, który powiedział, że chińska technologia użyta w ramach sieci 5G będzie mogła zabijać na odległość. Przed produktami pochodzącymi z Państwa Środka ostrzegał również amerykański sekretarz stanu Mike Pompeo. Powiedział on, że ten kto wygra wyścig o sieć 5G ten będzie rządził Internetem. Dodał też, że stosowanie chińskich technologii, spowoduje, że rząd w Pekinie uzyska dostęp do wrażliwych i poufnych danych. Twierdzenia te powinny być traktowane jako element geopolitycznej rywalizacji pomiędzy Stanami Zjednoczonymi i Chinami, gdzie rozwój nowoczesnej technologii staje się nowym obszarem konfrontacji tych mocarstw. Nie oznacza to jednak, że zagrożenia związane z wdrożeniem sieci 5G nie są realne i nie powinny być traktowane poważnie.

Powszechna automatyzacja oraz zwiększenie się liczby urządzeń podłączonych do sieci powoduje, że powiększa się przestrzeń ataku. Hakerzy mają o wiele większy wyborów punktów dostępowych do sieci. Ponadto zakłócenie transportu danych, albo ich skorumpowanie poprzez przesłanie błędnych informacji, może doprowadzić do fizycznych zniszczeń i śmierci ludzi. Co więcej o wiele trudniej będzie wykryć jakąkolwiek złośliwą aktywność w cyberprzestrzeni. Dodatkowo wiele z funkcji rdzenia sieci będzie się odbywało w chmurze i bazowało na sztucznej inteligencji, której zadaniem będzie nadzorowanie i zarządzanie skomplikowanymi zasobami sieciowymi. Hakerzy mogą zaatakować i manipulować algorytmami wpływając na prace systemów opartych na sztucznej inteligencji. Chmura również zostanie dostarczona przez zewnętrznego odbiorcę, który powinien podlegać rygorystycznej kontroli. Z wyżej wymienionych powodów bezpieczeństwo i odporność powinny być priorytetem już na samym początku budowy nowych sieci. Uczestniczy międzynarodowej konferencji w Pradze poświęconej 5G apelowali o branie pod uwagę ryzyka wpływu państw trzecich, szczególnie dostarczycieli technologii, zwłaszcza ich model rządów i umowy o współpracy w dziedzinie bezpieczeństwa. Zwraca się również uwagę na to, że to operatorzy muszą dbać o kontrolę bezpieczeństwa swoich sieci – stwierdzono na międzynarodowej konferencji w Pradze poświęconej 5G.

Ze względu na znaczenie dla państwa, należy wykonać wszechstronną i kompleksową analizę ryzyka przed wdrożeniem technologii 5G, aby poznać jakie zagrożenie niesie dostarczany w jej ramach sprzęt. Zaaprobowanie źle zabezpieczonego sprzętu od niezaufanego producenta może grozić poważnymi konsekwencjami i stać się idealnym celem dla hakerów. Analiza ryzyka i certyfikacja produktów przeprowadzona przy wdrożeniu sieci 5G powinna być sprawdzianem dla świeżo kształtującego się w Polsce systemu cyberbezpieczeństwa. Umożliwia ona również stworzenie pewnego schematu dokonywania oceny bezpieczeństwa łańcucha dostaw, który powinien na stałe zostać zaadaptowany jako element polityki bezpieczeństwa państwa.

### System cyberbezpieczeństwa

Skuteczny system cyberbezpieczeństwa powinien obejmować szerokie spektrum podmiotów z sektora prywatnego i publicznego, cywilnego i wojskowego, które współpracują w celu stworzenia systemu gwarantującego ochronę przed zagrożeniami w cyberprzestrzeni. Ze względu na fakt, że technologia IT dostarczana jest z całego świata, a jej łańcuch dostaw obejmuje różne podmioty, kluczowym elementem systemu musi być proces sprawdzania bezpieczeństwa sprzętu i oprogramowania IT.

Polska rozpoczęła budowę własnego systemu cyberbezpieczeństwa stosunkowo późno i musi gonić innych partnerów z Unii Europejskiej w tym względzie. Bodźcem inicjującym pracę nad systemowym i kompleksowym podejściem do cyberbezpieczeństwa był raport NIK z 2015 roku, w którym wskazano liczne zaniedbania. Przede wszystkim zwrócono uwagę na brak spójnych i systemowych działań przeciwko zagrożeniom występującym w cyberprzestrzeni oraz brak jednolitego ośrodka decyzyjnego. Dzisiaj mamy obowiązującą od roku Ustawę o Krajowym Systemie Cyberbezpieczeństwa, która stanowi fundament systemu cyberbezpieczeństwa. Wprawdzie nie rozwiązuje ona wszystkich problemów wymienionych w raporcie, a sama ustawa podawana jest krytyce to stanowi jednak fundament do dalszego działania. Ustawa podzieliła odpowiedzialność na trzy główne zespoły CSIRT: jeden zlokalizowany w Ministerstwie Obrony, drugi w NASK i trzeci w ABW. Powołano również pełnomocnika rządu ds. cyberbezpieczeństwa oraz Kolegium ds. Cyberbezpieczeństwa, które jest ciałem doradczym w skład którego wchodzą przedstawiciele najważniejszych resortów. Elementem polskiego systemu cyberbezpieczeństwa musi być również mechanizm pozwalający na ocenę ryzyka dla bezpieczeństwa łańcucha dostaw.

### Ryzyko dla bezpieczeństwa łańcucha dostaw

Wprowadzenie jednolitego standardu bezpieczeństwa w całym łańcuchu dostaw jest niezwykle istotnym elementem polityki cyberbezpieczeństwa. Państwo kupując za granicą kluczową technologię dla swoich usług cyfrowych jak np. e-dowodów musi mieć pewność, że będzie ona bezpieczna i będzie zapewniała odpowiednią ochronę prywatności. W przypadku technologii 5G łańcuch dostaw wszystkich rozwiązań jest podatny na takie same zagrożenia związane z międzynarodową siecią dostawców. Dostarczanie sprzętu komputerowego ze wbudowanymi „tylnymi furtkami" (backdoor), które umożliwiają szpiegowanie, przejmowanie danych, zmianę kierunku przepływu informacji czy też zainfekowanie systemów komputerowych jest koszmarem dla operatorów infrastruktury krytycznej, polityków i wojskowych. W sieci 5G problem ten dotycz rdzenia sieci, ale również tzw. krawędzi, gdzie zapewnienie bezpieczeństwa jest nawet trudniejsze. „Tylnie furtki" mogą zostać zainstalowane w stacjach bazowych, umożliwiając przejęcie danych oraz manipulowanie nimi. Wykrycie takiego włamania, którego celem jest kopiowanie lub przejmowanie danych jest bardzo trudne, ponieważ taka stacja bazowa zachowuje się normalnie.

W przeszłości mieliśmy już przypadki, w których bezpieczeństwo łańcucha dostaw zostało naruszone. Informacje ujawnione przez Edwarda Snowdena oraz wyciek danych z CIA pokazują skalę współpracy sektora prywatnego z amerykańskim wywiadem. Wbudowane „tylne furtki" w systemie Windows umożliwiały agencjom wywiadowczym włamywanie się do komputerów praktycznie na całym świecie. Hardware był również zagrożony, gdyż członkowie amerykańskiego wywiadu montowali w fazie produkcji, „tylne furtki" umożliwiające szpiegowanie. Naturalnie taka aktywność podejmowana jest również przez innych producentów oprogramowania, w szczególności wątpliwości budzi technologia z państw autorytarnych takich jak Rosja i Chiny. Rosyjska firma KasperskyLab została złapana na gorącym uczynku, kiedy jej serwery zostały wykorzystane przez rosyjski wywiad do szukania dokumentów i narzędzi hakerskich NSA. Problem bezpieczeństwa dostaw pojawia się również przy budowie 5G, ponieważ liderem na tym polu są firmy chińskie. Wprawdzie nie zostały one złapane na gorącym uczynku, to od dawna Stany Zjednoczone i ich sojusznicy podejrzewają je o bliską współpracę z rządem. Co w takim razie należy zrobić i jak zabezpieczyć sieć 5G w Polsce?

### Sieć 5G a system cyberbezpieczeństwa państwa

Polska nie jest jedynym państwem, które stoi przed wyzwaniem bezpiecznego wprowadzenia technologii 5G. Dlatego też warto przyjrzeć się sposobom w jakie radzą sobie inne państwa. Najbardziej radykalnym rozwiązaniem jest wykluczenie danego producenta z budowy sieci 5G. Tak postąpiły m.in. Stany Zjednoczone i Australia w przypadku chińskiej firmy Huawei. Decyzję tą tłumaczono zagrożeniem dla bezpieczeństwa narodowego. Nie przedstawiono jednak żadnych dowodów na potwierdzenie oskarżeń, co rodzi liczne spekulacje co do prawdziwych motywów tej decyzji. Z polskiego punktu widzenia decyzja ta była początkowo rozważana przez rząd, ale nie ma on jednak racji bytu w polskich warunkach. Z ekonomicznego punktu widzenia byłoby to niezwykle kosztowne i wiązałoby się nie tylko z budowaniem sieci 5G innymi środkami, ale również z odtworzeniem istniejącej struktury 3G i 4G, ponieważ ta w dużej mierze bazuje na rozwiązaniach chińskiego producenta. Zdaniem kierownictwa polskiego oddziału Huawei nawet 50% wszystkich anten komórkowych, które są obecnie w Polsce używane w sieciach różnych operatorów zostało zainstalowanych przez chińską firmę. Ponadto decyzja o wykluczeniu takiego producenta miałaby znaczne reperkusje polityczne i narażała Polskę na retorsje ze strony Chin. Opcja wyrzucenia danego producenta jest ostatecznym i bardzo mało prawdopodobnym rozwiązaniem, również w przyszłości.

Zamiast wyrzucać daną firmę, alternatywnym pomysłem jest opracowanie odpowiedniego mechanizmu zarządzania ryzykiem i minimalizacji potencjalnego zagrożenia. Taki model wybrała Wielka Brytania, która kwestię Huawei i sieci 5G rozwiązała inaczej, ograniczając dostęp tego producenta do sieci uważanych za kluczowe z punktu widzenia bezpieczeństwa narodowego. Niektórzy eksperci krytykują jednak stanowisko zajęte przez Londyn, argumentując, że w sieci 5G inaczej niż w przypadku 4G nie będzie możliwe oddzielenie rdzenia od warstwy radiowej. W raporcie o bezpieczeństwie sieci 5G opublikowanym przez Centrum Doskonalenia Cyberobrony NATO, autorzy argumentują, że technologia 5G zmniejsza odseparowanie pomiędzy rdzeniem a krawędzią sieci telekomunikacyjnej, co wiąże się z tym, że nie ma możliwości ograniczenia wpływu dostawcy technologii na krawędź. Inaczej mówiąc w sieci 5G część funkcji, która była tradycyjnie wykonywana w rdzeniu sieci będzie przeprowadzona na jej krawędzi.

Analizując kwestię Wielkiej Brytanii, warto również wskazać na model współpracy rządu brytyjskiego z Huawei. W 2010 roku podpisane zostało porozumienie między rządem Wielkiej Brytanii a Huawei, na mocy którego służby brytyjskie mogą dokonywać testów infrastruktury, sprzętu i oprogramowania chińskiego giganta w ramach Huawei Cyber Evaluation Centre. Brytyjscy rządowi eksperci razem z pracownikami chińskiego giganta sprawdzają pod kątem bezpieczeństwa produkty, a stawiane wymagania są bardzo restrykcyjne. W trakcie badań udało się zidentyfikować wiele błędów w kodzie, co powinno doprowadzić do poprawy bezpieczeństwa produktów w przyszłości. Podobne Centra Bezpieczeństwa istnieją również w innych państwach europejskich jak np. Belgia czy Niemcy. Niestety na razie żadna inna firma nie poszła śladami chińskiego giganta, a taki rodzaj współpracy publiczno-prywatnej z pewnością wzmocniłby bezpieczeństwo. W Polsce padła propozycja ze strony chińskiej firmy, która oferowała rządowi dostęp do swoich kodów źródłowych, ale według informacji polskiego oddziału Huawei, rząd w Warszawie nie skorzystał z tej propozycji. W przyszłości tego typu propozycje powinny zostać jednak podjęte, ponieważ stanowią przykład pozytywnej współpracy publiczno-prywatnej i przyczyniają się do wzmocnienia bezpieczeństwa, ponieważ nigdy zbyt duża ilość testów nie jest czymś złym. Niestety taka opcja również nie jest idealna, ze względu na konieczność przeanalizowania ogromnej ilości kodu. Jest to czasochłonne zajęcie wymagające zaangażowania dużej liczby specjalistów. Ponadto należy pamiętać, że praktycznie każda aktualizacja systemu może takie „tylne furtki" wgrać, dlatego możliwa jest sytuacja, że sprawdzony pod kątem bezpieczeństwa system i zakwalifikowany do dalszego użytku otrzymuje aktualizację z „tylną furtką".

Omawiając bezpieczeństwo sieci 5G, trzeba wskazać na jeszcze dwa rozwiązania, które funkcjonują w Wielkiej Brytanii i Niemczech, a które można wprowadzić w Polsce. Pierwszym jest obowiązek dywersyfikacji dostawców infrastruktury krytycznej, polegający na tym, że nie uzależniamy sieci 5G od jednego producenta. Podmiot, który dostarczy technologię dla sieci 5G uzyska ogromny dostęp do danych. Informacje przesyłane i odbierane przez urządzenia mobilne, inteligentne domy czy samochody będą transportowane przez infrastrukturę danego producenta, dlatego tak ważna jest dywersyfikacja. Ważne jest również to, że powinno to umożliwiać przełączanie się usług jednego operatora na usługi innego operatora w przypadku wystąpienia awarii lub ataku. Drugim dobrym pomysłem jest wprowadzenie kategorii „zaufanego dostawcy" (trusted vendor) wprowadzonego w Wielkiej Brytanii i Niemczech. Kryteria, które umożliwią zaklasyfikowanie danego producenta jako zaufanego odbiory nie powinny obejmować tylko i wyłącznie kwestii technicznych, ale też uwzględniać takie rzeczy jak kraj pochodzenia, transparentność firmy, incydenty szpiegowskie w historii czy relacje z władzami rodzinnego państwa. Ustalanie „zaufanego dostawcy" powinno odbywać się we współpracy z innymi krajami i forum Unii Europejskiej jest tu idealnym miejscem aby o tym decydować. Obie propozycje są rozważane przez rząd Polski i powinny być uwzględnione w ekosystemie bezpieczeństwa 5G.

### Bezpieczeństwo łańcucha dostaw

Bezpieczne wdrożenie sieci 5G w Polsce zbuduje rozwiązania systemowe, które powinny stać się fundamentem rozwoju dla bezpieczeństwa łańcucha dostaw wszystkich produktów IT. Jedną z najważniejszych zmian w tym obszarze będzie wprowadzenie aktu ds. cyberbezpieczeństwa Unii Europejskiej. Jego implementacja do polskiego porządku prawnego będzie wymagała zmian w obowiązującej legislacji jak np. w Ustawie o krajowym systemie cyberbezpieczeństwa. Wśród najważniejszych zmian, które wprowadza jest ustanowienie europejskich ram certyfikacji cyberbezpieczeństwa i określenie mechanizmu ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa oraz potwierdzania, że dane produkty bądź usługi spełniając określone wymogi bezpieczeństwa.

Jest to wyzwanie dla państw członkowskich, które będą musiały zbudować odpowiednie kompetencje oraz infrastrukturę do testowania certyfikowanego sprzętu. Europejski program certyfikacji będzie określał trzy poziomy bezpieczeństwa: podstawowy, istotny i wysoki. Poziom uzasadnienia zaufania dla danego urządzenia czy usług ICT powinien być proporcjonalny do poziomu ryzyka. Wydany na określonym poziomie certyfikat zapewnia, że produkty, usługi i procesy ICT spełniają odpowiednie wymogi bezpieczeństwa. Unijny program wydaje się stanowić dobrą podstawę do budowania fundamentów bezpieczeństwa łańcucha dostaw, jednak realną skuteczności tego rozwiązania będzie można ujrzeć dopiero w niedalekiej przyszłości. Należy przede wszystkim pamiętać, że o ile przygotowanie programów certyfikacji cyberbezpieczeństwa odbywa się na poziomie europejskim, o tyle same procesy certyfikacji przebiegają na poziomie krajowym. Akt cyberbezpieczeństwa nakłada na państwa konkretne obowiązki, które mają pomóc w budowie sprawnego systemu certyfikacji. Konieczne jest posiadanie krajowego organu ds. certyfikacji, krajowej jednostki akredytującej oraz jednostek oceniających zgodność.

Certyfikacja to jednak nie wszystko, ponieważ równie ważne jest odpowiednie zarządzaniem sprzętem w jednostkach administracji publicznej oraz podmiotach infrastruktury krytycznej. Sytuacja, w której nie ma odgórnych wytycznych i nadzoru nad sprzętem oraz oprogramowaniem stanowi poważne naruszenie i zagrożenie dla bezpieczeństwa łańcucha dostaw. Należy wyeliminować samowolkę poszczególnych ministerstw i innych jednostek i ujednolić używany sprzęt. Istotne byłoby również rozważanie przy zamówieniach publicznych, ryzyka bezpieczeństwa tak bardzo ważnego elementu.

### Suwerenność cyfrowa

Bezpieczeństwo łańcucha dostaw powinno wiązać się z tzw. suwerennością cyfrową czyli kontrolą nad własna sferą informacyjną. Państwo powinno dążyć do stworzenia jak największej liczby systemów opartych o autorskie rozwiązania rodzimej produkcji w obszarach kluczowych dla funkcjonowania państwa. Wyprodukowanie własnego procesora czy systemu operacyjnego wydaje się być poza zasięgiem polskich możliwości, ale stworzenie już np. bezpiecznego komunikatora szyfrującego dla polityków i urzędników nie jest. Na takie rozwiązanie zdecydowała się Francja. Obawiając się, szpiegowania ze strony popularnych aplikacji szyfrujących takich jak Telegram czy WhatsApp, których serwery zlokalizowane są poza terytorium Francji, Paryż zdecydował się na wprowadzenie własnego zaszyfrowanego programu. Ma on być wykorzystywany przez urzędników i członków rządu. Podobne rozwiązanie powinno znaleźć się w Polsce.

**Rekomendacje**

- Z uwagi na stopień skomplikowania zapewnienie ochrony sieci 5G w Polsce wymaga wielostopniowego podejścia obejmującego środki techniczne, zmiany prawne, działania dyplomatyczne oraz inwestycje w badania i rozwój oraz szkolenia z zakresu cyberbezpieczeństwa;

- Konieczna są regulacje polityczne, ponieważ środki techniczne jak szyfrowanie, VPN-y czy inne mechanizmy ochrony prywatności nie są w stanie zredukować ryzyka w sieci 5G;

- Należy wdrożyć w Polsce standardy bezpieczeństwa zapewniające, że sieci 5G będą zaprojektowane, zbudowane i utrzymywane w sposób maksymalnie uniezależniający poziom ich bezpieczeństwa od wyboru dostawców;

- Państwo powinno określić minimalne wymagania bezpieczeństwa, które sieci 5G budowane w Polsce muszą spełnić. Następnie należy je rozszerzyć na inne technologie używane w sektorach krytycznych dla funkcjonowania państwa;

- Celem administracji państwowej powinna być również weryfikacja zasad bezpieczeństwa w przypadku sieci 5G i obecnych na rynku urządzeń sieciowych;

- Celem zagwarantowania bezpieczeństwa sieci 5G konieczne jest podjęcie współpracy na arenie międzynarodowej i stworzenia wspólnej analizy ryzyka dla bezpieczeństwa i integralności łańcucha dostaw. Akt o cyberbezpieczeństwie UE, który wprowadza obowiązkowy system certyfikacji jest krokiem we właściwa stronę;

- Należy postawić wysokie wymagania odnośnie budowy i działania sieci 5G dot. bezpieczeństwa, certyfikacji produktów, dywersyfikacji dostawców oraz współpracy z producentami, jak też telekomami aby zminimalizować ryzyko wynikające z jej wdrożenia;

- Mechanizmy wytworzone przy systemie certyfikacji i badania bezpieczeństwa infrastruktury i produktów 5G powinny zostać przekształcone w stały element systemu cyberbezpieczeństwa wykorzystywany do badania nowych technologii pod tym kątem, zgodnie z wymaganiami europejskiego aktu ds. cyberbezpieczeństwa;

- Państwo polskie powinno postawić na jak największą suwerenność technologiczną cechującą się wprowadzeniem polskich rozwiązań z obszaru cyberbezpieczeństwo, jak np. szyfrowanych komunikatorów;

## prof. dr hab. A. Gruszczak

## Służby specjalne Polski w dobie współczesnych wyzwań cywilizacyjnych i technologicznych

Służby specjalne zajmują szczególne miejsce w ustroju politycznym każdego państwa. Spoczywa na nich odpowiedzialność za tworzenie jak najpełniejszego i najdokładniejszego obrazu rzeczywistości, która jest przedmiotem rządzenia. Instytucje władzy państwowej oraz osoby podejmujące w ich ramach kluczowe decyzje dotyczące ładu publicznego, pomyślności gospodarczej oraz bezpieczeństwa narodowego muszą dysponować jak najszerszą wiedzą o stanie spraw, leżących w ich gestii. Służby specjalne powołane zostały po to, aby dostarczać instytucjom i organom państwa wiedzy o bieżącej sytuacji wewnętrznej i międzynarodowej poprzez gromadzenie danych i informacji, ich przetwarzanie i analizowanie, przygotowywanie ocen sytuacyjnych, a także w określonych sytuacjach podejmowanie działań ograniczających lub eliminujących źródła zagrożeń dla interesu narodowego państwa.

We współczesnym świecie, cechującym się rosnącą złożonością, zalewem informacji z niezliczonych źródeł, rywalizacją o wpływy polityczne i ekonomiczne, szybkością zachodzących zmian, organizacja i działania służb specjalnych stają się szczególnie odpowiedzialne i znaczące dla bezpieczeństwa i pomyślności społeczeństwa i państwa. Dążenie do obiektywizacji opisu i oceny stanu rzeczy nigdy nie było tak utrudnione, jak w czasach obecnych. Cytat z Ewangelii wg św. Jana „Poznajcie prawdę, a prawda was wyzwoli”, widniejący m.in. na ścianie hallu głównego budynku CIA w Langley, nabiera szczególnego znaczenia. Zdolności dotarcia do prawdziwych, tj. wiernie obrazujących istniejącą rzeczywistość, informacji znacząco się rozwinęły dzięki postępowi technologicznemu i nowym narzędziom i metod pozyskiwania oraz przetwarzania danych i informacji. Mimo to, wiedza o prawdziwym, obiektywnym stanie rzeczy tworzona jest z rosnącymi trudnościami, gdyż coraz bardziej rozwinięte zdolności poznawcze są zaburzone przez rozproszenie, zdeformowanie, zakłócenie i zmanipulowanie źródeł tej wiedzy. Tym trudnościom towarzyszą niepokój i niepewność co do rzeczywistej wartości danych i informacji oraz lęk przed błędami i „wpadkami” o bardzo poważnych konsekwencjach.

Te dylematy i problemy towarzyszą większości państw świata, dążących do jak najlepszego zapewnienia swojego bezpieczeństwa i realizacji podstawowych interesów w zmieniającym się i coraz bardziej skomplikowanym świecie. Polskie służby specjalne także muszą stawić czoła tym wyzwaniom. Dotychczasowe systemowe rozwiązania nie gwarantują zdolności do skutecznej odpowiedzi na nasilające się zagrożenia, z upływem czasu mogą stanowić obciążenie utrudniające, czy wręcz uniemożliwiające elastyczne reagowanie na zagrożenia, zwłaszcza nowego typu. Wieloletnie zaniedbania normatywno-organizacyjne, skłonność do upolitycznienia służb specjalnych i związana z tym płynność kadrowa, a także niedopracowane zasady i mechanizmy nadzoru i kontroli nad służbami specjalnymi powodują pilną konieczność głębokich zmian strukturalno-systemowych, w wyniku których Rzeczpospolita Polska będzie lepiej chroniona przed zagrożeniami zewnętrznymi i wewnętrznymi.

Niniejszy rozdział ma charakter prognostyczno-rekomendacyjny. Zawiera propozycje przebudowy systemu służb specjalnych w kierunku znacznego zwiększenia zdolności do diagnozowania, przewidywania i przeciwdziałania najpoważniejszym zagrożeniom dla narodowych interesów państwa polskiego.

**Priorytety reformy służb specjalnych:**

1. Modernizacja – dopasowanie organizacji, wyposażenia oraz metodyki działania do współczesnych wyzwań; wykorzystanie wzorcowych praktyk służb specjalnych/wywiadowczych innych państw.

2. Profesjonalizacja – nowoczesny system naboru, szkolenia i doskonalenia zawodowego funkcjonariuszy służb specjalnych; skuteczny system motywacyjny i awansowy; specjalizacja zawodowa połączona ze stałym rozwojem wiedzy i umiejętności.

3. Konsolidacja – stworzenie spójnego, skutecznego i funkcjonalnego systemu służb specjalnych stanowiącego narodową wspólnotę bezpieczeństwa skupioną wokół centrum decyzyjnego umocowanego przy szefie rządu jako organie władzy wykonawczej.

4. Odpolitycznienie – unikanie podatności kierownictwa służb specjalnych na naciski partii politycznych (zwłaszcza będących u władzy), krzewienie zasady służebności wobec państwa i narodu, dążenie do bezstronnych i obiektywnych rezultatów działalności służb.

5. Odpowiedzialność - wpojenie zasad etyki zawodowej; mechanizmy dyscyplinujące funkcjonariuszy i egzekwujące normy bezpieczeństwa informacji (zwłaszcza niejawnych) także po zakończeniu czynnej działalności w służbach specjalnych; wzmocnienie mechanizmów nadzoru i kontroli ze strony właściwych organów władzy państwowej.

**B. Wyzwania**:

**a) globalne:**

– Wzrastająca złożoność współczesnego środowiska bezpieczeństwa ułatwiająca rozprzestrzenianie się zagrożeń.

– „Cyfrowe tsunami”- zalew informacji generowanych przez użytkowników Internetu przy stałym, liczbowym ich wzroście; rosnące tempo obiegu informacji; mieszanie danych odzwierciedlających rzeczywistość z niby-informacjami oderwanymi od rzeczywistości, albo mniej lub bardziej ją deformującymi

– Ekspansja sieci głębokiej (deep web) i ukrytej (dark net) powiązana ze wzrostem przestępczości i bezpośrednich zagrożeń dla państwa i jego obywateli.

– Rosnąca rola technologii informatycznych opartych na zastosowaniu sztucznej inteligencji, zwłaszcza w zakresie drążenia (mining) danych wielkoskalowych (big data), przetwarzania informacji oraz generowania syntetycznej wiedzy stanowiące podstawę analiz wywiadowczych

– Wielopoziomowość struktur decyzyjnych (w wymiarze wewnętrznym i międzypaństwowym); zwiększająca się liczba decydentów lub uczestników procesów decyzyjnych działających na różnych poziomach (państwa, organizacji międzynarodowych, przedsiębiorstw, grup eksperckich, społeczeństwa); krzyżowanie procesów decyzyjnych na poziomie wewnętrznym i międzynarodowym (także ponadnarodowym).

– Komercjalizacja bezpieczeństwa; rosnąca oferta usług analityczno-rozpoznawczych ze strony firm prywatnych; pokusa outsourcingu, czyli zlecania pewnych czynności analitycznych podmiotom prywatnym.

**b) zewnętrzne**

– Ekspansywna i agresywna strategia budowy/odbudowy mocarstwowej pozycji na arenie międzynarodowej Chin i Rosji; stały rozwój potencjału militarnego, zwłaszcza przez Chiny; ekspansywna (Chiny w Azji Wschodniej, Australii i Oceanii, Afryce; Rosja na Bliskim Wschodzie i Północnej Afryce), agresywna (Rosja na Ukrainie) i roszczeniowa (Chiny w rejonie Morza Południowochińskiego; Rosja na Dalekiej Północy) polityka zagraniczna; nadzwyczajny wzrost aktywności służb wywiadowczych obu państw.

– „Biznesowy” model bezpieczeństwa globalnego forsowany przez USA; forsowanie amerykańskich produktów i usług, zwłaszcza w sektorze obronnym, głównie w państwach sojuszniczych; zamiary administracji Trumpa uzależniania gwarancji bezpieczeństwa sojuszników USA (NATO) od zwiększenia nakładów na obronność.

– Rozwój technologii generowania, pozyskiwania, przetwarzania i analizy danych, tworzenie algorytmów generujących przekaz treściowy, ekspansja systemów sztucznej inteligencji i uczenia maszynowego, masowe wykorzystanie botów, inteligentnych asystentów, crowdsourcingu.

– Renacjonalizacja polityki bezpieczeństwa narodowego w obrębie wspólnoty euroatlantyckiej, utrudniająca skuteczną, wzajemnie korzystną współpracę; afirmacja interesu narodowego przez rządy USA, Wielkiej Brytanii i Francji.

– Kryzys tożsamości UE oraz impas w realizacji istniejących oraz wdrażaniu planowanych projektów wzmocnienia bezpieczeństwa Unii; mozolnie budowane zręby wspólnoty wywiadowczej UE (głównie w przeciwdziałaniu zagrożeniom terrorystycznym) stały się mało użyteczne wskutek niechęci do przekazywania istotnych informacji o zagrożeniach; deficyt zaufania między służbami wywiadowczymi państw członkowskich.

– Rozbudowa potencjału i zdolności wywiadowczych mocarstw regionalnych (Turcja, Iran, Indie, Brazylia); ponadregionalny i globalny zasięg ich aktywności wywiadowczej; intensywne działania w cyberprzestrzeni, zwłaszcza w mediach społecznościowych.

**c) wewnętrzne**

– Upartyjnienie państwa poprzez praktykę patronażu politycznego i wasalizacji struktur państwa przez rządzącą formację polityczną; zamknięcie dialogu z opozycją mogącego służyć dobrze pojętemu interesowi narodowemu; zwiększenie ryzyka błędów decyzyjnych wskutek odrzucania lub unikania krytyki.

– Brak spójnej i realistycznej strategii modernizacji i rozwoju państwa, społeczeństwa i gospodarki; niepewna perspektywa makroekonomiczna i finansowa, uzależniająca wzrost gospodarczy od koniunktury zewnętrznej i sztucznie generowanego popytu wewnętrznego; nacisk na pobudzenie konsumpcji na rynku wewnętrznym przez szczodre programy socjalne utrwala „pułapkę średniego rozwoju" i w dalszej kolejności zwiększa ryzyko nierównowagi finansów publicznych oraz osłabienia bezpieczeństwa ekonomicznego kraju.

– Niestabilność systemu administrowania sferą bezpieczeństwa wskutek częstych zmian prawnych i personalnych; zwiększenie ryzyka narażenia instytucji bezpieczeństwa państwa, w tym służb specjalnych na wrogie działania ze strony obcych służb wywiadowczych; obniżenie efektywności instytucji bezpieczeństwa oraz administracji publicznej wskutek braku ciągłości i systematyczności działań.

– Niezrównoważone nakłady na bezpieczeństwo państwa, preferujące elementy militarne kosztem organów bezpieczeństwa wewnętrznego i (częściowo) służb specjalnych; kosztowna budowa Wojsk Obrony Terytorialnej o wątpliwym wkładzie w realizację strategicznych interesów bezpieczeństwa państwa; kosztowne projekty rozbudowy infrastruktury wojskowej (tzw. Fort Trump) i zakupy uzbrojenia pod silnym wpływem Stanów Zjednoczonych. Pogłębiający się niedobór profesjonalnych zasobów ludzkich wskutek spadku jakości kształcenia, niezrównoważonych migracji oraz rosnącej atrakcyjności pracodawców prywatnych; spadek zainteresowania pracą w instytucjach i służbach bezpieczeństwa kraju, utrzymujące się wakaty; obniżenie poziomu przygotowania kandydatów do pracy w organach ładu i porządku publicznego, a także w służbach specjalnych.

**C. Cele:**

**1) Określenie strategicznych priorytetów i podstawowych obszarów działań służb specjalnych**, dostosowanych do założeń strategii bezpieczeństwa narodowego.

W pierwszej kolejności należy wypracować model realnego i efektywnego wspomagania procesów decyzyjnych na poziomie strategicznym państwa, mocno skorelowanego ze strategią bezpieczeństwa narodowego państwa. Wyznaczenie priorytetowych obszarów działań służb specjalnych i wywiadowczych na podstawie szczegółowej diagnozy stanu państwa oraz analizy strategicznej środowiska międzynarodowego umożliwi odpowiednią organizację systemu służb specjalnych, relokację zasobów ludzkich, technicznych i finansowych, a także sprecyzowanie potrzeb odnośnie do rozwoju i doskonalenia działań poszczególnych służb.

Ważnym obszarem działania jest wzmocnienie zdolności rozpoznania zagrożeń wewnętrznych, w tym w obszarze gospodarki i nauki, w kierunku zwiększenia umiejętności podejmowania skutecznych działań wyprzedzających pojawiające się zagrożenia oraz neutralizujących negatywne zjawiska i procesy. Budowa systemu krajowej oceny sytuacyjnej umożliwi uruchamianie mechanizmów monitorowania poziomu wdrażania strategii i korygowania jej założeń pod wpływem zmian w środowisku bezpieczeństwa. Skuteczne reagowanie na dynamiczne zmiany polityczne, społeczne, świadomościowe i technologiczne jest miarą sprawności systemu bezpieczeństwa wewnętrznego w wymiarze wykrywania, identyfikowania i zapobiegania zagrożeniom i źródłom ryzyka. Ma też bezpośredni wpływ na zwalczanie przestępstw i czynów naruszających ład publiczny dzięki włączeniu do oceny sytuacyjnej elementów wywiadu kryminalnego.

Kolejnym obszarem priorytetowym jest zewnętrzny wymiar bezpieczeństwa narodowego, odnoszący się do źródeł ryzyka, zagrożeń i szans powstających poza terytorium państwa polskiego lub mających charakter ponadnarodowy. We współczesnym usieciowionym, współpowiązanym świecie zasiedlonym przez liczne podmioty międzynarodowe, państwowe, pozapaństwowe i lokalne, ryzyko szybkiego powstawania, rozprzestrzeniania się i szerokiego oddziaływania zagrożeń jest szczególnie wysokie. Dlatego władze państwowe muszą mieć obszerną, aktualną i przydatną wiedzę o sytuacji międzynarodowej w kontekście wyzwań i zagrożeń. Rozwój zdolności wywiadowczych (rozpoznawczych i analitycznych) dotyczących sytuacji międzynarodowej jest koniecznym wymogiem efektywnego wspierania rządu w realizacji zasadniczych celów polityki zagranicznej państwa oraz w przeciwdziałaniu i zwalczaniu zagrożeń powstających poza terytorium RP.

Ostatnim priorytetowym obszarem działań służb specjalnych jest zastosowanie, rozwój i doskonalenie narzędzi, metod i technik czerpiących z najnowszych technologii informatycznych i komunikacyjnych. Postulowany system krajowej oceny sytuacyjnej musi powstać na bazie nowoczesnej infrastruktury umożliwiającej maksymalizację procesu pozyskiwania i przetwarzania informacji poprzez wykorzystanie systemów opartych na sztucznej inteligencji, wspomagających przygotowanie gotowych produktów analitycznych dla potrzeb decydentów. Obraz świata powstający w świadomości współczesnych mieszkańców kreowany jest w coraz większym stopniu przez media elektroniczne. Internet i media społecznościowe wpływają na zachowania i decyzje, także negatywne, zakłócające ład publiczny lub zagrażające interesom narodowym. Obecnie chaos medialny i zalew informacji mogą być częściowo opanowane wyłącznie przy zastosowaniu wielkoskalowych, zautomatyzowanych systemów informatycznych wspomaganych przez sztuczną inteligencję. Internet, a także jego ukryte warstwy (deep web i darknet), muszą być przedmiotem szczególnej uwagi służb specjalnych. To oznacza konieczność systemowych i organizacyjnych rozwiązań umożliwiających skuteczne działania wywiadowcze w infosferze i cyberprzestrzeni.

**2) Przebudowa instytucjonalna systemu służb specjalnych,** poprzez utworzenie Narodowej Wspólnoty Bezpieczeństwa, oddzielenie agencji wywiadowczych od służb dochodzeniowo-śledczych powiązanych z organami ścigania, a także wyposażenie organów ścigania w umiejętności wywiadowcze.

Na służbach specjalnych spoczywa obowiązek skutecznego działania na rzecz wspomagania procesów decyzyjnych będących w gestii najwyższych organów władzy państwowej odpowiedzialnych za bezpieczeństwo państwa polskiego, jego suwerenność, niezależność polityczną i integralność terytorialną. Równocześnie winny dysponować możliwościami przeciwstawienia się aktywności podmiotów zagranicznych, w szczególności obcych służb wywiadowczych, zagrażającej podstawowym interesom bezpieczeństwa narodowego, niezawisłości politycznej oraz ładu publicznego.

Struktura organizacyjna służb specjalnych powinna być przejrzysta, spójna i funkcjonalnie zintegrowana. Ma zatem odzwierciedlać prawny rozdział uprawnień i zadań, organizację i dystrybucję zasobów finansowych, materialnych i kadrowych, a także podległość służbową wobec organów władzy wykonawczej i odpowiedzialność wobec organów kontroli i nadzoru, w szczególności właściwej komisji parlamentarnej.

Należy ostrożnie podchodzić do nadmiernej jej rozbudowy, powoływania nowych instytucji i organów, zaopatrzonych w odpowiednie środki wyposażenia i utrzymania, by uniknąć niepotrzebnego „mnożenia bytów" i rozmycia odpowiedzialności za skutki ich działań.

Z uwagi na bezpośredni związek z polityką bezpieczeństwa państwa, służby specjalne powinny zostać podporządkowane Prezesowi Rady Ministrów, który w bieżących sprawach będzie działał przez ministra właściwego ds. służb specjalnych. Minister – członek Rady Ministrów będzie bezpośrednio podlegał premierowi oraz koordynował prace Narodowej Wspólnoty Bezpieczeństwa (tworzącą szczególnego rodzaju „wspólnotę wywiadowczą") oraz Krajowe Biuro Śledcze. Jako szef takiej wspólnoty, minister ds. służb specjalnych będzie odpowiedzialny za zespolenie działań poszczególnych służb oraz dostarczanie jednolitych produktów analizy wywiadowczej kluczowym decydentom, w szczególności premierowi oraz właściwym ministrom.

Jego umocowanie w Radzie Ministrów spowodowane jest wielorodnością współczesnych zagrożeń bezpieczeństwa narodowego, mających często charakter przekrojowy, międzyresortowy, a także odnoszący się do licznych aspektów bezpieczeństwa, nie tylko „twardego rdzenia", ale też bezpieczeństwa informatycznego, komunikacyjnego, żywnościowego, ekonomicznego, zdrowotnego itp. Mimo dużego ryzyka upolitycznienia działań ministra, bez względu na opcję ideologiczną i przynależność partyjną, realizacja zadań wywiadowczych wynikających z interesów bezpieczeństwa narodowego narzuca służebną i wykonawczą pozycję w stosunku do Prezesa Rady Ministrów i członków rządu.

Utrwalona praktyka nadawania służbom specjalnym uprawnień dochodzeniowo-śledczych spowodowała rozproszenie kompetencji między te służby a organy ścigania (głównie Policję) oraz trudności koordynacji działań w zakresie planowania, przygotowania i egzekwowania decyzji w trakcie czynności operacyjnych. Nakładanie się niektórych uprawnień szczególnych, impas decyzyjny albo wydłużający się łańcuch podejmowania decyzji wskutek niejasności i nieprecyzyjności przyjętych reguł, powodowały unikanie szybkich i zdecydowanych działań instancji decyzyjnych oraz rozproszenie odpowiedzialności za skutki (nie)podjęcia decyzji. Aby przerwać tę problematyczną praktykę, należy wyłączyć czynności dochodzeniowo-śledcze z zakresu obowiązków służb specjalnych, w szczególności Agencji Bezpieczeństwa Wewnętrznego, pozostawiając je wyłącznie w gestii organów ścigania. Spowoduje to następujące skutki:

- ABW zwolniona z obowiązku prowadzenia czynności o charakterze policyjnym będzie mogła skupić się na monitorowaniu terytorium RP z zadaniem wykrywania, interpretowania i dostarczania wiedzy o najpoważniejszych zagrożeniach bezpieczeństwa wewnętrznego Polski, włączając w to zadania kontrwywiadowcze, zorientowane na wrogą działalność agenturalną obcych służb.

- Czynności dochodzeniowo-śledcze związane z podejrzeniem popełnienia lub popełnieniem poważnych przestępstw zagrażających bezpieczeństwu wewnętrznemu oraz ładowi publicznemu wymagają wyodrębnienia specjalistycznej formacji zajmującej się śledztwami w sprawach dotyczących poważnej i zorganizowanej przestępczości kryminalnej, w tym o powiązaniach zagranicznych (nielegalny handel bronią i materiałami wybuchowymi; nielegalny obrót narkotykami; handel ludźmi, organami i tkankami; pranie pieniędzy; podrabianie i fałszowanie dokumentów, środków płatniczych, papierów wartościowych), a także zagrożeniach o charakterze politycznym (terroryzm, ekstremizm, radykalizm ideologiczny i religijny). Taka formacja o roboczej nazwie Krajowe Biuro Śledcze (KBS) zastąpiłaby Centralne Biuro Śledcze Policji (CBSP), Departament Postępowań Karnych ABW oraz biuro Generalnego Inspektora Informacji Finansowej (GIIF) wykorzystując ich doświadczenie, dorobek i zasoby kadrowe. Odrębnym i szczególnie traktowanym zagrożeniem bezpieczeństwa jest korupcja i działalność na szkodę interesów finansowych państwa. W ramach KBS funkcjonowałby wyodrębniony komponent organizacyjny w celu przeciwdziałania i zwalczania korupcji, który przejąłby zadania prewencyjne i dochodzeniowo-śledcze Centralnego Biura Antykorupcyjnego.

- Policja powinna uzupełnić działania prewencyjne i dochodzeniowo-śledcze o elementy rozpoznania wywiadowczego (intelligence-led policing). Ten model funkcjonuje w wielu państwach świata na różnych kontynentach, nie tylko w krajach o wysokim poziomie przestępczości i innych zagrożeń bezpieczeństwa, takich jak terroryzm czy ekstremizm. Podstawy wiedzy i umiejętności analizy wywiadowczej, metod i technik pozyskiwania informacji, korzystania z narzędzi informatycznych winny być przekazane i wpojone funkcjonariuszom Policji w podstawowym szkoleniu, a także kursach specjalistycznych przeznaczonych dla policjantów w zależności od charakteru i środowiska pełnionej służby.

**3) Inwestycja w służby wywiadowcze w celu ich profesjonalizacji i większej efektywności.** Wskutek rozwoju systemów masowej komunikacji, głównie internetu, konieczne jest zdecydowane zwiększenie nakładów na rozwój zdolności analitycznych, a także system zatrudnienia i szkolenia. Pion analityczny w poszczególnych agencjach i służbach włączonych do Narodowej Wspólnoty Bezpieczeństwa musi dysponować odpowiednimi zasobami technicznymi (oprzyrządowaniem, oprogramowaniem, dedykowanymi aplikacjami systemowymi), oraz odpowiednio wykwalifikowanym personelem. Infrastruktura techniczna analityki wywiadowczej powinna odpowiadać jak najwyższym standardom, czemu mają sprzyjać krajowe zdolności techniczne i technologiczne oraz możliwości pozyskania gotowych aplikacji z zewnątrz przy współpracy z kluczowymi sojusznikami RP.

Warunkiem profesjonalizacji służb specjalnych jest poprawa systemu naboru, szkolenia i doskonalenia zawodowego oraz warunków zatrudnienia poprzez jasno określoną ścieżkę awansu oraz przejrzysty i uczciwy system premiowania za szczególne osiągnięcia na służbie. Nabór do służb specjalnych, zwłaszcza agencji wywiadowczych, powinien być poprzedzony rozpoznaniem potencjalnych zasobów kadrowych na szeroko rozumianym rynku pracy. Należy wzmocnić i udoskonalić praktyki marketingowe, a jednocześnie rozwijać kontakty w środowiskach szczególnie predestynowanych do przyszłej pracy w służbach specjalnych: uczelniach wyższych, prywatnych firmach konsultacyjnych, ośrodkach analitycznych (think tankach). Większą uwagę należy poświęcić współpracy ze szkołami wyższymi, uczelniami technicznymi oraz uniwersytetami kształcącymi na kierunkach związanych z bezpieczeństwem, komunikacją i analizą informacji.

Szkolenie funkcjonariuszy służb specjalnych powinno zmierzać ku wąskiej specjalizacji. Oprócz ogólnego, wprowadzającego kursu w początkowym okresie zatrudnienia, należy uruchomić ścieżki szkolenia specjalistycznego pod kątem poszczególnych służb, zakresu ich działań oraz obszaru zainteresowań. W tym celu należy przebudować istniejący system szkolenia w kierunku koncentrycznej sieci ośrodków. Centralną instytucją szkolenia będzie Główny Ośrodek Szkolenia Służb Specjalnych (GOSSS), odpowiedzialny za ogólne przygotowanie ram metodyczno-dydaktycznych, programów szkolenia ogólnego i specjalistycznego, zabezpieczenia kadry wykładowców i instruktorów oraz wyposażenia i utrzymania infrastruktury systemu szkoleniowego. GOSSS będzie prowadził podstawowy kurs dla nowo przyjętych pracowników służb specjalnych. Wokół Głównego Ośrodka będą działać

Ośrodki specjalistycznego kształcenia pod kątem poszczególnych służb i agencji: Szkoła Wywiadu (podległa Szefowi Agencji Wywiadu), Szkoła Bezpieczeństwa Wewnętrznego (podległa szefowi Agencji Bezpieczeństwa Wewnętrznego), Szkoła Bezpieczeństwa Informacji (podległa Szefowi Agencji Bezpieczeństwa Informacji), Szkoła Cyberbezpieczeństwa (podległa Szefowi Agencji Bezpieczeństwa Informacji), Ośrodek Badań Terroryzmu (podległy Szefowi Narodowej Wspólnoty Bezpieczeństwa), Szkoła Analizy Kryminalnej (podległa Szefowi Krajowego Biura Śledczego). Te ośrodki będą oferować specjalistyczne przeszkolenie nowo zatrudnionych funkcjonariuszy, jak też kursy doskonalące dla pracowników z dłuższym stażem podnoszące kwalifikacje poprzez uwzględnienie zmian w środowisku bezpieczeństwa i innowacji technologicznych.

Pozyskanie pracowników o wysokich kwalifikacjach na rynku pracy wymaga zaoferowania atrakcyjnych i odpowiednio konkurencyjnych warunków zatrudnienia w porównaniu z ofertami podmiotów prywatnych, zwłaszcza przedsiębiorstw międzynarodowych w branży informatycznej, analityki biznesowej (business intelligence) i analizy konkurencji (competitive intelligence). Bez zapewnienia odpowiednio wysokich środków na zatrudnienie wysokiej klasy specjalistów, budowa maksymalnych zdolności rozpoznania i analizy danych i informacji na potrzeby służb specjalnych będzie wysoce utrudniona. Podobnie ważnym i odpowiedzialnym działaniem jest zapewnienie atrakcyjnej ścieżki kariery zawodowej poprzez spójny, przejrzysty i uczciwy system awansu i premiowania za szczególne osiągnięcia. Korzystne warunki zatrudnienia i wynagrodzenia muszą wiązać się z wysoką dyscypliną i odpowiedzialnością służbową funkcjonariuszy, w szczególności w zakresie bezpieczeństwa informacji niejawnych oraz tajemnic służbowych i państwowych. Dzięki temu nastąpi uszczelnienie przepływu informacji w obrębie służb specjalnych zapobiegające wyciekom „sensacji" oraz wynurzeniom sfrustrowanych funkcjonariuszy kontestujących warunki i okoliczności zatrudnienia.

**4) Rozwój współpracy międzynarodowej** i odbudowa zaufania w środowisku tradycyjnych zachodnich sojuszników i partnerów. Współczesne zagrożenia mają coraz częściej wymiar transgraniczny, międzynarodowy, toteż skuteczne im przeciwdziałanie i ich zwalczanie wymagają międzynarodowej współpracy właściwych organów państwowych. Polska jako członek Unii Europejskiej i NATO ma możliwość korzystania z różnych form i mechanizmów współpracy wywiadowczej. Formalne kanały wymiany informacji i współpracy wywiadowczej muszą jednak odpowiadać określonym wymogom i zasadom, przede wszystkim pewności prawa, odpowiedzialności za rzetelność przekazywanych treści, zapewnienia należytego poziomu bezpieczeństwa danych i informacji oraz, co najważniejsze, wzajemnego zaufania między współpracującymi służbami.

Współpraca wywiadowcza w ramach Unii Europejskiej jest ściśle związana ze specyficznym charakterem tej organizacji, przede wszystkim intensywnymi powiązaniami transgranicznymi między osobami i podmiotami gospodarczymi, swobodą podróżowania w strefie Schengen (dzięki zniesieniu kontroli na granicach wewnętrznych), przeniesieniem ciężaru kontroli ruchu osobowego na granice zewnętrzne. Korzyściom związanym ze swobodnym przepływem osób, towarów, usług i kapitałów towarzyszą negatywne zjawiska, takie jak szybkie i dość łatwe rozprzestrzenianie zagrożeń (terroryzm, przestępczość zorganizowana) oraz przeszkody we współpracy między państwami członkowskimi UE wynikające z różnic systemów prawa krajowego oraz, nierzadko, braku woli politycznej.

Niektóre zmiany prawno-administracyjne dokonane przez obecne władze RP zostały zakwestionowane przez Trybunał Sprawiedliwości UE jako niezgodne z prawem unijnym, a przez to podważające zasadę pewności prawa i niezależności władzy sądowniczej. Jest to bardzo poważna przeszkoda w realizacji praktycznej współpracy, zwłaszcza w tak istotnym obszarze, jak współpraca wywiadowcza. Bez przywrócenia ładu prawnego zgodnego z zasadami członkostwa Polski w UE zasada wzajemnego zaufania będzie działać w bardzo ograniczonym zakresie, co może pozbawić polskie służby specjalne dostępu do wielu informacji istotnych dla bezpieczeństwa państwa. Konieczna jest jak najszybsza odbudowa zaufania i roboczej współpracy poprzez naprawę naruszonych elementów polskiego prawa.

### D. Zadania

Przygotowanie całościowego rządowego planu reformy służb specjalnych – czas realizacji: 12 miesięcy.

Wdrożenie, na drodze zmian legislacyjnych i organizacyjno-instytucjonalnych, modelu nowoczesnego i efektywnego systemu służb specjalnych, w tym wywiadowczych, powiązanych z właściwymi organami bezpieczeństwa państwa – czas realizacji: 36 miesięcy.

Stworzenie spójnego systemu naboru, kształcenia i profesjonalizacji pracowników służb specjalnych w powiązaniu z jasną i uczciwą ścieżką awansu zawodowego – czas realizacji: 24 miesiące.

Odbudowa współpracy międzynarodowej na zasadzie wiarygodnej współpracy, pewności prawa i wysokiego poziomu zaufania – czas realizacji: 18 miesięcy.

### E. Rekomendacje:

- Wypracowanie modelu realnego i efektywnego wspomagania przez służby specjalne procesów decyzyjnych na poziomie strategicznym państwa, silnie skorelowanego ze strategią bezpieczeństwa narodowego państwa oraz strategicznymi wytycznymi sojuszów międzynarodowych, w których Polska uczestniczy.

- Przebudowa instytucjonalna systemu służb specjalnych, obejmująca oddzielenie agencji wywiadowczych od służb dochodzeniowo-śledczych powiązanych z organami ścigania, wzmocnienie i scalenie zdolności rozpoznania i analizy wywiadowczej, a także wyposażenie organów ścigania w umiejętności wywiadowcze.

- Profesjonalizacja służb specjalnych poprzez inwestycje w odpowiednie zasoby techniczne, poprawę systemu naboru, szkolenia i doskonalenia zawodowego pracowników, a także przejrzysty i uczciwy system zatrudnienia, premiowania i awansu służbowego.

- Odbudowa zaufania u tradycyjnych zachodnich sojuszników i partnerów w celu prowadzenia stałej, skutecznej i roboczej współpracy w zakresie identyfikowania źródeł zagrożeń bezpieczeństwa, wczesnego powiadamiania o bezpośrednich zagrożeniach oraz dzielenia się wiedzą o kluczowych aspektach bezpieczeństwa narodowego i międzynarodowego.

Skala czasowa realizacji zadań reformy służb specjalnych

| Lp. | Zadanie | 6 m-c | 12 m-c | 18 m-c | 24 m-c | 30 m-c | 36 m-c | 42 m-c | 48 m-c |
|---|---|---|---|---|---|---|---|---|---|
| 1. | Całościowy plan reform | 🟧 | 🟧 | | | | | | |
| 2 | Wdrożenie modelu | | | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 | 🟨 |
| 3 | System naboru i szkolenia | | | 🟦 | 🟦 | 🟦 | 🟦 | | |
| 4 | Współpraca międzynarodowa | | 🟩 | 🟩 | 🟩 | | | | |

**dr M. Kolaszyński**

## Budowa systemu nadzoru i kontroli jako warunek efektywnego działania służb specjalnych w demokratycznym państwie

### Wstęp

W Polsce nadal dużym wyzwaniem pozostaje kontrola i nadzór nad służbami specjalnymi. Jest to niepokojące, ponieważ w państwie demokratycznym prawidłowe mechanizmy w tym zakresie są warunkiem sine qua non efektywnego działania służb odpowiedzialnych za pozyskiwanie informacji o zagrożeniach dla bezpieczeństwa państwa. Mimo to od wielu lat brakuje istotnych reform w tym aspekcie. Już w 2014 r. Najwyższa Izba Kontroli informowała w sposób alarmujący o potrzebie stworzeniach mechanizmów nadzorczych. Takie samo wyzwanie stawia Strategia Bezpieczeństwa Narodowego z tego samego roku. Na potrzebę stworzenia realnych mechanizmów kontrolnych w zakresie ochrony praw i wolności jednostki zwrócił uwagę Trybunał Konstytucyjny – też w 2014 r. W wielu innych państwach Unii Europejskiej, w odpowiedzi na aktualne wyzwania, podjęto reformę systemu kontroli i nadzoru. W Polsce na długo przed 2014 r. zaoponowała w tej materii stagnacja. Z pewnością nie wynika ona z doskonałości wykształconych mechanizmów nadzorczych i kontrolnych.

### 1. Kontrola i nadzór służb specjalnych - czyli kogo?

Charakterystyczne dla Polski pojęcie „służb specjalnych" bierze swój początek w budowaniu mechanizmów nadzoru i kontroli. Jako określenie służb wywiadowczych pojawia się ono po raz pierwszy w Regulaminie Sejmu wraz z ustanowieniem w 1995 r. Sejmowej Komisji do spraw Służb Specjalnych. Wtedy określono, że pod tym pojęciem należy rozumieć Urząd Ochrony Państwa i Wojskowe Służby Informacyjne – ówczesne cywilne i wojskowe służby wywiadowcze. W ten sposób określono zakres podmiotowy prac nowej sejmowej komisji, a służby wywiadowcze coraz powszechniej zaczęto określać w naszym kraju jako służby specjalne. Rok później pojęcie to wprowadzono do ustawodawstwa w związku z powołaniem rządowego Kolegium do spraw Służb Specjalnych.

Na brak precyzji tego pojęcia zwracano uwagę już w latach 90. Specjalne czyli jakie? Nie jest to wcale tak oczywiste. Co ma wyróżniać służby specjalne na tle innych? W połowie lat 90. często utożsamiano je z wywiadem i kontrwywiadem. Tak też rozumiano to pojęcie podczas prac nad powołaniem sejmowej komisji stałej w 1995 r. Straciło ono na aktualności w 2006 r. wraz z włączeniem do katalogu służb specjalnych Centralnego Biura Antykorupcyjnego. Od tego momentu wyróżnikiem dla służb specjalnych przestały być zadania wywiadowcze i kontrwywiadowcze, a „specjalne" pozostały właściwie tylko niektóre instytucje kontroli i nadzoru nad nimi (np. sejmowa komisja i rządowe kolegium). Jako grupa służb: ABW, AW, CBA, SKW, SWW nie posiadają wyróżniających je zadań. Chociaż co do powszechnych odczuć nie traci chyba na aktualności opinia jednego z respondentów CBOS na temat jednej ze służb specjalnych (ABW): „na pewno na osiedlu ani na ulicy bezpieczeństwa nam nie zapewnią tylko właśnie, tak jak pani mówiła, gdzieś wyżej".[1]

W Polsce wyróżnikiem dla tych instytucji nie są też uprawnienia do pozyskiwania w sposób niejawny informacji. W istocie identyczne kompetencje posiadają służby policyjne, przede wszystkim Policja i Straż Graniczna. Służb

---

[1] CBOS, Rola Policji i innych służb w zapewnieniu bezpieczeństwa i porządku publicznego. Wizerunek Funkcjonariuszy Wybranych Służb Policji. Raport z badań FGI, Warszawa, grudzień 2008, s. 33.

specjalnych nie odróżnia sposób zorganizowana - podobnie jak w przypadku różnego typu policji są to struktury scentralizowane, zhierarchizowane i w dużym stopniu zmilitaryzowane. Nie trudno zauważyć absurdalność konkluzji, że służby specjalne to takie, które są w specjalny sposób kontrolowane i nadzorowane. Jest to wywrócenie normalnego porządku rzeczy, w którym to jakieś szczególne cechy danej instytucji: zadania, uprawnienia, może struktura organizacyjna decydują o szczególnych środkach kontrolnych i nadzorczych czy nawet szczególnych rozwiązaniach instytucjonalnych w tym zakresie.

Rozważania na temat pojęcia „służb specjalnych" nie posiadają jedynie akademickiego charakteru. Zwróćmy uwagę, że prowadzą one do fundamentalnego pytania: jakie instytucje mają być poddane systemowi szczególnej kontroli i nadzoru. Ze względu na jakie kryteria mają być wyróżnione te podmioty? Czy ze względu na wykonywane zadania, np. wywiad, kontrwywiad czy ze względu na przyznane uprawnienia do zdobywania informacji, np. czynności operacyjno-rozpoznawcze lub ze względu na inne kryterium, choćby mniejszą transparentność działań dla obywateli. To cechy wyróżniające te instytucje powinny być przesłanką dla szczególnych rozwiązań nadzorczo-kontrolnych. Jak te instytucje ostatecznie nazwiemy jest kwestią drugorzędną.

## 2. Kontrola i nadzór to konieczność

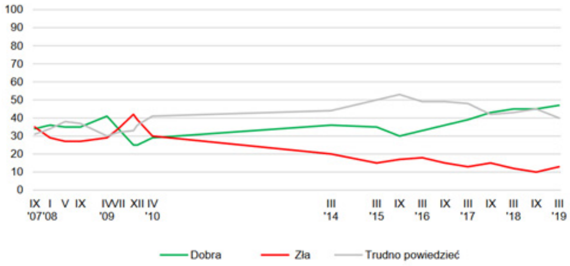
Dlaczego państwa demokratyczne przywiązują dużą wagę do kontroli nad służbami specjalnymi (wywiadowczymi) i tworzą w tym celu specjalne instytucje? W pierwszej kolejności zwróćmy uwagę na negatywny aspekt tego zagadnienia. Kontrolujemy te służby, ponieważ nie chcemy żeby prowadziły własną, autonomiczną wobec władz politykę. Więcej - chcemy żeby nie prowadziły żadnej polityki – żeby były neutralne politycznie, niezaangażowane w bieżące spory polityczne. Taka cywilna bariera przed ich aktywnością polityczną jest istotna ze względu na potencjał tych instytucji. Mają one uprawnienia pozwalające na głęboką ingerencję w życie obywateli i w bieżącą politykę. Ponadto najczęściej są usytuowane blisko ośrodka władzy. Do tego są zorganizowane w sposób niedemokratyczny, charakteryzujący się niewielką transparentnością, hierarchią, centralizacją czy działaniem na podstawie rozkazów. W tym negatywnym aspekcie cywilna kontrola jawi się jako bariera przed nadmiernym wpływem służb specjalnych na bieg spraw publicznych.

Podstawowym celem kontroli jest ulepszenie działalności danej instytucji i to stanowi aspekt pozytywy zagadnienia. Dzięki nadzorowi i kontroli jesteśmy w stanie ocenić, czy działania służb specjalnych są nie tylko skuteczne i efektywne, ale też legalne i praworządne. Umożliwia nam to ocenę, czy dobrze wykonują powierzone zadania i czy są one zgodne z wytycznymi rządzących - to cywilne władze mają decydować o strategicznych kwestiach związanych z organizacją i funkcjonowaniem służb specjalnych oraz rozliczać je z wykonywanych zadań. Chcemy żeby były one wkomponowane w konstytucyjne zasady ustrojowe, w tym w zorganizowany na ich podstawie system organów państwowych. Podobnie jak inne instytucje, zgodnie z art. 1 obowiązującej konstytucji, mają one służyć dobru wspólnemu wszystkich obywateli.

Problem w tym, że obywatel o służbach specjalnych wie niewiele. Z uwagi na powierzone zadania są to instytucje o niskiej transparentności. Duża część ich pracy jest objęta tajemnicą państwową i ujawnienie jej szczegółów opinii publicznej niweczyłoby skuteczne działania. Dlatego między innymi w państwie demokratycznym powoływane są instytucje kontrolne. Pracują one również pod rygorem ochrony informacji niejawnych. Jednak jedną z ich ról może być legitymizowanie działania służb specjalnych poprzez informowanie o ich działalności. W ten sposób pomagają one w budowaniu do nich zaufania i mogą zwiększyć ich rozpoznawalność.

Zaufanie obywateli do polskich służb specjalnych trudno dzisiaj jednoznacznie ocenić, ponieważ nie ma zbyt wielu aktualnych danych w tej materii. Pierwotnym problemem nadal wydaje się rozpoznawalność tego typu instytucji. Z przeprowadzonych przez CBOS 10 lat temu badań wynika, że aż 47% Polaków nie potrafiło ocenić działalności ABW (pozytywne opinie wyrażało 26% respondentów, negatywne 27%). W przypadku CBA wyniki tego samego badania wyglądały następująco: 36% respondentów nie potrafiło ocenić działalności tej instytucji, 25% oceniało pozytywnie, 39% negatywnie.[2] Wojskowe służby specjalne i Agencja Wywiadu nie zostały objęte badaniem. Cyklicznie CBOS pyta jedynie o ocenę działalności CBA. W marcu 2019 r. nadal duża część respondentów (40%) nie potrafiło ocenić pracy tej instytucji.

Ocena działalności Centralnego Biura Antykorupcyjnego w latach 2007-2019



Źródło: CBOS, Oceny działalności instytucji publicznych, Komunikat z badań nr 44/2019.

Trzeba podkreślić, że niewiedza Polaków na temat działania instytucji nie dotyczy tylko służb specjalnych. Nawet wśród konstytucyjnych organów podobne wyniki notują Trybunał Konstytucyjny (36%), Rzecznik Praw Obywatelskich (42%), Najwyższa Izba Kontroli (41%). W przeciwieństwie do tych instytucji służby specjalne mają jednak ograniczone możliwości samodzielnego budowania zaufania. Ponadto można wskazać na instytucje bliższe służbom specjalnym, których pracę Polacy potrafią ocenić. Tutaj najlepszym przykładem jest Policja – tylko 9% respondentów nie potrafiło ocenić działalności tej formacji mundurowej. Trudno przewidzieć, czy oraz na ile system kontroli i nadzoru może przyczynić się do większej rozpoznawalności służb specjalnych i być przyczynkiem do budowania zaufania do tych instytucji. Na pewno przy budowaniu takiego systemu trzeba mieć na względzie konieczność efektywnego komunikowania instytucji kontrolnych z opinią publiczną. W założeniu powinny one wystawiać świadectwo służbom specjalnym, że działają zgodnie z prawem, w interesie obywateli, w sposób profesjonalny, rzetelny i gospodarny. Takie świadectwo mogą wystawić tylko instytucje kontrolujące o dużym autorytecie.

### 3. Kto nadzoruje i kontroluje służby specjalne?

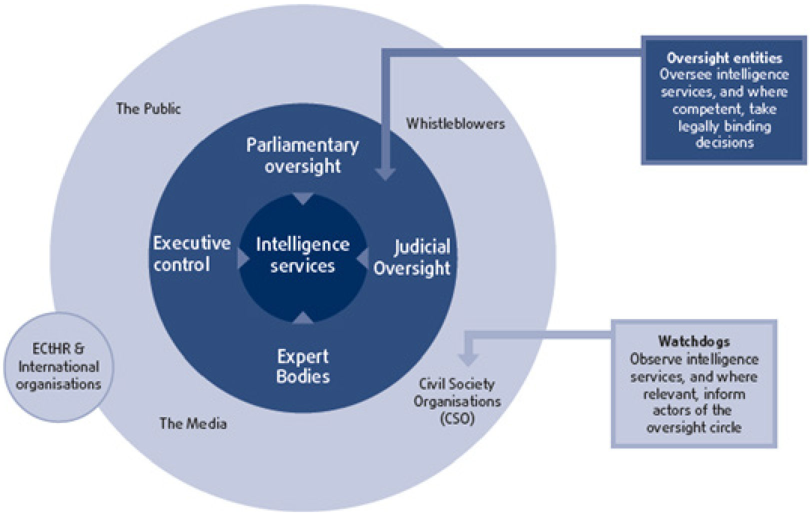
Wiele podmiotów sprawuje kontrolę i nadzór nad służbami specjalnymi w państwach demokratycznych. Nadzór, który poza kontrolą umożliwia merytoryczny wpływ na działalność instytucji, jest sprawowany z natury rzeczy przez wybrane organy egzekutywy. W przypadku kontroli na pierwszym miejscu wymieniany jest parlament, przy czym podkreśla się zarówno jego funkcję ustawodawczą przejawiającą się w stanowieniu podstawowych ram prawnych dla działalności w omawianej materii, jak i funkcję kontrolną. Z kolei organy władzy sądowniczej są wymieniane w kontekście wydawania zgody na zastosowanie uprawnień inwigilacyjnych oraz rozstrzygania w drodze orzecznictwa spraw związanych z działalnością służb specjalnych. Zwraca się też uwagę na rolę ombudsmanów oraz najwyższych organów kontroli (supreme audit institutions).

Poniższy schemat prezentuje instytucje zajmujące się nadzorem i kontrolą nad uprawnieniami inwigilacyjnymi służb specjalnych, co stanowi newralgiczną część działalności tych instytucji. Odnośnie do polskich rozwiązań jest to schemat uproszczony, ponieważ wśród instytucji kontrolnych nie znalazł się Rzecznik Praw Obywatelskich i Naj-

---

[2] CBOS, Opinie o działalności Prezydenta, Parlamentu, ZUS, ABW i CBA, Warszawa, grudzień 2009, ss. 6-9.

wyższa Izba Kontroli, które również zajmują się u nas tą materią. Z drugiej strony schemat zawiera wyspecjalizowane organy eksperckie (expert bodies), które nie występują w polskich rozwiązaniach w zakresie kontroli i nadzoru.



Źródło: European Union Agency For Fundamental Rights, Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update, Luxembourg 2017, s. 65

Na schemacie w zewnętrznym okręgu uwzględniona została kontrola prowadzona przez środki masowego przekazu oraz sprawowana w ramach społeczeństwa obywatelskiego. Zajmuje ona ważne miejsce w ocenie działalności służb specjalnych. Główną jej rolę upatruje się w ujawnianiu nieprawidłowości w działalności służb, informowaniu społeczeństwa oraz zachęcaniu do publicznej debaty na ich temat. W tym miejscu należy jeszcze raz podkreślić konieczności informowania obywateli o prowadzonej działalności kontrolnej i nadzorczej.

Rozważając kwestie instytucji kontroli i nadzoru powinniśmy zwrócić uwagę, że służby specjalne w wielu elementach podlegają kontroli i nadzorowi na tych samych zasadach co cała administracja rządowa. Służby specjalne są instytucjami w dużym stopniu wkomponowanymi w rozwiązania ustrojowe. Do takiej, nazwijmy to „standardowej" kontroli można zaliczyć działalność orzeczniczą Trybunału Konstytucyjnego. W tym wypadku nie ma żadnego wyjątku dla ustaw regulujących materię związaną z organizacją i funkcjonowaniem służb specjalnych. Nie jest też ograniczona działalność Rzecznika Praw Obywatelskich. Szereg innych organów musi w przypadku służb specjalnych stosować jedynie pewne modyfikacje proceduralne najczęściej związane z ochroną informacji niejawnych. Standardowe instytucje kontrolne są bardzo istotne, ponieważ pozwalają nam wkomponować służby specjalne w normalne funkcjonowanie państwa. Instytucje wyspecjalizowanej kontroli i nadzoru powinny być powoływane tylko wtedy, kiedy jest to uzasadnione i konieczne.

### 4. Nadzór - jak rząd korzysta ze służb specjalnych

Służby specjalne nie działają w instytucjonalnej próżni. Jak wspomniano wcześniej, powinny mieć zadania powierzane przez cywilne władze (np. zapotrzebowanie na informacje) i być z tych zadań rozliczane. Jak to się czasem określa – służby specjalne są instrumentem egzekutywy odpowiedzialnym za dostarczanie informacji o zagrożeniach dla bezpieczeństwa państwa. Odpowiedzialność za ich funkcjonowanie ponosi władza wykonawcza, dlatego musi mieć na nie wpływ. W tym miejscu dotykamy kluczowego problemu, jakim jest zakres wpływu rządu na służby specjalne. Ograniczone kompetencje nadzorcze oznaczają brak możliwości wykorzystania potencjału służb specjalnych i zagrożenie, że będą one same wyznaczać sobie zadania. Z kolei większa możliwość bezpośredniej ingerencji oznacza, że członkowie rządu (politycy) mogą mieć zbyt duży wpływ na ich funkcjonowanie, co może oznaczać ryzyko ich wykorzystywania do celów politycznych.

Jedną z barier dla takiego nieograniczonego wpływu ze strony polityków jest struktura organizacyjna polskich służb specjalnych. Wykształciła się ona w 1990 r. Założono wtedy podział monolitu, jakim był ówczesny resort bezpieczeństwa wewnętrznego na ministerstwo i autonomiczne służby. Ministerstwa stały się cywilne i odpowiedzialne za politykę bezpieczeństwa. Z kolei służby, takie jak Policja i UOP, miały być neutralne politycznie i fachowe. Policja i UOP były od tej pory jedynie nadzorowane przez ministra, co oznacza, że posiadały one autonomię, a na ich czele stali szefowie – centralne organy administracji rządowej. To rozwiązanie organizacyjne miało doniosłe znaczenie, ponieważ w założeniu pozwało na oddzielenie polityki od merytorycznej działalności służb specjalnych. Pod względem formalnym ten model obowiązuje w ustawodawstwie po dziś dzień. Nie zmienia tego bezpośredni nadzór premiera nad cywilnymi służbami specjalnymi sprawowany od 1997 r. Nadzorcy (obecnie: Prezes Rady Ministrów, Minister Obrony Narodowej, czasem minister koordynator do spraw służb specjalnych) nie powinni być bezpośrednio zaangażowani w merytoryczne kierowanie działalnością służb specjalnych, lecz odpowiadać za nadzór nad szefami tych instytucji. Mają oni prawo wkraczać w działalność szefów służb, gdy upoważniają ich do tego ustawy. Założeniem jest oddzielenie tego co cywilne i polityczne (ministerstwo) od tego co fachowe i neutralne politycznie (służby). W praktyce wyznaczenie tej granicy jest bardzo trudne, jeśli w ogóle możliwe.

Często zapomina się o tym, że nadzór jest limitowany a środki nadzorcze powinny być jasno wskazane w aktach normatywnych. Do typowych środków nadzoru egzekutywy w państwach Unii Europejskiej zaliczamy:

- formułowanie polityki, priorytetów i wytycznych wobec służb specjalnych;

- powoływanie i odwoływanie kierownictwa służb specjalnych;

- projektowanie budżetu;

- zatwierdzanie współpracy ze służbami specjalnymi innych państw.

Mając na uwadze powyższe wyliczenie można stwierdzić, że w Polsce władza wykonawcza dysponuje standardowymi środkami nadzorczymi. Warto wspomnieć, że w niektórych państwach (Francja, Irlandia, Luksemburg, Malta, Holandia i Wielka Brytania) egzekutywa odpowiada za wyrażanie zgody, czasem zarządzanie, niektórych środków inwigilacji obywateli. Takie rozwiązanie występowało też w przeszłości w Polsce i obecnie znajduje zastosowanie w przypadku niektórych metod operacyjnych.

Dlaczego zatem ten typowy jak na państwa UE nadzór wykazuje widoczne przejawy słabości. Konieczność zmian w tej materii została dostrzeżona w Strategii Bezpieczeństwa Narodowego z 2014 r., zgodnie z którą „konieczne jest skorygowanie systemu nadzoru nad nimi oraz zwiększenie ich zdolności do przygotowania zintegrowanego produktu informacyjnego”[3]. W tym samym roku kontrolę nadzoru nad służbami specjalnymi przeprowadził NIK. Jej wyniki nota bene zostały utajnione z uwagi na ochronę informacji niejawnych. Z upublicznionego komunikatu wynika, że „obowiązujące przepisy ograniczają możliwość sprawowania skutecznego nadzoru nad służbami specjalnymi przez Prezesa Rady Ministrów”[4]. W ocenie NIK „(...) w wielu

---

[3] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 48.

[4] Zob. Komunikat na oficjalnej stronie Najwyższej Izby Kontroli pt. „Nadzór nad służbami specjalnymi” zamieszczony w dziale „Aktualności”, URL: http://www.nik.gov.pl/aktualnosci/nadzor-nad-sluzbami-specjalny mi.html (data dostępu: 7.07.2019).

obszarach służby specjalne, pozbawione zewnętrznego cywilnego nadzoru, kontrolują same siebie”[5].

Dla wyjaśnienia tej słabości kluczowe wydają się dwa zagadnienia. Po pierwsze, niedostateczne uregulowanie procedury dostępu do informacji i dokumentów przez organy nadzorujące, dającej pogodzić się z koniecznością ochrony informacji niejawnych. Po drugie, ograniczony cywilny aparat administracyjny, który wspierałby organ nadzoru w jego pracy. Nadzór to nie jest zadanie dla jednej osoby, wymaga stałych struktur, procedur oraz przejrzystych zasad jego przeprowadzania. Tytułem przykładu można odwołać się do włoskich rozwiązań w zakresie nadzoru nad służbami specjalnymi. Jest to o tyle zasadne, że w wielu elementach przypominają one polskie rozwiązania. Służby są tam nadzorowane przez premiera – tak jak w Polsce cywilne służby specjalne. Szef rządu może przekazać większość swoich uprawnień nadzorczych ministrowi bez teki (w Polsce minister koordynator do spraw służb specjalnych) albo podsekretarzowi stanu. We Włoszech działa też międzyresortowe gremium odpowiedzialne za wyznaczanie strategicznych zadań dla służb specjalnych (w Polsce – Kolegium do Spraw Służb Specjalnych).

Zasadnicze znaczenie mają zaobserwowane różnice pomiędzy włoskim i polskimi rozwiązaniami. W Włoszech kluczową instytucją w systemie nadzoru jest Departament Wywiadu i Bezpieczeństwa (Il Dipartimento delle informazioni per la sicurezza, DIS). To on stanowi aparat urzędniczy mający zajmować się permanentnym nadzorem nad służbami specjalnymi. Do jego zadań należy koordynowanie wszystkich działań wywiadowczych, ocena rezultatów pracy służb specjalnych oraz przekazywanie istotnych informacji zebranych przez nie premierowi. DIS odpowiada za strategiczne analizy i oceny dla decydentów politycznych, zapewnia wymianę informacji między służbami specjalnymi i policyjnymi. Ponadto kontroluje, przy pomocy jednej ze swoich jednostek organizacyjnych, działalność służb. Dba o komunikację międzyinstytucjonalną i promowanie kultury bezpieczeństwa. Powyższe stanowi tylko część katalogu zadań tej instytucji. Jest to jednak wystarczające, aby oddać jej charakter.

DIS dysponuje rozbudowaną strukturą organizacyjną. Na jego czele stoi Dyrektor Generalny mianowany przez Prezesa Rady Ministrów. W skład departamentu wchodzą następujące biura: biuro odpowiedzialne za kontrolę służb specjalnych (Ufficio centrale ispettivo, UCI), biuro odpowiedzialne za koordynację i zarządzanie danymi, które są w posiadaniu służb wywiadowczych (Ufficio centrale degli archi vi, UCA), biuro, które zajmuje się administracyjną ochroną tajemnic państwowych, w tym przyznawaniem lub cofaniem poświadczenia bezpieczeństwa (Ufficio centrale per la segretezza, UCSe) oraz szkoła wywiadu (Scuola di formazione). W Polsce brakuje takich rozbudowanych struktur odpowiedzialnej za stałą ocenę i wykorzystanie pracy służb specjalnych.

Istotna w ramach nadzoru jest konieczność koordynacji między służbami specjalnymi oraz innymi instytucjami bezpieczeństwa narodowego. Warto wspomnieć, że krytyczne uwagi NIK dotyczyły również rodzimej instytucji koordynującej - Kolegium do spraw Służb Specjalnych. NIK stwierdził, że podejmowane przez premiera w trakcie posiedzeń tego gremium decyzje, formułowane jako polecenia między innymi dla szefów służb specjalnych, w dużej części nie były następnie weryfikowane. Zdaniem NIK „brak systemowego rozwiązania służącego monitorowaniu stopnia realizacji ocen i opinii Kolegium, jak również decyzji Przewodniczącego Kolegium pozbawia te organy możliwości bieżącej analizy wykorzystania zajętych przez Kolegium stanowisk oraz ich przydatności do realizacji zadań przez służby specjalne”[6].

Podkreślmy też, że ściśle rzecz biorąc nadzór nie jest niezależny. Rząd, z uwagi na odpowiedzialność polityczną za

---

[5] Ibidem.
[6] Ibidem.

działanie służb specjalnych, nie zawsze będzie zainteresowany ujawnianiem niewygodnych dla siebie faktów. Jednak skutecznie sprawowany nadzór stanowi nieodzowny przyczynek do zewnętrznej kontroli. Rolą egzekutywy jest informowanie o działalności służb specjalnych i o tym jak są wykorzystywane jako instrument rządzenia. Skuteczny nadzór to dopiero podstawa dla budowy systemu zewnętrznej kontroli.

### 5. Parlament – polityczna kontrola służb specjalnych

Rola parlamentu w kontroli nad służbami specjalnymi musi być rozpatrywana w kontekście jej polityczności. Podstawowe pytanie brzmi, czy taką kontrolę można oddzielić od doraźnego nacisku partyjno-politycznego na służby specjalne. Już na wstępie trzeba zaznaczyć, że parlament, w Polsce zgodnie z obowiązującą konstytucją przede wszystkim Sejm, sprawuje kontrolę nad Radą Ministrów. Stąd co najmniej równie istotny jak kontrola służb specjalnych jest stały monitoring tego, jak te służby są nadzorowane przez rząd i poszczególnych ministrów. Nieocenioną zaletą kontroli parlamentarnej jest jej uniwersalność, czyli możliwość oceny różnych aspektów zagadnienia: prawnych, politycznych, społecznych i ekonomicznych. Wadą – z punktu widzenia niezależności kontroli – jest jej polityczność.

Parlament daje możliwość do chyba najbardziej wszechstronnej oceny nadzoru nad służbami specjalnymi. Jednocześnie w ograniczonym stopniu nadaję się do kontroli działalności samych służb, ponieważ debata parlamentarna dająca możliwość do tak wieloaspektowej ocen nie pozwala na zachowanie tajemnicy państwowej. Ta ostania z kolei stanowi podstawę wielu działań służb specjalnych. Stosowane przez nie metody pracy bardzo często objęte są tajemnicą państwową. Aby Sejm miał dostęp do takich informacji muszą być stworzone szczególne ramy instytucjonalne, których celem jest umożliwienie dostępu do niektórych tajemnic. Niezależnie od zastosowanych rozwiązań, zawsze będą one stały w sprzeczności z debatą parlamentarną, która jest jawna. W przypadku kontroli parlamentarnej mamy do czynienia z dwoma rodzajami kontroli: tradycyjną (standardową) i wyspecjalizowaną, wykonywaną przez Sejmową Komisję do spraw Służb Specjalnych. Istota tej drugiej sprowadza się do wyłonienia przez Sejm niewielkiej komisji, która w jego imieniu sprawuje kontrolę nad służbami specjalnymi. Dzięki temu, że jest to stosunkowo niewielkie grono osób, można jego członkom powierzyć niektóre tajemnice służb.

Do tradycyjnych środków kontroli zaliczamy takie jak: interpelacja, zapytanie poselskie, debata parlamentarna. Oczywiście nie pozwalają one na bieżącą i stałą kontrolę działalności służb specjalnych. Dają jednak możliwość rozliczania członków Rady Ministrów z nadzoru nad służbami specjalnymi – z tego jakie cele wyznaczają tym instytucjom oraz w jaki sposób rozliczają je z wykonywanych zadań. Tradycyjne środki kontroli pozwalają na debatę na temat stałej, konsekwentnej polityki wobec służb specjalnych. Nie powinno się lekceważyć tego rodzaju kontroli. Jeśli miałby zostać wypracowany konsensus wokół reformy i zarządzania służbami specjalnymi, to musiałoby się to stać na forum parlamentu. Wynika to choćby z jego doniosłych funkcji ustawodawczych i kreacyjnych.

W Sejmie działa Sejmowa Komisja do spraw Służb Specjalnych, która ma dostępu do niektórych tajemnic służb specjalnych. Z formalnego punktu widzenia komisja jest jednym ze stałych organów Sejmu o charakterze wewnętrznym i pomocniczym. W rzeczywistości jej rola polega na reprezentowaniu Sejmu. Można stwierdzić, że w praktyce ustrojowej bardzo często nie tyle pomaga ona Sejmowi a go wyręcza, ze wszystkimi tego negatywnymi konsekwencjami, o czym w dalszej części. O samodzielności tej komisji świadczy ustawowe zakotwiczenie oraz własne uprawnienia i obowiązki, które wykonuje ona niezależnie. Przykładowo podejmowane przez nią uchwały w sprawie wyrażania opinii co do kandydatów na szefów służb i ich zastępców mają charakter ostateczny. Sejm nie ma możliwości ich zmiany albo uchylenia, nie może również uchwalić własnego stanowiska w miejsce opinii komisji. Z uwagi na ochronę dostępu do informacji niejawnych utrudniona jest też merytoryczna kontrola pracy tej komisji.

W państwach Unii Europejskiej podobne wyspecjalizowane komisje występują powszechnie – brakuje ich jedynie w Irlandii i na Malcie. Na Słowacji i w Rumunii funkcjonuje nawet więcej niż jedna wyspecjalizowana komisja parlamentarna. Różny jest katalog zadań komisji poszczególnych państwach. Z reguły zakres przedmiotowy ich prac jest bardzo szeroki. Jednak kluczowy w tym wypadku jest dostęp do informacji na temat działalności służb specjalnych. W żadnym państwie UE komisje parlamentarne nie mają nieograniczonego dostępu do informacji wywiadowczych. W Polsce informacje na temat działalności operacyjnej są chronione przez same służby specjalne i zgodnie z ustawami mogą, ale nie muszą być udzielane posłom. Uzasadnione jest to ochroną źródeł informacji w tym osób, które je przekazują. Sejm w praktyce czerpie umiarkowane korzyści z prac komisji. Jest ona zorganizowana i działa w sposób, który przypomina bardziej realia służb specjalnych niż debaty parlamentarnej. Kluczowy w tej sytuacji staje się dostęp do informacji. O tym co może być udostępnione komisji, a co nie, decydują szefowie służb specjalnych. Jest to w dużej mierze ich uznaniowa decyzja, która jest ostateczna - nie podlega weryfikacji nadzorcy, np. premiera. Można stwierdzić, że ostatecznie o tym co będzie kontrolowane decydują podmioty kontrolowane. Jednak przy obecnym stanie kultury politycznej trudno odpowiedzialnie postulować za obligatoryjnym przekazywaniem wszystkich informacji sejmowej komisji. Polityczność kontroli parlamentarnej jest trudną do przezwyciężenia przeszkodą dla budowania niezależnych mechanizmów kontrolnych.

Polska kontrola parlamentarna nad służbami specjalnymi stoi w pewnym rozkroku. Siłą parlamentu jest jawność, debata, ścieranie różnych wizji i próba wypracowania kompromisu. Natomiast kontrola nad służbami specjalnymi bardzo często jest redukowana na forum Izby do próby poznawania „tajemnic" tych instytucji, co z góry jest skazane na niepowiedzenie. Z drugiej strony skupianie się na tym co niejawne nie przyczynia się do inicjowania debaty na temat polityki i nadzoru rządu wobec służb specjalnych. W ostatecznym rozrachunku Sejm takiej poważnej debaty nie prowadzi, a komisja próbując zgłębić „tajemnicę" służb nie kontroluje, a raczej je afirmuje. W obecnej kadencji Sejmowa Komisja do spraw Służb Specjalnych wydała 130 opinie i 10 dezyderatów. Zdecydowana większość opinii – około 100 – nie zawiera żadnej treści merytorycznej i ogranicza się do, jak mantra powtarzanego, stwierdzania „komisja postanowiła pozytywie zaopiniować...". Na drugim miejscu pod względem liczebności znajdują się opinie niejawne. Na trzecim te, które postulują zwiększenie budżetów poszczególnych służb specjalnych. Można też wskazać kilka opinii odnoszących się do projektów aktów normatywnych. Dodajmy do tego, że Sejmowa Komisja do spraw Służb Specjalnych nie wypracowała od 1995 r. żadnego jawnego raportu o stanie służb specjalnych i nadzoru nad nimi, które mógłby zainicjować debatę na ten temat. W wielu państwach Unii Europejskiej normą jest obowiązek publikowania rocznych raportów ze swojej działalności. Często są to obszerne dokumenty. Jeśli zestawimy dorobek Sejmowej Komisji do spraw Służb Specjalnych z inną rodzimą instytucją odpowiedzialną za kontrolę, np. Najwyższą Izbą Kontroli, to obraz działalności komisji będzie raził skromnością, nie tyle nawet pod względem ilościowym, co merytorycznym.

### 6. Niezależne organy kontroli[7]

Podstawową zaletą władzy sądowniczej i organów ochrony prawa jest ich bezstronność, czyli to co stanowi esencję kontroli. W tej grupie znajdują się takie organy jak: Rzecznik Praw Obywatelskich oraz Najwyższa Izba Kontroli. Wśród podmiotów o konstytucyjnych gwarancjach niezależności znajdują się również sądy (powszechne, administracyjne i wojskowe) oraz Trybunał Konstytucyjny.

Warto dodać, że w Polsce nie ma wyspecjalizowanej, niezależnej instytucji, która zajmowałaby się jedynie kontrolą działalności służb specjalnych. W wielu państwach powstają tego typu zewnętrzne wobec egzekutywy organy. Obecnie w 16 państwach UE funkcjonuje jeden bądź więcej takich organów dedykowanych dla służb specjalnych. Mają one szereg zalet. Po pierwsze są niezależne, ponieważ mają zagwarantowaną neutralność polityczną, czym odróżniają się od wyspecjalizowanej kontroli parlamentarnej. Z uwagi na swoją niezależność mają szerokie uprawnienia dostępu do informacji na temat działalności operacyjnej służb specjalnych. Po drugie, instytucje te działają permanentnie, a kontrola służb specjalnych jest ich podstawowym zadaniem. Dzięki temu mogą kontrolować ich bieżącą działalność. Ma to szczególną zaletę w przypadku kontroli działalności operacyjnej służb. Trzecia zaleta wynika po części z drugiej. Permanentna działalność wymusza wysoki stopień specjalizacji wokół zagadnień związanych z pracą służb specjalnych. Chodzi przy tym zarówno o znajomość aspektów prawnych, jak i kwestii technicznych związanych z inwigilacją. Zazwyczaj organy tego typu posiadają też własny personel administracyjny.

Sposób powoływania członków tego typu instytucji jest bardzo różny. Przykładowo w Belgii i Bułgarii są oni powoływani przez parlament, w Chorwacji przez wyspecjalizowaną komisję do spraw wewnętrznych i bezpieczeństwa narodowego, w Grecji przez konferencję przewodniczących parlamentu. Są państwa, w których za wybór odpowiedzialna jest egzekutywa, np. Austria, Dania (za wyjątkiem przewodniczącego), Szwecja, Wielka Brytania. Liczba członków tego typu instytucji również nie przedstawia żadnej reguły, np. w Belgii – 3 członków, w Bułgarii – 5 członków, w Chorwacji i Grecji – 7 członków.

W wielu państwach organy tego typu mają zagwarantowaną własną administrację, np. w Niemczech Komisja G-10 jest obsługiwana przez 13 osobowy sekretariat właściwy również dla Parlamentarnego Gremium Kontrolnego, w Grecji zapewniony jest 38 osobowy aparat urzędniczy. Z kolei w Belgii jako personel pomocniczy występuje 5 osobowa służba śledcza złożona m.in. z przedstawicieli służby wywiadowczej i służby policyjnej oraz 16 osobowy personel administracyjny. W Holandii, poza 12 osobowym personelem, została utworzona sieć współpracy złożona z ekspertów, m.in. naukowców, regularnie doradzających komisji przy przygotowaniu specjalistycznych raportów. Zapewnia to stały dostęp do wiedzy w tematyce inwigilacji.

Niezwykle istotne są wymogi stawiane członkom tego typu eksperckich organów. Trudnym zagadnieniem pozostaje ustalenie zakresu wiedzy, jakiej należy oczekiwać od tych osób i na podstawie jakich kryteriów ją weryfikować. W niektórych państwach określono wymogi dotyczące wykształcenia, np. w Chorwacji niektórzy członkowie muszą być absolwentami: prawa, nauk politycznych, elektrotechniki. W Belgii w komisji musi zasiadać co najmniej dwóch absolwentów prawa. Z kolei w Austrii wymagana jest wiedza z zakresu praw i wolności jednostki. Poza wykształceniem często spotykanym wymogiem jest praktyka prawnicza (np. Austria, Grecja), w tym przede wszystkim uprawnienia sędziowskie. Są jednak państwa, w których poza doświadczeniem prawniczym wymaga się od niektórych członków wiedzy z zakresu techniki i technologii informacyjnych. Tak jest przykładowo we Francji. Inną spotykaną możliwością jest zasiadanie w tych gremiach byłych parlamentarzystów.

---

[7] W tej części wykorzystałem swoje rozważania zamieszczone w komentarzu Niezależne organy eksperckie – sposób na kontrolę działalności inwigilacyjnej służb specjalnych i policyjnych? Zamieszczonym na stronie Fundacji Instytut Bezpieczeństwa i Strategii, https://fibis.pl (data dostępu: 2.08.2019).

Do przykładowych zadań i uprawnień tego typu organów należą:

- zatwierdzanie środków inwigilacyjnych;
- rozpatrywanie skarg (obywateli) na działalność służb specjalnych;
- możliwość żądania dokumentów i informacji od służb specjalnych;
- wydawanie opinii dla władzy wykonawczej lub ustawodawczej, m.in. dotyczących procesu legislacyjnego;
- możliwość wszczynania dochodzeń z własnej inicjatywy i na wniosek innych organów.

Należy podkreślić, że powoływanie wyspecjalizowanych organów eksperckich do kontroli działalności inwigilacyjnej nie jest wymaganym standardem w ramach niezależnej kontroli nad służbami specjalnymi. Europejski Trybunał Praw Człowieka dopuszcza możliwość kontrolowania działalności inwigilacyjnej w taki sposób. Jednak jako podstawowe rozwiązanie wskazuje kontrolę sądowniczą nad tego typu działalnością służb (Sprawa Klass i inni przeciwko Niemcom: wyrok ETPCz z dnia 18 listopada 1977 r.).

W Polsce kontrola nad czynnościami operacyjno-rozpoznawczymi – bo tak ustawowo określa się działalność inwigilacyjną – pozostawia wiele do życzenia. Koronny przykład: nadal żaden niezależny organ nie rozpatruje skarg obywateli na tego typu działalność służb specjalnych i policyjnych. Nie tylko w tym punkcie nie został wykonany wyrok Trybunału Konstytucyjnego z 30 lipca 2014 r. Nadal brakuje skutecznej kontroli zewnętrznej udostępniania służbom danych telekomunikacyjnych, pocztowych i internetowych. Przypomnijmy, że we wspomnianym orzeczeniu Trybunał wymaga niezależnej kontroli każdego udostępnienia danych telekomunikacyjnych. Wynika z tego konieczność wprowadzenia kontroli jednostkowej, zindywidualizowanej.

Obecnie nie mamy w Polsce takiej kontroli, a ta która jest ustawowo zagwarantowana w dużym stopniu wydaje się iluzoryczna. Jest ona sprawowana przez sądy okręgowe jedynie ex post i wyrywkowo. Brak kontroli uprzedniej i jednostkowej to nie jedyny mankament obecnych rozwiązań. Dodajmy, że nie wiemy właściwie nic na temat sposobu przeprowadzenia kontroli. Akty normatywne nie zawierają nawet podstawowych rozstrzygnięć odnośnie procedury kontrolnej. Więcej – organ kontroli nie ma nawet możliwości rzetelnego ustalenia stanu faktycznego, tj. rzeczywistej oceny ilości danych pozyskanych przez poszczególne służby oraz sprawuje kontrolę jedynie nad samym uzyskiwaniem danych. Poza kontrolą pozostaje gromadzenie i obowiązek zniszczenia danych. W ocenie obecnego zakresu kontroli łatwiej określić czego sąd nie może. Brakuje między innymi możliwości monitorowania treści pozyskanych danych, co w konsekwencji uniemożliwia ocenę sądu, czy sięganie po owe dane było, zgodnie z konstytucyjnymi zasadami ograniczania praw i wolności jednostki, konieczne i proporcjonalne. Ostatecznie, sądy mają niewielkie możliwości dokonywania realnych czynności kontrolnych. To szefowie służb decydują o tym, co znajdzie się w sprawozdaniu i co będzie podlegać kontroli. Nie trzeba przekonywać, że z niezależną kontrolą ma to niewiele wspólnego.

Na pierwszy rzut oka nieco lepiej wygląda weryfikacja innego uprawnienia inwigilacyjnego – kontroli operacyjnej przez sądy powszechne i wojskowe. Mamy w tym wypadku do czynienia z kontrolą uprzednią. Jednak i w tej sytuacji sąd nie ma możliwości zapoznania się z całością materiałów dotyczących badanego przypadku. Może on zbadać jedynie to, co przedstawią mu służby. Ten typ kontroli został ustanowiony w 2001 r. Więcej możemy zatem powiedzieć na temat praktyki tej kontroli, o której nieco mówią nam udostępniane publicznie statystyki. Wiemy z nich, że w rodzimych realiach sądy akceptują około 99% wniosków szefów służb specjalnych o zastosowanie kontroli operacyjnej. Wynik imponujący i stawiający nas jednocześnie w rozterce: nieomylne służby czy iluzoryczność kontroli?

Niestety coś niepokojącego łączy oba rodzaje kontroli sądowej – tę ustanowioną w 2001 r. nad kontrolą operacyjną oraz tę ustanowioną w 2016 r. nad danymi telekomunikacyjnymi, internetowymi i pocztowymi. Zwróćmy uwagę, że w obu wypadkach ustawodawca nie zagwarantował trwałych struktur organizacyjnych w ramach sądów, które miałyby zajmować się tego typu działalnością. Ponadto nie zapewnił dodatkowych środków finansowych i kadrowych przeznaczonych na ten cel. Innymi słowy: ogranicza to możliwość desygnowania sędziów, dla których kontrola działalności inwigilacyjnej byłaby aktywnością pierwszoplanową. Sędziów, którzy mogliby w tej materii się wyspecjalizować i którzy byliby wyposażeni w odpowiedni aparat pomocniczy (urzędniczy). Zapewnienie odpowiednich struktur administracyjnych pozwalających na permanentną kontrolę jest uzasadnione skalą zjawiska: w 2018 r. służby specjalne i policyjne pozyskały ponad 1,3 mln danych. Jeśli chodzi o kontrolę operacyjną, to tylko w przypadku Policji złożono w tym samym roku około 8,5 tys. wniosków.

Zarówno Trybunał Konstytucyjny, jak i Europejski Trybunał Praw Człowieka nie przesądzają formy organizacyjnej przeprowadzania kontroli działalności inwigilacyjnej służb specjalnych i policyjnych. Ma być to jednak kontrola niezależna i rzeczywista. W państwach Unii Europejskiej wykształciły się dwa modele takiej weryfikacji działalności inwigilacyjnej. W 12 państwach Unii Europejskiej, podobnie jak w Polsce, odpowiadają za nią sądy. Alternatywą dla takiego rozwiązania jest powoływanie niezależnych organów eksperckich dedykowanych dla służb specjalnych. Obecnie, co zostało już wspomniane, w 16 państwach UE występuje to drugie rozwiązanie. Warto zwrócić uwagę na organy eksperckie. Z jednej strony pozwala to na poszukiwanie alternatywy dla sądowej kontroli. Z drugiej strony, taka analiza wiele mówi nam na temat możliwości usprawnienia rodzimych rozwiązań. Kluczowe dla poprawnego funkcjonowania organów eksperckich są oprócz niezależności: profesjonalizm, ustawiczne działanie, zaplecze administracyjne i eksperckie. Tego samego wymaga poprawnie zaprojektowana kontrola sądownicza – aby sądy mogły zajmować się weryfikowaniem działalności inwigilacyjnej muszą zostać stworzone możliwości organizacyjne i funkcjonalne dla tego typu działalności. Można rozważać powołanie w Polsce organu eksperckiego – to jedna z możliwości. Druga możliwość to reforma uprawnień władzy sądowniczej, która powinna zapewnić stałą, profesjonalną i zabezpieczoną trwałą strukturą organizacyjną kontrolę nad działalnością inwigilacyjną służb specjalnych i policyjnych. Musi być to też kontrola, która – jak w przypadku organu eksperckiego – pozwala wskazać jasno strukturę i osobę odpowiedzialną za jej przeprowadzenie. Pozostając przy status quo w tej materii, skazujemy się w Polsce na kontrolę iluzoryczną.

## 7. System kontroli i nadzoru nad służbami specjalnymi?

Tytułem podsumowania warto zastanowić się nad tym, czy w Polsce istnieje system kontroli i nadzoru nad służbami specjalnymi. Przypomnijmy, że system to pewna struktura, zorganizowana w sposób uporządkowany według określonych założeń i zasad. Ponadto elementy takiego systemu pozostają ze sobą w silniejszych lub słabszych powiązaniach organizacyjnych i funkcjonalnych.

W Polsce kontrola i nadzór nad polskimi służbami specjalnymi nie spełnia powyższego warunku organizacyjnej jedności. Obejmuje ona co prawda różne instytucje, ale nie tworzą one logicznej całości. Ostatecznie nie jest to system komplementarny, pozwalający na kontrolę i nadzór nad wszystkimi istotnymi aspektami działalności służb specjalnych. W tej sytuacji trudno mówić o dopenianiu się tych instytucji i tworzeniu przez nie efektu synergii. Wydaje się, że optymistycznie możemy założyć, że w Polsce istnieją jedynie elementy takiego systemu, jednak brak jest rozwiązań systemowych.

Aby taki system stworzyć potrzeba odpowiedzi na szereg pytań. Można wskazać na kluczowe problemy w tym względzie:

- brak klarownie wyróżnionych instytucji, które powinny podlegać systemowi kontroli i nadzoru. Normatywna definicja służb specjalnych nie spełnia tego warunku. Założeniem wstępnym dla budowy całościowego systemu powinno być podjęcie decyzji, czy budować go tylko dla służb wywiadowczych, czy także dla służb wywiadowczo-policyjnych;

- system kontroli i nadzoru powinien zwiększać rozpoznawalność służb specjalnych i budować zaufanie do tych instytucji. Poszczególne instytucje nadzorcze i kontrole muszą informować o swojej aktywności. Zapewnia to otwartą debatę na temat służb specjalnych;

- skuteczny nadzór i kontrola nie może narażać państwa na ujawnienie informacji niejawnych. Wymaga to budowy procedur dostępu do nich dla osób godnych zaufania, które będą ponosiły indywidualną odpowiedzialność za ewentualne ujawnienie tajemnic państwowych;

- muszą zostać uregulowane granice nadzoru sprawowanego przez polityków. Organy nadzorcze muszą mieć zapewnione rozbudowane cywilne zaplecze merytoryczne i administracyjne, co umożliwi stałą kontrolę służb specjalnych oraz koordynację ich pracy z innymi instytucjami bezpieczeństwa.

- do budowy systemu powinny być wykorzystane standardowe środki kontroli dostępne w ramach porządku konstytucyjnego (np. parlament, Najwyższa Izba Kontroli, Rzecznik Praw Obywatelskich). Pozwala to na budowanie kultury politycznej i organizacyjnej wokół służb specjalnych i zwiększa szanse na otwartą debatę na ich temat;

- system powinien zapewniać efektywną i niezależną kontrolę ekspercką nad działalnością operacyjną służb specjalnych. Za taką kontrolę mogą odpowiadać sądy przygotowane pod względem organizacyjnym i merytorycznym, w tym z fachowym zapleczem albo specjalne do tego celu powolne organy eksperckie;

- budowa systemu kontroli i nadzoru musi uwzględniać aktualne wyzwania związane z masową inwigilacją, nowymi technologiami oraz koniecznością kontroli międzynarodowej współpracy służb wywiadowczych.

**Rekomendacje:**

- klarowne wyodrębnienie służb podlegających kontroli i nadzorowi;

- organy kontroli i nadzoru powinny szerzej informować o swojej działalności;

- organy nadzorcze i kontrolne muszą mieć zapewnione rozbudowane zaplecze merytoryczne i administracyjne;

- budowa stałej i niezależnej kontroli eksperckiej nad działalnością operacyjną służb specjalnych i policyjnych.

## Cz. Rybak

## Model systemu ochrony tajemnicy państwowej jako efektywne narzędzie zabezpieczania interesów państwa

Jednym z warunków przyjęcia Polski do NATO była zmiana obowiązującej od 1982 r. (okres stanu wojennego - sic!) ustawy o tajemnicy państwowej i służbowej. W styczniu 1999 r. Sejm RP uchwalił ustawę o ochronie informacji niejawnych, która diametralnie zmieniała system pojęciowy dot. ochrony tajemnic państwa. Ustawa nadal dzieliła tajemnice na państwowe (“ściśle tajne” i “tajne”) i służbowe (“poufne” i “zastrzeżone”), zawierała jednak katalog informacji objętych tajemnicą “ściśle tajne” oraz “tajne” oraz opisywała tryb uzyskiwania dostępu do tajemnic. Wprowadzała również pojęcie “służby ochrony państwa”. Dokument zawierał wiele nieścisłości i błędów prawnych, m.in. w 2001 r. jedną z noweli wprowadzono możliwość realizacji postępowania odwoławczego i skargowego w przypadku odmowy wydanie osobie sprawdzanej poświadczenia bezpieczeństwa lub jego cofnięcia, a kolejną nowelą (z 2005 r.) - możliwość zawieszenia i umorzenia postępowania. Po dwudziestu trzech nowelizacjach, w sierpniu 2010 r., parlament uchwalił nową - obowiązującą do dziś - ustawę o ochronie informacji niejawnych[1] [zwaną dalej “Ustawą”]. Aktualnie przygotowywana jest nowa ustawa, która ma wejść w życie od 1 października br. - jest to jednak wciąż projekt, wobec którego nie została uruchomiona ścieżka legislacyjna.

Obowiązująca od dziewięciu lat Ustawa wprowadziła kilka zasadniczych i szereg pomniejszych zmian. Poniżej przedstawiono cztery - w opinii autora - najpoważniejsze. Uznano, iż najważniejszym organem odpowiedzialnym za system ochrony informacji niejawnych w kraju jest Szef ABW (wcześniej ABW i SKW były podmiotami równoległymi). Po pierwsze, Szef ABW pełni funkcję krajowej władzy bezpieczeństwa, czyli nadzoruje system ochrony informacji niejawnych w stosunkach RP z innymi państwami i organizacjami międzynarodowymi. Po drugie, ABW nadzoruje funkcjonowanie systemu ochrony informacji niejawnych we wszystkich krajowych jednostkach organizacyjnych, z wyłączeniem jednostek podległych i nadzorowanych przez MON oraz ataszatów obrony i żołnierzy w służbie czynnej, które nadzoruje SKW.

Kolejna zmiana polegała na rezygnacji z podziału informacji niejawnych na tajemnicę państwową i tajemnicę służbową. Zrezygnowano z umieszczenia w ustawie wykazu informacji stanowiących informacje niejawne o klauzuli “ściśle tajne” i “tajne” na rzecz weryfikacji poziomu tajności owej informacji na podstawie ogólnej definicji dot. poziomu szkody dla Rzeczpospolitej Polskiej. I tak, informacjom niejawnym nadaje się klauzulę “ściśle tajne”, gdy ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla RP, “tajne” - poważną szkodę, “poufne” - spowoduje szkodę, a “zastrzeżone” - może mieć szkodliwy wpływ.

Trzecia zmiana to odejście od sztywnych okresów ważności nadanych klauzul niejawności. Wprowadzono możliwość określenia z góry daty lub wydarzenia, po którym nastąpi zmiana lub zniesienie klauzuli tajności, jak również możliwość odrębnego klauzulowania poszczególnych części dokumentu. Wprowadzono też obowiązek okresowego przeglądu dokumentów niejawnych (nie rzadziej niż raz na 5 lat) w celu określenia, czy informacje w nich zawarte nadal spełniają ustawowe warunki, będące podstawą do nadania im klauzuli tajności. W zależności od wyniku przeprowadzonego przeglądu, klauzula może zostać utrzymana, zmieniona lub też całkowicie zniesiona.

---

[1] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz.U z 2019 r., poz. 742)

Ostatnią z najważniejszych zmian jest oparcie systemu bezpieczeństwa fizycznego i teleinformatycznego na procesie szacowanie ryzyka.

Nowa ustawa nie zmieniła jednak żadnych zasad związanych ze strukturalnym nadzorem nad systemem ochrony informacji niejawnych. Nadzór nad systemem posiadają służby specjalne - ABW i SKW, przy czym - jak już wspomniano wyżej - Szef ABW pełni funkcję krajowej władzy bezpieczeństwa.

Tadeusz Koczkowski, przedstawiciel Krajowego Stowarzyszenia Ochrony Informacji Niejawnych, oceniając nową ustawę o ochronie informacji niejawnych, twierdził w roku 2011, iż ”Twórcy nowej ustawy zakładają że będzie ona miała istotny wpływ na usprawnienie funkcjonowania systemu ochrony informacji niejawnych w Polsce, w tym na zwiększenie jego elastyczności, pośrednio również na sektor finansów publicznych, zwłaszcza na budżet państwa i budżet jednostek samorządu terytorialnego, na konkurencyjność gospodarki i przedsiębiorczość, bezpieczeństwo państwa, czy jakość demokracji.”[2] Ale czy to założenie było uzasadnione?

Szefowie ABW i SKW są centralnymi organami administracji rządowej. Strukturalnie Szef ABW podlega Prezesowi Rady Ministrów. Szef SKW podlega Ministrowi Obrony Narodowej, z zastrzeżeniem uprawnień Premiera. Nadzór nad działaniami ABW i SKW w zakresie ochrony informacji niejawnych pełni bezpośrednio Prezes Rady Ministrów. W Ustawie przewidziano kilka elementów sprawowania przez niego nadzoru:

- rozstrzyganie sporów dot. zawyżenia lub zaniżenia klauzuli tajności, jeśli stroną sporu jest ABW lub SKW (Premier do tego zadania może upoważnić Szefa Kancelarii Prezesa Rady Ministrów, sekretarza stanu albo podsekretarza stanu w Kancelarii Prezesa Rady Ministrów),
- prowadzenie kontroli prawidłowości realizacji postępowań sprawdzających, kontrolnych postępowań sprawdzających oraz postępowań bezpieczeństwa przemysłowego realizowanych przez ABW lub SKW,
- rozpatrywanie odwołań od decyzji o odmowie wydania poświadczenia bezpieczeństwa, o cofnięciu poświadczenia bezpieczeństwa albo o umorzeniu postępowania sprawdzającego lub kontrolnego postępowania sprawdzającego wydanych przez ABW lub SKW,
- rozpatrywanie odwołań od decyzji o odmowie wznowienia postępowania oraz od decyzji o odmowie uchylenia decyzji wydanej w wyniku postępowania wydanych przez ABW lub SKW,
- rozpatrywanie odwołań od decyzji o odmowie wydania świadectwa bezpieczeństwa przemysłowego, decyzji o cofnięciu świadectwa oraz decyzji o umorzeniu postępowania bezpieczeństwa przemysłowego.

Poza nadzorem bezpośrednim sprawowanym przez Premiera (lub Ministra Koordynatora) nadzór nad ABW i SKW sprawuje również Parlament (Komisja ds. Służb Specjalnych), Kolegium ds. Służb Specjalnych oraz inne organy państwa np. NIK lub sądownictwo administracyjne.

Decyzje Prezesa Rady Ministrów, wynikające z odwołań w wymienionych wyżej sprawach z zakresu ochrony informacji niejawnych, mogą być przedmiotem kontroli Wojewódzkiego Sądu Administracyjnego w Warszawie oraz NSA.

W 1999 r., w związku z wejściem w życie pierwszej ustawy o ochronie informacji niejawnych, w Urzędzie Ochrony Państwa powstał Departament Ochrony Informacji Niejawnych, który był strukturalną częścią Departamentu Kontrwywiadu. W późniejszym okresie Departament ten

---

[2] T. Koczkowski „Rewolucja czy ewolucja w ochronie informacji niejawnych. Ułatwienie czy utrudnienie dla Przedsiębiorców”, Chemik, 2011

został wyodrębniony jako jednostka niezależna od Kontrwywiadu i w takiej formie funkcjonuje nadal. Ponadto zagadnieniami bezpieczeństwa przetwarzania informacji niejawnych w systemach teleinformatycznych zajmuje się Departament Bezpieczeństwa Teleinformatycznego. Oba departamenty mają swoje jednostki (wydziały, sekcje) w poszczególnych Delegaturach oraz Wydziałach Zamiejscowych. W SKW zadania podzielone są podobnie, systemowo - ochroną informacji niejawnych zajmuje się Zarząd V, sferą bezpieczeństwa teleinformatycznego - osobna jednostka Biuro Bezpieczeństwa Cybernetycznego.

ABW i SKW realizują zadania z zakresu ochrony informacji niejawnych głównie na podstawie Ustawy. W raporcie z działalności ABW za rok 2014, szef ABW stwierdza, iż "Działania podejmowane przez ABW mają głównie charakter prewencyjny, oparty na minimalizowaniu zagrożeń w obszarze ochrony informacji niejawnych oraz ustaleniowo-wyjaśniający. Ich celem jest zapobieganie przypadkom ujawniania informacji niejawnych podmiotom do tego nieuprawnionym, a gdy do tego dojdzie – ustalenie osób za to odpowiedzialnych."[3] Podobnie działa SKW.

„Działania ABW w zakresie nadzoru nad systemem ochrony informacji niejawnych, zgodnie z właściwością Agencji, są realizowane w obszarach bezpieczeństwa:

- osobowego – rozumianego jako procedury sprawdzeniowe służące weryfikacji wiarygodności osób ubiegających się o uzyskanie dostępu do informacji niejawnych i uniemożliwieniu takiego dostępu osobom niedającym rękojmi zachowania tajemnicy oraz szkolenia osób przed udzieleniem im dostępu do informacji klauzulowanych;

- przemysłowego – ujmowanego jako procedury sprawdzeniowe wobec firm ubiegających się o wydanie świadectwa bezpieczeństwa przemysłowego;

- fizycznego – w tym określanie standardów i zapewnianie fizycznych warunków do ochrony informacji niejawnych oraz kontrola ich przestrzegania;

- teleinformatycznego – polegającego na certyfikacji urządzeń i akredytacji systemów teleinformatycznych."[4]

Poza instytucjami państwowymi i samorządowymi, które realizując swoje ustawowe działania przetwarzają informacje niejawne, dostęp do informacji niejawnych niezbędny jest szeregowi przedsiębiorców, których działalność związana jest z dostawami towarów lub świadczeniem usług na rzecz tych instytucji. Wszystkie te przedsiębiorstwa muszą uzyskać tzw. świadectwa bezpieczeństwa przemysłowego, które uprawniają je do dostępu do informacji niejawnych o odpowiedniej klauzuli oraz do przetwarzania tych informacji w odpowiednim zakresie.

Corocznie, jak wynika z informacji publikowanej na stronie www.abw.gov.pl[5] oraz www.skw.gov.pl[6], ABW wydaje ok. 200-300 świadectw bezpieczeństwa przemysłowego, SKW ok. 10-40. Aktualnie w kraju ok. 100 przedsiębiorców posiada dostęp do informacji niejawnych o klauzuli "ściśle tajne", ok. 600 do "tajne", w tym ok. 350 również do klauzuli "NATO SECRET" i "SECRET UE/EU SECRET", a ok. 60 do "ESA SECRET". Pozostali, w ilości ok. 1000, posiadają dostęp do informacji niejawnych o klauzuli "poufne" i odpowiadających jej klauzulom organizacji międzynarodowych. Incydentalnie zdarza się, iż służby ochrony państwa dokonują odmowy wydania świadectwa bezpieczeństwa przemysłowego.

---

[3] Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2014 r., ABW, Warszawa, 2015

[4] tamże

[5] https://bip.abw.gov.pl/bip/informacje-niejawne-1/nadzor-nad-systemem-oc/bezpieczenstwo-przemys/148,BEZPIECZENSTWO-PRZEMYSLOWE.html, 08.06.2019

[6] https://www.skw.gov.pl/bezpieczenstwo-przemyslowe.html, 08.06.2019

Z uwagi na fakt, iż zasadniczą rolę w systemie ochrony informacji niejawnych w kraju odgrywa ABW, w dalszej części opracowania uwzględniona zostanie jedynie rola ABW.

Aktualnie zgłoszonych do ABW jest 1.477 Kancelarii Tajnych[7], z których w 993 przechowuje się dokumenty o klauzuli “ściśle tajne”, a w 484 - “tajne”.

Ponadto ABW wydaje rocznie ok. 9-11 tys. poświadczeń bezpieczeństwa. Odmów wydania poświadczeń bezpieczeństwa jest ok. 30 rocznie. Należy pamiętać, iż poza nielicznymi wyjątkami - ABW wydaje poświadczenia bezpieczeństwa do najwyższych klauzul: “Tajne” i “Ściśle tajne”.

ABW, w ramach realizacji zadań związanych z bezpieczeństwem teleinformatycznym, corocznie wydaje ok. 700 świadectw akredytacji systemów TI, ok. 600 certyfikatów ochrony elektromagnetycznej, ok. 10 certyfikatów ochrony kryptograficznej oraz ok. 1,4 tys. certyfikatów zgodności.

Kontrola systemu ochrony informacji niejawnych prowadzona przez ABW realizowana jest w sposób planowy - ok. 50 kontroli rocznie oraz w sposób doraźny - do 10 kontroli doraźnie w roku. Bardzo rzadko kontrole te skutkują składaniem przez ABW zawiadomień o podejrzeniu popełnienia przestępstwa - przykładowo, w roku 2014 zostało złożone jedno tego rodzaju doniesienie do Prokuratury.

Realizując masowe sprawdzenia osób i podmiotów gospodarczych przed dopuszczeniem ich do dostępu do informacji niejawnych, ABW pozyskuje ogromną ilość informacji. Ankieta Bezpieczeństwa Osobowego liczy 25 stron i zawiera bardzo szczegółowe informacje o sytuacji rodzinnej, współmieszkańcach, historii życia zawodowego i osobistego, karalności, kontaktach zagranicznych, stanie zdrowia, nałogach oraz sytuacji majątkowo-finansowej (w tym również osób prowadzących wspólne gospodarstwo domowe). Weryfikacja tych informacji przez ABW trwa znacznie dłużej niż zapisane w Ustawie, instrukcyjne 3 miesiące.

Procedura ta jest nieefektywna, bowiem opiera się na błędnym założeniu, że zgromadzone informacje na temat przeszłości danej osoby pozwolą ocenić, czy daje rękojmię zachowania tajemnicy czy nie. Ocena końcowa ma charakter arbitralny.

Należy jednak zadać sobie pytanie, czy analiza danych historycznych ma zasadnicze znaczenie dla tzw. rękojmi zachowania tajemnicy? Trzeba pamiętać, że poświadczenia są wydawane na kilka lat - w przypadku dostępu do informacji o klauzuli „Poufne” na 10 lat - i w tym okresie ABW praktycznie w ogóle nie weryfikuje sytuacji osoby dopuszczonej do dostępu do tych informacji. Po co zatem tak ogromna porcja informacji „podarowana” ABW przez samych zainteresowanych? Ilość odmów wydania poświadczeń bezpieczeństwa to zaledwie kilka promili z ogólnej liczby postępowań - trudno zatem nie odnieść wrażenia, iż ABW zbiera te informacje zupełnie bezcelowo, albo - niestety - może zbierać je do innych celów niż sprawy związane z ochroną informacji niejawnych.

Tomasz Borkowski, były dyrektor Biura Kolegium ds. Służb Specjalnych, w jednym ze swoich artykułów przedstawił opinię dot. pokusy wykorzystywania informacji uzyskanych w toku prowadzonych postępowań: „Jeszcze w końcu lat 90-tych ubiegłego wieku, w okresie wdrażania pierwszej ustawy o ochronie informacji niejawnych, a zarazem nawiązywania współpracy w ramach NATO, przedstawiciele partnerskich służb lub innych instytucji realizujących postępowania sprawdzające w krajach „starego” NATO przestrzegali nas przed pokusą wykorzystywania informacji zdobytych w postępowaniu do innych celów, gdyż byłoby to sprzeczne ze standardami państwa prawa, a zarazem podważałoby wiarygodność służby. Pamiętam rozmowę ze starszym oficerem jednej z natowskich służb, który mówił: „Jeżeli w toku waszych procedur wykryjecie obcego szpiega, musicie mieć możliwość niezwłocznego poin-

---

[7] http://www.abw.gov.pl/download/1/2458/Wykazkancelariitajnychlipiec2018.xlsx, 09.06.2019 r. (aktualizacja na dzień 7.05.2019 r.)

formowania właściwych organów. Ale jeżeli wasza służba zacznie wykorzystywać wrażliwe informacje przekazywane przez ludzi do werbunku agentury, stracicie wiarygodność, a ludzie będą się bali z wami rozmawiać i będą unikać udzielania wam jakichkolwiek istotnych informacji".”[8]

Skrajnie odmiennie podchodzi się do dostępu do informacji niejawnych o klauzuli „Zastrzeżone" - tu w ogóle nie prowadzi się jakiegokolwiek sprawdzenia osoby dopuszczanej, nie sprawdza się nawet, czy była karana albo czy nie toczy się przeciwko niej postępowanie karne lub karno-skarbowe. Ponieważ nie wydaje się poświadczeń do dostępu do informacji zastrzeżonych, a jedynie Kierownik Jednostki Organizacyjnej wydaje stosowne upoważnienia - całość odpowiedzialności za zachowanie rękojmi spoczywa na owym kierowniku. Dla jasności, Kierownika Jednostki Organizacyjnej nie sprawdza - nawet w minimalnym stopniu - nikt. A informacji o klauzuli „Zastrzeżone" jest w obiegu zdecydowanie najwięcej.

Niestety duża uznaniowość i brak realnej kontroli może prowadzić do błędów i nadużyć - to służby decydują, komu poświadczenie wydać, a komu je cofnąć. Przykłady z ostatnich lat, opisywane przez media, to np. cofnięcie przez służby poświadczenia bezpieczeństwa byłemu wiceszefowi ABW płk. Jackowi Mące[9], kandydatowi do Sejmowej Komisji ds. Służb Specjalnych Antoniemu Macierewiczowi[10] czy też dyrektorowi Departamentu Zwierzchnictwa nad Siłami Zbrojnymi w Biurze Bezpieczeństwa Narodowego gen. Jarosławowi Kraszewskiemu[11].

ABW w 2012 r. twierdziła, iż „W zakresie realizacji postępowań sprawdzających nowa ustawa wprowadziła większą swobodę oceny zasadności podejmowania niektórych czynności, do tej pory obligatoryjnych. Zmiany te spowodowały przyspieszenie realizacji procedur, tym bardziej, że nowa ankieta bezpieczeństwa osobowego, zawierająca bardziej precyzyjne informacje, pozwala na wcześniejszą weryfikację danych."[12] Okres trwania procedury sprawdzającej nie został jednak skrócony, a sprawdzenia, które w założeniu nie miały być obligatoryjne, takimi się stały. W efekcie postępowania sprawdzające trwają nawet po kilkanaście miesięcy.

W przypadku świadectw bezpieczeństwa przemysłowego, za otrzymanie którego firmy płacą po kilkadziesiąt tysięcy złotych, Ustawa przewiduje ciągły monitoring danych dotyczących przedsiębiorcy. W ciągu 30 dni należy bezwzględnie informować ABW o zmianach danych zawartych w kwestionariuszu bezpieczeństwa, i to zarówno podczas rozpatrywania wniosku, jak i w okresie jego ważności. Poza tym, w zależności od stopnia świadectwa, ABW weryfikuje zastosowane środki bezpieczeństwa fizycznego oraz akredytuje systemy teleinformatyczne, w których przetwarzane będą informacje niejawne.

Oczywiście można by uznać, iż jest to naturalna troska o bezpieczeństwo informacji niejawnych - niestety wiąże się to ze zbyt dużą uznaniowością ABW. Brak możliwości odwołania się (w niektórych aspektach) oraz iluzoryczna kontrola sądowa powodują, iż to ABW decyduje o tym, jaki podmiot będzie miał dostęp do rynku związanego z dostępem do informacji niejawnych.

Przykładowo, w art. 48 ust. 4 Ustawy zawarto informację, iż od odmowy udzielenia akredytacji systemu teleinformatycznego nie służy odwołanie. Przepis nie zawiera nawet wzmianki o tym, iż taka odmowa powinna być uzasadniona. W tej sytuacji przedsiębiorca nie ma możliwości złożenia kolejnego - poprawionego - wniosku, gdyż nie wie, jakie uwagi do poprzedniego miała ABW. Podobnie sytuacja wygląda w zakresie możliwości wynikającej z art. 48 ust. 12,

---

[8] https://osluzbach.pl/2019/05/23/borkowski-ustawa-m-kaminskiego-jak-w-dyktaturze/ (10.06.2019)

[9] https://dorzeczy.pl/kraj/46501/Byly-szef-ABW-wygral-w-sadzie-z-premier-i-obecnym-szefem-Agencji.html, 12.06.2019

[10] https://www.tvn24.pl/wiadomosci-z-kraju,3/macierewicz-bez-tajemnic,73844.html, 12.06.2019

[11] https://www.tvp.info/42956550/glowny-prezydencki-doradca-ds-wojska-odchodzi-z-bbn, 13.06.2019

[12] Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w roku 2011, ABW, Warszawa, 2012

kiedy to ABW „w szczególnie uzasadnionych przypadkach" ma prawo nakazać wstrzymanie przetwarzania informacji niejawnych w systemie teleinformatycznym posiadającym akredytację bezpieczeństwa teleinformatycznego do przetwarzania informacji niejawnych o klauzuli „Zastrzeżone". Uznaniowo również ABW może określić okres ważności akredytacji systemu teleinformatycznego - do 5 lat (art. 48 ust. 2 Ustawy), bez podania jakichkolwiek kryteriów.

W przypadku postępowań związanych z uzyskaniem świadectwa bezpieczeństwa przemysłowego, przedsiębiorca, w sytuacji otrzymania decyzji o umorzeniu postępowania bezpieczeństwa przemysłowego, odmowie wydania lub cofnięciu świadectwa może skierować odwołanie do Prezesa Rady Ministrów (art. 69 ust. 1 Ustawy). Jak uznają autorzy wydawnictwa "Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych", jeśli podstawą odmowy był zarzut niezorganizowania w terminie 6 miesięcy od daty wszczęcia postępowania kompleksowego systemu ochrony informacji niejawnych w zakresie zidentyfikowania i wdrożenia metodyki szacowania ryzyka, a co za tym idzie - brak możliwości właściwej oceny ryzyka ze względu na przyjęte w niej kryteria oceny oraz brak gwarancji ciągłości zarządzania ryzykiem w przypadku wprowadzenia zmian w zasobach systemów teleinformatycznych, to sąd może albo uchylić decyzję i przekazać ją podmiotowi realizującemu postępowanie do ponownego rozpatrzenia, albo uznać skargę za bezzasadną. W sytuacji, gdy podstawą odmowy jest zarzut niewłaściwego przyjęcia kryteriów oceny ryzyka i braku możliwości stosowania przyjętej metodyki szacowania dla zachowania ciągłości zarządzania ryzykiem związanym z przetwarzaniem informacji niejawnych w systemach teleinformatycznych, sąd może dopuścić środek dowodowy w postaci dowodu z opinii biegłego. Biegłym w tym zakresie może być jednak tylko obecny lub były funkcjonariusz ABW lub SKW, a to czyni wątpliwą jego bezstronność. [13]

Wymienieni autorzy konkludują, iż "podmioty nadzorujące system bezpieczeństwa informacji niejawnych mają uprawnienia władcze o charakterze uznaniowym, co w praktyce może utrudniać jednostkom organizacyjnym (przedsiębiorcom) realizację racjonalnej i elastycznej ochrony informacji niejawnych (...)" oraz "(...) procedury odwoławcze w zakresie akredytacji systemów teleinformatycznych, jak i bezpieczeństwa przemysłowego nie gwarantują skutecznej ochrony praw podmiotów zobowiązanych. W dalszym ciągu nowe przepisy [Ustawy - przyp. autora] zdają się uprzywilejowywać podmioty nadzorujące krajowy system bezpieczeństwa informacji niejawnych. Nowe przepisy nie przyczyniają się też do zauważalnego wzrostu transparentności działania państwa i jego aparatu."[14] Podobnie wypowiedział się Dariusz Gregorczyk recenzując książkę Sławomira Zalewskiego - "Ochrona informacji niejawnych. Wybrane zagadnienia bezpieczeństwa osobowego": "Prymat czynników formalnych w prowadzonych procedurach może być elementem negatywnym i może doprowadzić do sytuacji wykorzystania tajemnicy przeciwko obywatelowi przez państwo. Dobrze skonstruowane procedury oparte na przejrzystych przepisach powinny jednak stać się skutecznym narzędziem ochrony informacji niejawnych, praw obywatela, a więc w rezultacie sprzyjać wzrostowi bezpieczeństwa państwa."[15]

Trudno nie zgodzić się z przedstawionymi wyżej poglądami. Aktualnie prowadzone są prace nad nową ustawą o ochronie informacji niejawnej. Zgodnie z zapisami w projekcie, ma ona wejść w życie w dniu 1 października br. Nie sposób wskazywać na szczegółowe zapisy tego projektu, które mogą oczywiście zostać zmienione w toku prac parlamentarnych - wymowa projektu wskazuje na kolejny oręż, dzięki któremu służby będą mogły zdobywać wiele precyzyjnych informacji o obywatelach i podmiotach funkcjonujących w ramach systemu ochrony informacji niejawnych. Dodatkowo zachowają, a nawet zdecydowanie zwiększą, uznaniową decyzyjność w zakresie dopuszczenia

---

[13] Za M. Jabłoński, T.Radziszewski " Bezpieczeństwo fizyczne i teleinformatyczne informacji niejawnych", Presscom Sp. z o.o., Wrocław 2012

[14] Tamże

[15] Przegląd bezpieczeństwa wewnętrznego 13/15, ABW, Warszawa, 2015

do przetwarzania informacji niejawnych zarówno osób, jak i przedsiębiorców, a także będę mieć wpływ na obsadę stanowisk pełnomocników ds. ochrony informacji niejawnych oraz kierowników kancelarii tajnych.

Fundacja Instytut Bezpieczeństwa i Strategii przedstawiła w maju br. na swoim portalu www.fibis.pl szereg uwag dot. funkcjonującego w Polsce systemu ochrony informacji niejawnych[16]. Niestety projekt nowej ustawy nie rozwiązuje żadnego z przedstawionych problemów, raczej je pomnaża.

Jak wygląda system ochrony informacji niejawnych w innych krajach? Analizując poszczególne systemy w krajach europejskich zauważa się, iż w niektórych z nich za system ten odpowiadają zupełnie niezależne od służb specjalnych urzędy. I tak, przykładowo, są to:

- Czechy: Narodowy Urząd Bezpieczeństwa (NBU) oraz Narodowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informatycznego (NÚKIB),
- Słowacja: Narodowy Urząd Bezpieczeństwa (NBU),
- Rumunia: Narodowy Rejestr Informacji Niejawnych (ORNISS),
- Belgia: Narodowa Władza Bezpieczeństwa (ANS).

Przyglądając się bliżej modelowi funkcjonującemu u naszego południowego sąsiada zauważamy, iż zgodnie z § 5 ustawy nr 153/1994 o służbach wywiadowczych Republiki Czeskiej, Informacyjna Służba Bezpieczeństwa (Bezpečnostní informační služba - BIS) zajmuje się działaniami zagrażającymi bezpieczeństwu informacji stanowiących tajemnicę państwową lub służbową. BIS nie zajmuje się jednak prowadzeniem postępowań w zakresie dostępu do informacji niejawnych, tak jak to jest w przypadku ABW (służba takie postępowania, zgodnie z § 9 ustawy nr 148/1998 o ochronie informacji niejawnych, może prowadzić jedynie wobec własnych funkcjonariuszy). Za kwestie bezpieczeństwa informacji niejawnych w Czechach odpowiada Narodowy Urząd Bezpieczeństwa (Národní bezpečnostní úřad - NBU) oraz Narodowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informatycznego (Národní úřad pro kybernetickou a informační bezpečnost - NÚKIB).

Mimo swej nazwy żaden z tych urzędów nie jest służbą specjalną. Urząd (NBU) został powołany w dniu 1 sierpnia 1998 roku na mocy ustawy nr 148/1998 o ochronie informacji niejawnych i jest centralnym organem administracji w zakresie ochrony informacji niejawnych oraz wydawania certyfikatów dostępu do tych informacji. Z kolei Narodowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informatycznego (NÚKIB) został powołany 1 sierpnia 2017 roku na podstawie ustawy nr 205/2017 o bezpieczeństwie cybernetycznym. Urząd ten jest obecnie centralnym organem administracji ds. bezpieczeństwa cybernetycznego, w tym również w zakresie ochrony informacji niejawnych w systemach informatycznych i teleinformatycznych oraz w zakresie ochrony kryptograficznej. NÚKIB odpowiada np. za certyfikację systemów informatycznych, środków technicznych i kryptograficznych. Urzędy te funkcjonują poza systemem czeskich służb specjalnych.

Ustawa o ochronie informacji niejawnych nr 412/2015 wprowadziła kontrolę NBU ze strony Izby Poselskiej. Izba ustanowiła specjalny organ kontrolny „Stałą komisję ds. kontroli działalności NBU”. Komisja liczy siedmiu członków. W ustawie określono również dokumenty i informacje, które dyrektor NBU przedkłada komisji. Są to informacje o działalności NBU, informacje na temat poszczególnych postępowań oraz materiały dotyczące budżetu urzędu.

W starej ustawie w art. 9 (ustawy nr 148/1998 o ochronie informacji niejawnych) był zapis, że Wywiad Wojskowy (Vojenské zpravodajství) wydaje poświadczenia bezpieczeństwa w zakresie kompetencji Ministerstwa Obrony. Zmiana

---

[16] https://fibis.pl/czas-na-nowy-model-systemu-ochrony-tajemnicy-panstwowej-w-polsce/, 15.06.2019

nastąpiła w roku 2003 na podstawie rozporządzenia Rządu RC nr 1251 z 10 grudnia 2003. Od tego roku MON utraciło możliwość przeprowadzania postępowań w zakresie dostępu do informacji niejawnych. Zgodnie z nową UOIN nr 412/2005 wszelkie postępowania w zakresie dostępu do informacji niejawnych niezależnie, czy jest to sfera cywilna czy wojskowa, prowadzi NBU i NÚKIB. Wyłączone są z tego tylko służby wywiadowcze i czeskie MSW (np. Policja).

NBU współpracuje ze wszystkimi służbami specjalnymi RC, Policją, MSW i innymi instytucjami w zakresie zwracania się do tych instytucji o przekazywanie informacji niezbędnych do przeprowadzenia postępowania sprawdzającego. Ankiety bezpieczeństwa osobowego są podobne do tych stosowanych w Polsce.

U drugiego z naszych południowych sąsiadów - Słowacji, tematem ochrony informacji niejawnych zajmuje się instytucja o tej samej nazwie co w Czechach - Narodowy Urząd Bezpieczeństwa (Národný bezpečnostný úrad). NBU jest centralnym organem ds. ochrony informacji niejawnych, szyfrów, bezpieczeństwa cybernetycznego i zaufanych usług (podpis elektroniczny). Urząd powstał w roku 2001, od 1 listopada 2001 r. przejął kompetencje Ministerstwa Spraw Wewnętrznych. Nie jest to służba specjalna. Ze służbami specjalnymi łączy go jedynie procedura sprawdzeniowa. Urząd zwraca się do służb i innych instytucji o wszelkie niezbędne informacje potrzebne do zakończenia danej procedury.

Urząd przedkłada informację roczną z działalności Specjalnej Komisji ds. Kontroli NBU Słowackiej Rady Narodowej. Komisja w przypadku stwierdzenia naruszenia przepisów ma obowiązek zawiadomić Radę Narodową, Prokuratora Generalnego i rząd RS.

Na podstawie § 17 (3) ustawy o ochronie informacji niejawnych nr 215/2004, Wywiad Wojskowy (Vojenské spravodajstvo) przeprowadza postępowania sprawdzające II, III i IV stopnia (Poufne, Tajne i Ściśle tajne) wobec osób pozostających w stosunku służbowym lub stosunku pracy z Ministerstwem Obrony lub innymi organizacjami i instytucjami, których organem założycielskim jest MON. Zebrane przez Wywiad Wojskowy w trakcie postępowania materiały, z jego opinią i propozycją decyzji muszą zostać przekazane do Narodowego Urzędu Bezpieczeństwa. Spory pomiędzy tymi instytucjami rozstrzyga komisja Narodowej Rady Republiki. Również pracownicy słowackich służb specjalnych, wojskowych i cywilnych oraz policji, których postępowania prowadzą te instytucje, mogą się zwrócić z odwołaniem do tejże komisji parlamentu.

Z kolei w Rumunii systemem ochrony informacji niejawnych zajmuje się Narodowy Rejestr Informacji Niejawnych (ORNISS), który został utworzony rządowym rozporządzeniem wyjątkowym nr 153 z dnia 7 listopada 2002 roku, opublikowanym w Oficjalnym Dzienniku Rumunii nr 826 z dnia 15 listopada 2002 roku. Rozporządzenie wyjątkowe zostało zatwierdzone ustawą nr 101 z dnia 24 marca 2003 roku opublikowaną w Oficjalnym Dzienniku Rumunii, część I, nr 207 z dnia 31 marca 2003 roku.

ORNISS wykonuje zadania z zakresu regulacji, autoryzacji, kontroli oraz archiwizacji zgodnie z przepisami Ustawy nr 182/2002 o ochronie informacji niejawnych, Standardów Państwowych ochrony informacji niejawnych przyjętych przez Decyzję Rządową nr 585/2002 oraz Norm Organizacji Paktu Północnoatlantyckiego dot. ochrony informacji niejawnych w Rumunii przyjętych przez Decyzję Rządową nr 353/2002.

W celu wykonywania powierzonych zadań ORNISS posiada uprawnienia do żądania niezbędnych informacji od szefów służb i organów publicznych, podmiotów gospodarczych z wkładem państwowym oraz innych publicznych i prywatnych osób prawnych. Szefowie służb i organów publicznych, podmioty gospodarcze z wkładem państwowym oraz inne publiczne lub prywatne osoby prawne są obowiązane przekazać do dyspozycji ORNISS dane i informacje związane z ochroną informacji niejawnych na ich polu działalności, z wyjątkiem przypadków przewidzianych prawem.

Z kolei w Belgii, funkcję krajowej władzy bezpieczeństwa, zgodnie z dekretem wykonawczym do ustawy o ochronie informacji niejawnych i poświadczeniach bezpieczeństwa z 24 marca 2000 r., pełni organ o nazwie Autorité Nationale de Securité (Narodowa Władza Bezpieczeństwa). Jest to organ kolegialny, który odpowiada za wydawanie i odbieranie poświadczeń bezpieczeństwa oraz za sprawowanie nadzoru nad systemem ochrony informacji niejawnych. Na zasadzie wyjątku, funkcję Narodowej Władzy Bezpieczeństwa w stosunku do osób zatrudnionych w cywilnej Służbie Bezpieczeństwa (Sûreté de l'État/Veiligheid van den Staat - VSSE) i kandydatów do służby pełni dyrektor generalny VSSE.

Przedstawione wyżej cztery modele systemu ochrony informacji niejawnych, które opierają się na niezależności podmiotów odpowiedzialnych za system od służb specjalnych, stanowią rozwiązanie warte rozważenia i w Polsce. W państwach demokratycznych nie powinno się z zasady gromadzić zbyt wielu danych o obywatelu w jednym miejscu i tą drogą poszły te kraje, tworząc niezależne urzędy ds. ochrony informacji niejawnych. Były Generalny Inspektor Ochrony Danych Osobowych, dr Wojciech Wiewiórowski, w rozmowie z redaktorem Tomaszem Sekielskim przeprowadzonej w 2013 r. zwracał uwagę, że zarówno podmioty prywatne, jak i publiczne generalnie mają tendencję, by wiedzieć o nas jak najwięcej. Przypominał jednak, że art. 51 ust. 2 Konstytucji RP wprost stanowi, że władza publiczna może gromadzić o obywatelu tylko te informacje, które są niezbędne w demokratycznym państwie prawnym. Nie ma zatem prawa zbierać informacji, które mogą być jej „przydatne", „potrzebne", „logiczne" czy „ekonomicznie opłacalne", co postanowiono w 1997 roku, uchwalając polską Konstytucję i że była to reakcja na państwo totalitarne. Przestrzegał również, iż pamięć państwa totalitarnego powinna wciąż tkwić w naszych głowach, ponieważ dane zebrane nawet do najbardziej cnotliwych celów, mogą być niecnie wykorzystane i przez instytucje prywatne, i przez instytucje państwowe.[17]

System, w którym za ochronę informacji niejawnych odpowiadają służby specjalne, nie jest rozwiązaniem optymalnym. ABW, zgodnie z art. 5 ustawy o ABW oraz AW[18], realizuje cały szereg zadań, wśród których "realizowanie, w granicach swojej właściwości, zadań związanych z ochroną informacji niejawnych oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych"[19] jest jednym z wielu. Ponadto, zakres odpowiedzialności ABW stale się powiększa, np. o zapobieganie zdarzeniom o charakterze terrorystycznym (od 2016 r.) czy o CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym (od 2018 r.). ABW prowadzi też działalność operacyjną, dochodzeniowo-śledczą i analityczną a także - w zakresie ochrony informacji niejawnych - administracyjną (w oparciu o KPA). Zarządzanie tak wielkim podmiotem, z tak wieloma zadaniami i kompetencjami, jest niezwykle skomplikowane. Przy dużej "wadze" zadań zasadniczych (zwalczanie szpiegostwa, terroryzmu, ochrona ekonomicznych interesów państwa), temat ochrony informacji niejawnych nie jest przez ABW traktowany priorytetowo, choćby w zakresie kadrowym.

Aby zapewnić bezpieczeństwo i prawidłowe funkcjonowanie systemu ochrony informacji niejawnych, Fundacja Instytut Bezpieczeństwa i Strategii postuluje zatem, by w Polsce powołana została odrębna od służb specjalnych instytucja (urząd) - krajowa władza bezpieczeństwa informacji niejawnych (robocza nazwa KWBIN) - odpowiedzialna za kreowanie polityki państwa w sferze informacji niejawnych, wydawanie certyfikatów (poświadczeń i świadectw) dostępu do tajemnic państwa osobom i firmom, nadzór i kontrolę nad instytucjami wydającymi takie certy-

---

[17] https://giodo.gov.pl/pl/1520001/6608, 20.06.2019

[18] Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2018 r. poz. 2387 ze zmianami)

[19] Art. 5 ust. 1 pkt 3 ustawy o ABW oraz AW

fikaty swoim funkcjonariuszom, żołnierzom i pracownikom, wydawanie świadectw akredytacji systemów teleinformatycznych przetwarzających informacje niejawne, certyfikację środków ochrony elektromagnetycznej, nadzór i kontrolę nad instytucjami przetwarzającymi informacje niejawne (w tym służby wywiadowcze i policyjne), współpracę międzynarodową, prowadzenie negocjacji umów międzynarodowych w zakresie informacji niejawnych, tworzenie standardów dotyczących ochrony informacji niejawnych oraz szkolenia i działania prewencyjne. Urząd ten przejąłby instytucjonalną odpowiedzialność za system ochrony informacji niejawnych od ABW i SKW. Służby te certyfikowałyby (tak jak dotychczas) swoich funkcjonariuszy oraz udzielałyby pomocy w procesie sprawdzeń osób i podmiotów gospodarczych, realizowanym przez KWBIN. Instytucja ta podlegałaby bezpośrednio Prezesowi Rady Ministrów.

Podobny postulat przedstawił w Tomasz Borkowski w cytowanym wyżej artykule, który urząd o podobnych kompetencjach nazwał roboczo Urzędem Ochrony Informacji Niejawnych[20].

Proponowane rozwiązanie uniemożliwi służbom specjalnym (głównie ABW) zawłaszczenie systemu ochrony tajemnic państwa i nadużywanie dominującej pozycji w tej sferze do limitowania dostępu do działalności związanej z możliwością przetwarzania informacji niejawnych arbitralnie wybranym osobom i podmiotom, według własnego uznania, często kierując się pozamerytorycznymi lub wręcz partykularnymi celami, w tym politycznymi. Uniemożliwi również służbom pozyskiwanie wrażliwej wiedzy o obywatelach, która to wiedza może być wykorzystywana do zupełnie innych celów niż ochrona informacji niejawnych.

**Rekomendacje**

- Z uwagi na brak precyzyjnych uregulowań oraz duża uznaniowość służb przy wydawaniu poświadczeń bezpieczeństwa, świadectw bezpieczeństwa przemysłowego czy świadectw akredytacji systemów teleinformatycznych konieczne jest pilne dokonanie reformy całego systemu przyznawania dostępu przedsiębiorców do rynku związanego z przetwarzaniem informacji niejawnych oraz dostępu obywateli do wykonywania funkcji publicznych lub gospodarczych, gdy zajmowanie tych stanowisk wiąże się z dostępem do informacji niejawnych.

- W ramach zmian należy wdrożyć ramy prawne i system kontroli dostępu i wykorzystania uzyskanych w procesie certyfikacji ogromnych ilości informacji, często wrażliwych, o obywatelach i ich środowisku, co w małej mierze przekłada się na rękojmię zachowania tajemnicy tak aby wiedza ta nie była gromadzona w innych celach niż przyznawanie dostępu do informacji niejawnych.

- Elementem kluczowym zmian w systemie powinno stać się, wzorem innych krajów europejskich, które odstąpiły od wykorzystywania służb specjalnych do nadzoru nad systemem ochrony informacji niejawnych, powołanie w Polsce urzędu - krajowej władzy bezpieczeństwa informacji niejawnych (KWBIN) - którego jedynym zadaniem będzie sprawowanie nadzoru na systemem ochrony informacji niejawnych w pełnym zakresie. Takie rozwiązanie uniemożliwi służbom specjalnym zawłaszczenie systemu ochrony tajemnic państwa i nadużywanie dominującej pozycji w tej sferze do limitowania dostępu do działalności związanej z możliwością przetwarzania informacji niejawnych. Uniemożliwi również służbom pozyskiwanie wrażliwej wiedzy o obywatelach, która to wiedza może być wykorzystywana do zupełnie innych celów niż ochrona informacji niejawnych.

---

[20] https://osluzbach.pl/2019/05/23/borkowski-ustawa-m-kaminskiego-jak-w-dyktaturze/

**prof. dr. hab. H. Królikowski, dr A. Jagnieża, G. Matyasik**

## W poszukiwaniu modelu współpracy wojsk obrony terytorialnej z wojskami specjalnymi

Zmieniająca się sytuacja geopolityczna za wschodnią granicą Polski, w tym zwiększające się zagrożenie wynikające m.in. z podprogowego konfliktu zbrojnego, czego przykładem była aneksja Krymu przez Rosję na przełomie lutego i marca 2014 roku, unaoczniła dysfunkcję do powszechnej obrony obszaru kraju.[1] Z tego względu decyzją rządu postanowiono zwiększyć wielkość i jakość sił zbrojnych. W tym celu dokonano nowelizacji ustawy o powszechnym obowiązku obrony i od 1 stycznia 2017 roku rozpoczęto w Polsce budowę nowego rodzaju sił zbrojnych jakim są Wojsk Obrony Terytorialnej.[2] Ówczesna decyzja parlamentu stanowiła konieczny krok na drodze do wdrożenia procesu komplementarnego rozwoju sił zbrojnych RP, które powinny być zdolne do prowadzenia działań nie tylko w trakcie trwania klasycznego konfliktu wojennego, ale także konfliktu poniżej progu wojny[3], tzw. konfliktu hybrydowego[4] oraz konfliktu w którym zawczasu przygotowane segmenty sił zbrojnych będą w stanie obok działań regularnych prowadzić także skuteczne działania nieregularne w tym także działania nieregularne w ramach konfliktu asymetrycznego[5].

Zgodnie z obowiązującymi dokumentami doktrynalnymi obrona terytorialna (OT) w ujęciu funkcjonalnym to zespół terenowych sił i środków wyodrębnionych z poszczególnych podsystemów tworzących system obronny państwa przygotowanych do realizacji zadań obronnych we wszystkich stanach gotowości państwa.[6] Celem działań OT jest udział w powszechnym przygotowaniu oraz wykorzystaniu sił i środków znajdujących się w dyspozycji państwa na szczeblu samorządu terytorialnego do zapobiegania i przeciwdziałania wszelkiego typu zagrożeniom o charakterze militarnym oraz niemilitarnym.[7] Warunkiem koniecznym sprawnego i skutecznego funkcjonowania OT w ujęciu systemowym jest osiągnięcie tzw. sprzężenia zwrotnego wszystkich elementów wchodzących w jego skład w skali całego państwa.[8] Z tego względu Wojska Obrony Terytorialnej z założenia stanowią formację obejmującą całe terytorium kraju, będąc zdolnymi do prowadzenia działań z użyciem środków militarnych i niemilitarnych przy wykorzystaniu dostępnych zasobów obywatelskich. Jednocześnie należy podkreślić, iż istotą działania jednostek WOT jest ich użycie w stałych rejonach odpowiedzialności.[9]

Do zadań Wojsk Obrony Terytorialnej w stanie gotowości obronnej państwa czasu wojny należy prowadzenie działań na poziomie taktycznym we współdziałaniu z pozostałymi rodzajami sił zbrojnych oraz elementami podsystemu niemilitarnego, zapewnienie powszechnej ochrony i obrony Stałych Rejonów Odpowiedzialności oraz wsparcie zabez-

---

[1] płk. dypl. Wojciech Prygiel, ppłk K. Bednarz, Nowy rodzaj sił zbrojnych, Przegląd Sił Zbrojnych, 5/2017;

[2] Dz.U. 2019 poz. 1541 Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 19 lipca 2019 r. w sprawie ogłoszenia jednolitego tekstu ustawy o powszechnym obowiązku obrony Rzeczypospolitej Polskiej;

[3] R. Jakubczak, K. Gąsiorek, H. M. Królikowski, J. Marczak, Działania nieregularne – elementy strategii bezpieczeństwa narodowego Polski, Warszawa 2011, s. 62-63;

[4] Szerzej o zjawisku wojny hybrydowej m.in.: A. Gruszczak, Hybrydowość współczesnych wojen – analiza krytyczna W: Asymetria i hybrydowość – stare armie wobec nowych konfliktów, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, s. 13; H. Królikowski, Hybrid Threats and Warfare, Are We Really Facing Something New?, w: Internal Security, 2017, t.9, s.9-21.

[5] M. Marszałek, Wojny nieregularne. Przeszłość i przyszłość, Warszawa 2016, s. 22-23;

[6] Wojska Obrony Terytorialnej w operacji DD-3.40, Warszawa 2018, s. 10;

[7] Tamże;

[8] Tamże;

[9] Tamże, s. 13-14;

pieczenia wejścia do walki sojuszniczych sił wzmocnienia.[10] Tym samym Wojska Obrony Terytorialnej ze względu na swój charakter i przeznaczenie będą realizowały zadania na poziomie taktycznym w ramach operacji reagowania kryzysowego oraz strategicznej operacji obronnej, przy czym zakłada się, iż WOT będą prowadzić działania w Stałych Rejonach Odpowiedzialności, a do głównych zadań taktycznych realizowanych przez jednostki WOT będzie należeć stałe prowadzenie rozpoznania zagrożeń, obrona, ochrona miejscowości, rubieży, węzłów komunikacyjnych i obiektów istotnych dla realizacji operacji obronnej oraz wprowadzenie do własnego regionu odpowiedzialności wojsk własnych oraz wojsk sojuszniczych.[11] Co istotne przewiduje się, że działania WOT na poziomie taktycznym w zależności od rozwoju sytuacji na froncie będą realizowane w strefie działań bezpośrednich, bądź w tylnej strefie działań oraz na terenach czasowo zajętych przez agresora.[12] Z tego względu w sposób naturalny nasuwa się wniosek, iż zadania jak i charakter Wojsk Obrony Terytorialnej determinują ich współpracę z Wojskami Specjalnymi które z kolei stanowią drugi z najmłodszych rodzajów sił zbrojnych.

Na czele utworzonych w 2007 roku Wojsk Specjalnych stoi Dowódca Komponentu Wojsk Specjalnych, który podlega bezpośrednio Dowódcy Generalnemu Rodzajów Sił Zbrojnych. Wojska Specjalne są tym elementem Sił Zbrojnych RP, który aktywnie uczestniczy w misjach poza granicami państwa w ramach NATO i Unii Europejskiej oraz udziela wsparcia państwom spoza NATO (Ukraina, Gruzja). W przypadku wybuchu wojny należy oczekiwać, że Wojska Specjalne powinny mieć możliwość działania na zapleczu przeciwnika. Personel Dowództwa Komponentu Wojsk Specjalnych będzie trzonem wielonarodowego dowództwa komponentu operacji specjalnych i z podległymi mu zespołami bojowymi będzie po raz drugi pełnić w 2020 roku dyżur bojowy w Siłach Odpowiedzi NATO.

Żołnierze Wojsk Specjalnych są ochotnikami, zawodowcami i profesjonalistami. Z racji wyjątkowego sposobu doboru, selekcji i szkolenia w siłach zbrojnych, Siły Operacji Specjalnych stanowią niewielki elitarny element. Liczebność Sił Zbrojnych Stanów Zjednoczonych to nieco ponad 1300000 żołnierzy, w tym Siły Operacji Specjalnych, to około 70000, czyli 5,4% liczebności wojska. Siły Zbrojne RP liczą około 120000 żołnierzy, z czego Wojska Specjalne to około 2500 żołnierzy, co daje 2,1% liczebności Wojska Polskiego. W Wielkiej Brytanii liczebność sił zbrojnych przekracza 190000, z tego Wojska Specjalne to niespełna 3000 ludzi, czyli około 1,5% całej armii.

W 2019 r. w ramach budżetu resortu obrony narodowej Wojska Specjalne otrzymały prawie 353000000 PLN (największy względny przyrost wśród rodzajów sił zbrojnych – około 20%). Kwota ta stanowi jednak tylko 0,79% budżetu MON. Wojska Specjalne są więc bardzo efektywnym, elastycznym co do form użycia ale i nie drogim jakby mogło się w potocznej opinii wydawać rodzajem sił zbrojnych.

Siły Operacji Specjalnych w NATO i w Polsce posiadają wysoki stopień ukompletowania, na poziomie 90-95% (jednostki specjalne dla osiągnięcia gotowości bojowej nie muszą być uzupełniane w drodze mobilizacji). To w połączeniu z systemem dyżurów bojowych i lekkimi strukturami organizacyjnymi przekłada się na mobilność taktyczną i strategiczną oraz bardzo wysoką gotowość bojową. Nie mniej ważna jest też możliwość łatwego ukrycia przemieszczania elementów Sił Operacji Specjalnych, np. w porównaniu z oddziałami zmechanizowanymi.

Z kolei na czele WOT stoi Dowódca Wojsk Obrony Terytorialnej, który podlega bezpośrednio Ministrowi Obrony Narodowej. W przeciwieństwie do Wojsk Specjalnych, WOT jest tworzony jako formacja powszechna, a nie elitarna. Stąd też proces rekrutacji i szkolenia w WOT nie jest tak złożony i długotrwały jak w Wojskach Specjalnych, a wy-

---

[10] Tamże, s. 16;

[11] Tamże, s. 21

[12] Tamże, s. 25

magania wobec przyszłych żołnierzy nie są tak restrykcyjne. We wrześniu 2019 roku WOT osiągnął liczebność nieco ponad 20000 żołnierzy (w odniesieniu do liczby żołnierzy jest to równowartość jednej lub dwóch dywizji, w zależności od przyjętego referencyjnego typu dywizji), co stanowi 16,2% liczebności SZ RP. Ogłoszone jeszcze w 2015 roku oficjalnie, choć zapewne nadmiernie optymistyczne plany zakładały 53000 żołnierzy WOT. Jako realne należy uznać jednak przekroczenie przez WOT w 2020 roku liczby 30000 żołnierzy. Należy podkreślić, iż w innych państwach idea utworzenia obrony terytorialnej także zakłada powszechność i nasycenie terytorium państwa jednostkami sił obrony terytorialnej. W Szwecji liczebność sił zbrojnych to około 22500 żołnierzy, podczas gdy Gwardia Narodowa (Hemvärnet) liczy 22000 żołnierzy. Z kolei siły zbrojne Danii liczą około 15500 żołnierzy, a siły Gwardii Narodowej (Hjemmeværnet) to 15600 aktywnych ochotników.

W 2019 wydatki resortu obrony narodowej na WOT zaplanowano w wysokości prawie 483500000 PLN, co stanowi 1,08 budżetu MON. Jest to spadek o prawie 15% wobec z 568000000 PLN w 2018 roku. Trudno więc zgodzić się z niekiedy podnoszonym argumentem, że WOT odbiera pieniądze innym rodzajom sił zbrojnych.

Pomimo wymienionych wyżej różnic obie formacje łączy na pewno duża motywacja żołnierzy do służby. Nie jest tajemnicą, że proces selekcji i szkolenia w Wojskach Specjalnych jest wyjątkowo wymagający, a służba trudna i niebezpieczna. Z kolei przyjęcie dodatkowych obowiązków poza rodzinnymi, służbowymi i podjęcie zobowiązania do szkolenia w ramach Terytorialnej Służby Wojskowej, też świadczy o silnej motywacji do służby.

Zagadką, a raczej informacją niejawną, pozostaje natomiast umiejscowienie Dowództwa Komponentu Wojsk Specjalnych i Dowództwa Wojsk Obrony Terytorialnej w wojennym systemie dowodzenia. Z tego względu nasuwa się też kilka pytań dotyczących zasad współpracy między WOT, a Wojskami Specjalnymi, a wśród nich zasadnicze pytanie czy taka współpraca jest w ogóle możliwa w obliczu faktu, że WOT jest przypisany do obrony terytorium państwa i Stałych Rejonów Odpowiedzialności, a Wojska Specjalne już dziś działają zagranicą w Polskich Kontyngentach Wojskowych w ramach NATO lub misji Unii Europejskiej, a na czas wojny są przygotowywane do operowania na terytorium przeciwnika? Co istotne, pytanie to odnosi się zarówno do okresu pokoju, jak i czasu kryzysu oraz wojny a odpowiedź na nie chociażby ze względu na potrzebę synergii działań musi być twierdząca.

W okresie pokoju wspólnym obszarem współpracy WOT oraz Wojsk Specjalnych powinno być szkolenie. Wojska Specjalne mają bezdyskusyjne kompetencje do przekazywania wiedzy teoretycznej i praktycznej, co czynią szkoląc formacje militarne w Afganistanie, Gruzji, Iraku i na Ukrainie. „Specjalsi" są więc naturalnym nauczycielem dla żołnierzy WOT. Formuła współpracy szkoleniowej pozwala też wykorzystać w procesie szkolenia WOT byłych żołnierzy jednostek specjalnych, którzy obecnie są poza służbą. Ten proces już zresztą ma miejsce. Żołnierze Jednostek Wojskowych Komandosów i GROM odgrywają kluczowe role w DWOT – Dowódcą WOT-u został generał dywizji Wiesław Kukuła, były Dowódca Jednostki Wojskowej Komandosów, natomiast Szefem Wydziału Szkolenia DWOT został pułkownik Konrad Korpowski były szef szkolenia JW GROM. Jednocześnie kilku dowódców brygad WOT także wywodzi się z Wojsk Specjalnych jak na przykład dowódca 11 Łódzkiej Brygady WOT pułkownik Paweł Wiktorowicz, żołnierz Jednostce Wojskowej Komandosów, jednocześnie absolwent prestiżowego kursu „Zielonych Beretów" w Fort Bragg w USA. Byłym specjalsem dowodzącym z kolei 7 Pomorską Brygadą OT jest komandor Tomasz Laskowski wcześniej zastępca dowódcy JW FORMOZA. Z kolei dowódca 13 Śląskiej Brygady WOT pułkownik Tomasz Białas to były szef pionu szkolenia w JWK w Lublińcu, instruktor spadochronowy i trzykrotny uczestnik misji w Iraku i Afganistanie. Ponadto w oparciu o żołnierzy Wojsk Specjalnych funkcjonuje Mobilny Zespół Szkoleniowy WOT. Dotychczasowa praktyka pokazuje zatem, iż tendencja wykorzystywania doświadczenia żołnierzy Wojsk Specjalnych w procesie szkolenia WOT powinna być nie tylko utrzymana ale dalej rozwijana.

Inny obszar współpracy to wspólne ćwiczenia jednostek Wojsk Specjalnych i WOT. Jeśli jednym z zadań pododdziałów WOT jest wykrywanie, izolowanie i zwalczanie grup specjalnych przeciwnika, to naturalnym partnerem do ćwiczeń są polskie pododdziały specjalne. Z drugiej strony jest to też znakomita okazja dla Wojsk Specjalnych do ćwiczenia działania na wrogim terenie. Dobrym przykładem takiego współdziałania były wspólne ćwiczenia Policji, Sił Zbrojnych RP i członków Podhalańskiej Obrony Terytorialnej, pod kryptonimem „Dywersanci", które odbyły się 21 października 2016 roku na terenie powiatu nowotarskiego w Gorcach. Zgodnie z założeniem, Grupa Operacyjna, składająca się z policjantów Komendy Powiatowej Policji w Nowym Targu oraz członków Podhalańskiej Obrony Terytorialnej, dowodzona przez wyznaczonego oficera Policji miała za zadanie przećwiczenie procedur i zasad działania, na wypadek pojawienia się na podległym im terenie grup dywersyjno – rozpoznawczych podgrywanych w tym przypadku przez żołnierzy Wojsk Specjalnych.

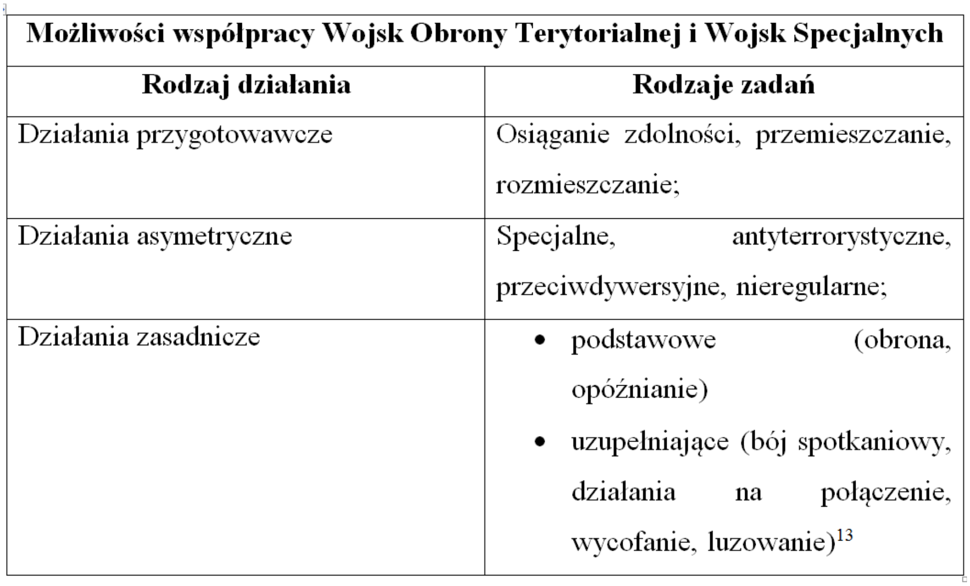
Potencjalnym obszarem współpracy WOT i Wojsk Specjalnych jest występowanie sytuacji kryzysowych, w tym zagrożeń poniżej progu wojny, jak na przykład zagrożeń terrorystycznych. W tym kontekście atutem Wojsk Specjalnych jest możliwość szybkiego przemieszczenia pododdziałów w dowolny rejon kraju, a z kolei zaletą WOT jest z jednej strony obecność WOT na całym terytorium państwa, zaś z drugiej strony zdolność do bardzo szybkiej mobilizacji pododdziałów. Gotowość do błyskawicznego działania WOT i jednostek Wojsk Specjalnych powoduje, że obydwa rodzaje sił zbrojnych w sytuacji konfliktu hybrydowego stają się naturalnymi partnerami, którzy wzajemnie uzupełniają się. Słabości WOT związane np. z wyposażeniem - w szczególności w ciężki sprzęt - oraz problem związany z wyszkoleniem np. kontrterrorystycznym w sposób naturalny wypełniane są przez zdolności i możliwości działania Wojsk Specjalnych, na przykład poprzez możliwości ogniowe JW AGAT oraz możliwości kontrterrorystyczne pozostałych pododdziałów Wojsk Specjalnych. Możemy wyobrazić sobie współdziałanie pododdziałów WOT i Wojsk Specjalnych, w którym pododdziały WOT odnajdują i izolują grupy specjalne przeciwnika (działające np. jako grupy przestępcze lub tzw. „zielone ludziki") a ich bezpośrednią likwidacją zajmują się podod-

działy specjalsów.

W okresie wojny obszarem wspólnego działania obu rodzajów Sił Zbrojnych jest aktywność na tzw. terytorium czasowo zajętym przez przeciwnika. Przy takim wariancie konfliktu dochodzi do pełnej symbiozy WOT-u i Wojsk Specjalnych. Pododdziały WOT-u przejmują funkcję przygotowania i zabezpieczenia działań pododdziałów wojsk specjalnych, począwszy od zabezpieczenia miejsc przejęcia (np. w wariancie przerzutu drogą powietrzną) po zabezpieczenie skrytek na broń, amunicję, żywność, wodę, po przygotowanie baz jako elementy wsparcia logistycznego, przechodząc dalej po wsparcie informacyjne a w tym oddelegowanie łączników, przekazywanie aktualnych informacji rozpoznawczych, informacji związanych z terenem, przeciwnikiem oraz otoczeniem i sytuacją ogólną. Pododdziały WOT prowadzące działania nieregularne mogą przeprowadzać działania mylące przeciwnika w celu umożliwienia wykonania zadań przez Wojska Specjalne. WOT mogą także wykonywać zadania ubezpieczające lub izolujące związane z realizacją zadania zasadniczego wykonywanego przez pododdział (pododdziały) Wojsk Specjalnych. W przypadku czasowej okupacji określonego terytorium „specjalsi" mogą także wspierać „terytorialsów" w procesie szkoleniowym tak jak czynili to Cichociemni szkoląc żołnierzy Armii Krajowej.

**Rekomendacje**

Czasy kryzysu i wojny wymagają wykorzystania w ramach organizacji systemu obronnego państwa zasobów Wojsk Obrony Terytorialnej oraz Wojsk Specjalnych w taki sposób, aby uzyskać optymalny efekt synergii w działaniu. Zagadnienie to wymaga zatem dalszych studiów oraz organizacji cyklu ćwiczeń które powinny stanowić podstawę wypracowania optymalnego modelu współpracy obydwu rodzajów sił zbrojnych.



| Możliwości współpracy Wojsk Obrony Terytorialnej i Wojsk Specjalnych | |
|---|---|
| **Rodzaj działania** | **Rodzaje zadań** |
| Działania przygotowawcze | Osiąganie zdolności, przemieszczanie, rozmieszczanie; |
| Działania asymetryczne | Specjalne, antyterrorystyczne, przeciwdywersyjne, nieregularne; |
| Działania zasadnicze | • podstawowe (obrona, opóźnianie)<br>• uzupełniające (bój spotkaniowy, działania na połączenie, wycofanie, luzowanie)[13] |

---

[13] Regulamin działań Wojsk Lądowych, Warszawa 2008, s. 14;

## J. Trzeciakowska

# OSINT jako narzędzie zarządzania strategicznego

### Siła informacji

Nie jest tajemnicą ani odkryciem, że siłę i pozycję negocjacyjną można mierzyć nie tylko zasobami finansowymi w dyspozycji, ale także informacjami, które się posiada, do których ma się dostęp oraz z którymi umie się pracować i wykorzystać je do realizacji własnych celów.

XXI wiek przyniósł nam realia, w których spojrzenie na informację i jej wartość trzeba przewartościować. Znaleźliśmy się w rzeczywistości, gdzie samo dotarcie do informacji zaczyna być problemem mniejszym aniżeli uporanie się z jej nadmiarem i wyselekcjonowanie kluczowych dla nas treści. Odpowiedzialny za to jest wykładniczy przyrost treści dostępnych w internecie, który stał się podstawowym, najłatwiej osiągalnym, najszybciej rozwijającym się zasobem informacyjnym. Jest to środowisko, w którym ogniskują się i mieszają między sobą działania rządów i biznesu, a w którym odnaleźć się muszą jednostki wykorzystujące informacje i dane dostępne w internecie w swojej codziennej działalności, czy to zawodowej czy prywatnej.

Internet w swej różnorodności stał się dobrodziejstwem i źródłem niemal nieograniczonego potencjału, dla tych, którzy umieją odnaleźć się w tych realiach, rozumieją jego specyfikę i niejednorodność. Jako potężny zasób informacji i danych stał się środowiskiem pracy szeroko rozumianej grupy profesjonalistów informacji: analityków, infobrokerów, służb wywiadowczych, organów kontroli i wielu innych, którzy w swojej codziennej pracy intensywnie wykorzystują techniki OSINT, o których specyfice i znaczeniu traktuje niniejszy artykuł.

### OSINT – od teorii do praktyki

OSINT (ang. open source intelligence) tłumaczy się jako zbiór technik, metod i narzędzi służących pozyskiwaniu danych i informacji ze źródeł jawnych, do których dostęp może mieć każdy obywatel. Nie oznacza to, że skorzystanie ze wszystkich zasobów klasyfikowanych jako jawne jest jednakowo proste i oczywiste dla przeciętnego użytkownika.

Mówiąc o OSINT należy rozpatrywać to zagadnienie w różnych perspektywach i z uwzględnieniem dynamiki zmian, jaka nieustannie odbywa się w świecie wywiadu jawnoźródłowego, zwanego także białym wywiadem. Tylko takie spojrzenie na zagadnienie pozwoli całościowo zrozumieć potencjał i ryzyka drzemiące w OSINT.

W pierwszej kolejności warto przypomnieć o ewolucji, jaka w OSINT nastąpiła na przestrzeni dekad. O ile sam biały (i nie tylko biały) wywiad nie jest rzeczą nową, o tyle m. in ze względu na rozwój technologii przeszedł on niesamowitą transformację. Stało się to oczywiście za sprawą internetu, który pozwolił na udostępnienie w wersji cyfrowej potężnych zasobów danych i informacji.

Ważnym punktem na tej drodze stał się rozwój internetu web 2.0., obserwowany od około 2001 roku, całkowicie zmieniający dotychczasowe standardy publikacji treści w sieci. O ile wcześniej przekaz treści w internecie był jednokierunkowy, od właściciela serwisu on-line i jego redakcji do czytelników, o tyle pierwsze platformy noszące znamiona dzisiejszych sieci społecznościowych, zaczęły te mechanizmy zmieniać. Twórcami treści stali się użytkownicy internetu, którzy zechcieli dzielić się swoją wiedzą, doświadczeniem i światopoglądem z resztą internetowej społeczności. To zmiana, która w perspektywie lat zaowocowała powstaniem i rozwojem platform społecznościowych, które dziś są standardem w atelier on-line'owych tubylców. Z perspektywy specjalistów OSINT na media społecznościowe patrzy się jak na potężny zasób o niezmierzonym i – w dłuższej perspektywie – dość nieprzewidywalnym potencjale informacyjnym.

OSINT nie jest jednak skoncentrowany tylko na zasobach zamkniętych w sieciach społecznościowych. Równie mocno wykorzystuje prasę, dostępne w wersji cyfrowej zasoby rejestrów dotyczących rozmaitych obszarów życia społecznego, materiały kartograficzne, zdjęcia, nagrania, zasoby danych statystycznych, bibliografie czy archiwa.

W obszarze zainteresowania specjalistów OSINT istotnym zasobem są informacje pozwalające analizować aktywność użytkowników internetu, w tym tzw. footprinty, a więc ślady, jakie pozostawiają po sobie użytkownicy internetu.

### OSINT – dla każdego inny

Zasoby danych i informacji, jakie mogą być eksplorowane przez specjalistów OSINT są mocno niejednorodne, a sam OSINT bywa różnie definiowany, w zależności od obszaru, na którym koncentruje się analityk. I tak, inaczej będzie wyglądać praktyka wywiadu jawnoźródłowego w wykonaniu pracownika wywiadowni gospodarczej, inaczej u infobrokera czy badacza analizującego rynki, jeszcze inaczej u pracownika organów kontroli bądź specjalisty bezpieczeństwa IT, tzw. pentestera. To wszystko powoduje, że każda z grup zawodowych wykorzystujących w swojej pracy OSINT, definiuje nieco inaczej jego istotę, wykorzystuje inne techniki pracy i wymaga stosowania różnych narzędzi wspierających proces OSINT. Nie chodzi jednak o znalezienie jednej definicji OSINT, ale spojrzenie na całe zagadnienie jako pole ogromnego potencjału do wykorzystania i dostosowania do specyfiki potrzeb różnych grup zawodowych. Tym bardziej, że transformacja zasobów informacyjnych jest procesem, który się dzieje, który wymaga, by aktualizować warsztat i metody w projektach wykorzystujących OSINT, a narzędzia stosowane przez – choćby – specjalistów marktingu dają się w OSINT skutecznie wykorzystać. Podobnie, narzędzia tworzone z myślą o pentesterach mogą być wsparciem w pracy infobrokera. Wszystko to zależy od konkretnych projektów i kryjących się za nimi potrzeb.

### OSINT w biznesie

Potencjał OSINT w realizacji celów biznesowych jest niemal niezmierzony, a to sprawia jednocześnie, że próba scharakteryzowania go w niniejszym artykule jest w rzeczywistości jedynie zasygnalizowaniem problematyki. Tym bardziej, na OSINT powinniśmy patrzeć jako na zagadnienie konieczne w stałej dyskusji i pragmatyce biznesu, bo służące realizacji kluczowych jego celów. Dlatego też w dalszej części tego materiału zaprezentowane zostały newralgiczne, choć absolutnie nie wszystkie obszary wykorzystania OSINT w biznesowej codzienności.

### Weryfikacja kontrahentów

O tym, że zarówno klientów jak i kontrahentów trzeba weryfikować, raczej nie trzeba nikogo przekonywać. Weryfikacja ta może być wielopłaszczyznowa i realizowana na różnym poziomie zaawansowania. Zaczynając od podstawowej weryfikacji czy podmiot, z którym chcemy współpracować w ogóle istnieje, czy osoba, która ma go reprezentować jest do tego uprawniona. Za kolejny krok możemy przyjąć weryfikację statusu płatnika VAT, czy sprawdzenia rejestrów dłużników i list sankcyjnych. W październiku tego roku w Polsce zacznie funkcjonować Centralny Rejestr Beneficjentów Rzeczywistych mający stanowić jedno z narzędzi w zapobieganiu m. in. praniu pieniędzy, stając się jednocześnie kolejnym zasobem do wykorzystania w procesie weryfikacji kontrahentów.

Jeżeli liczy się dla nas nie tylko sam aspekt wypłacalności, ale też jego wizerunek, zakres pracy, jaka jest do wykonania rośnie niemal wykładniczo, a zakres zasobów informacyjnych, jakie mamy do dyspozycji jest nieoceniony.

### Monitoring informacji

Sama czynność monitorowania to jedno z regularnych zadań specjalistów oddelegowanych do czuwania nad tym, co dzieje się w ruchu sieciowym. Wszystkie te działania mają zagwarantować bezpieczeństwo infrastrukturze IT i zapobiegać ryzykom, z jakimi mamy tam do czynienia, ale nie tylko ruch sieciowy daje się monitorować.

Z powodzeniem możemy poddawać mu zarówno zasoby o charakterze ilościowym i jakościowym, używając do tego szeregu mniej i bardziej zaawansowanych technik i narzędzi. Oto przykłady.

**- Zapomniane RSS.** Kanały RSS to technologia dziś i stosunkowo mało popularna wśród przedsiębiorców. W codziennej pracy można skutecznie wykorzystywać RSS do sprawnego, szybkiego zrealizowania prasówki koncentrującej się tylko na wybranych przez nas zagadnieniach i/lub tylko wyselekcjonowanych źródłach. Korzyść? Podstawowa to oszczędność czasu i koncentracja na samym przyswojeniu interesujących nas treści zamiast miotania się po szeregu portali, które będą rozpraszać nas nie zawsze ważnymi dla nas tematami. Oczywiście, skrajna informacyjna asceza też może się okazać błędną drogą, bo nie chodzi o to, by zamknąć się w prywatnej bańce informacyjnej i poruszać się tylko w zakresie RSSowych kolein. Idealnym rozwiązaniem byłby tutaj złoty środek, który dla każdego z użytkowników może oznaczać coś innego.

Monitorowanie informacji jakościowych on-line za pomocą RSS-ów może być ukierunkowane zarówno na monitorowanie własnej branży, marki czy konkurencji jak i dotyczyć konkretnych zagadnień związanych z realizowanymi przez nas projektami.

To jedna z metod na skuteczne zarządzanie pozyskiwanymi treściami i organizowanie sobie procesu gromadzenia danych i informacji w ramach projektów wykorzystujących OSINT.

Jakie oprogramowanie do RSS wybrać? Dużo zależy od naszych indywidualnych przyzwyczajeń w zakresie wykorzystywanego software'u oraz potrzeb informacyjnych. Do dyspozycji mamy zarówno aplikacje webowe jak i desktopowe. Niektóre z nich świetnie się sprawdzą w pozyskiwaniu treści ze źródeł polskojęzycznych, ale inne w takim przypadku okażą się mniej przydatne.

Dużym atutem czytników w wersji desktopowej (np. FeedReader, InoReader) jest możliwość wskazania silników wyszukiwarek, które chcemy wykorzystać w identyfikowaniu źródeł do monitorowania. Może to szalenie ułatwić pracę.

**- Alerty.** Budując warsztat do regularnego monitoringu treści, warto zwrócić także uwagę na usługę alertów. Mogą to być np. Google Alerts czy TalkWalker. Dzięki takiej usłudze można regularnie otrzymywać monity informujące o pojawieniu się treści odpowiadających naszemu zapytaniu. Oczywiście, narzędzia te będą wymagały odpowiedniego skalibrowania i – bardzo często – modyfikacji w opcjach alertów, aby finalnie dobrze adresowały nasze potrzeby. Dzięki temu, znów, możemy zaoszczędzić czas poświęcany na pisane każdorazowo ręczne kwerendy w wyszukiwarkach.

Kolejnym rozwiązaniem w monitoringu informacji będzie skorzystanie z dedykowanych do takich działań, komercyjnych aplikacji. W biznesie ich popularność koncentruje się na monitoringu mediów społecznościowych, klasycznego „informacyjnego FMCG".

### Marketing

Marketing to fantastyczne pole do popisu w zakresie biznesowego wykorzystania OSINT. Samo zaklasyfikowanie poszczególnych działań jako marketingowych jest z lekka umowne, ponieważ z powodzeniem moglibyśmy je przypisać też kompetencjom działów sprzedaży, analiz, rozwoju itp. Wykorzystanie OSINT dla potrzeb marketingu staje się jeszcze bardziej oczywiste, jeśli wrócimy do istoty tego, czym marketing jest. To przecież szereg działań mających pozwalać nam na budowanie strategii rozwoju firmy, na umacnianie jej pozycji i czuwanie nad tym, by stale wiedzieć, co dzieje się na rynku, na którym działamy. To nie tylko efektowne grafiki i interesujące posty w mediach społecznościowych, ale przede wszystkim twarde dane i konkretne informacje.

Obszar, w którym bez wątpienia OSINT będzie dla nas nieoceniony to analiza rynku, na którym działamy i analiza konkurencji. Budując dobrze skrojoną strategię pozyskiwania informacji o własnym rynku (choć mógłby to być też rynek klienta, jeśli np. zajmujemy się consultingiem biznesowym), dajemy sobie szansę na to, by poczuć, co dzieje się w branży.

Biały wywiad można z powodzeniem wykorzystać też jako sposób na generowanie sobie pomysłów do budowania strategii marki, strategii komunikacji i samego content marketingu. Jeżeli potrafimy umiejętnie pozyskać informacje branżowe, choćby z zasobów deep web dajemy sobie szanse na to, że dostarczane przez nas treści będą wyróżniać się spośród tego, co robi cała branża. Jeśli umiemy monitorować informacje na bieżąco, śledzić to, jak zachowują się użytkownicy internetu, co dzieje się choćby w mediach społecznościowych, a do tego wiemy, jak połączyć to np. z geolokalizacją, możemy budować sobie szerszą perspektywę spojrzenia na konkretne zagadnienia.

### Rekrutacja

Wejście w życie przepisów o RODO w ujęciu przepisów obowiązujących w Unii Europejskiej od maja 2018 roku spowodowało sporo konsternacji i wątpliwości wszędzie tam, gdzie w grę wchodzą dane osób. Takie obostrzenia mocno dotykają choćby osoby / firmy zajmujące się rekrutacją, natomiast, nie sposób wyobrazić sobie, że przestaliśmy wykorzystywać zasoby on-line do wyszukiwania potencjalnych pracowników, do weryfikacji choćby ich dorobku naukowego, jeśli taki deklarują.

Realia pozyskiwania informacji o osobach będą się kształtować dla nas odmiennie, jeśli poszukiwać będziemy np. pracowników zza wschodniej granicy. Okaże się wtedy, że przy rozsądnej konfiguracji narzędzi, będziemy mogli wyciągnąć dane z zamkniętych portali (np. społecznościówek dedykowanych celom prywatnym lub zawodowym) bez konieczności logowania się do nich.

### Anty-fakenews, anty-dezinfo

Samo pozyskanie informacji to połowa drogi. Druga połowa to jej umiejętne przeanalizowanie i wyciągnięcie wniosków. Aktualnie nieocenioną kompetencją przy pracy na zasobach online jest przeprowadzenie krytycznej analizy znalezionych treści. Mogą nam w tym pomóc dedykowane do tego narzędzia, aplikacje i źródła informacji. Ich znajomość i wykorzystywanie pozwoli nam nie dać się złapać na fenomen kolejnego niebieskiego wieloryba, o którym swego czasu było głośno także w Polsce. Finalnie takie podejście do wykorzystania dobrodziejstwa OSINTu może uchronić przedsiębiorstwa nie tylko przed stratą wizerunkową.

**Bezpieczeństwo**

Wykorzystanie technik OSINT-owych pozwala nam zweryfikować, jak wiele danych o naszym przedsiębiorstwie da się znaleźć w otwartych zasobach. Niekiedy prosta kwerenda w wyszukiwarce FTP pozwala zauważyć, że nie do końca wszystko zagrało jak należy w zabezpieczeniach serwerów. Stosunkowo łatwo możemy też zweryfikować czy przy stosowaniu prostych kwerend znajdują się tylko adresy mailowe pracowników, którzy są „eksponowani" przez firmę czy też dostępne są także adresy, które niekoniecznie miały być dostępne dla osób „przypadkowo" robiących kwerendę na temat naszego przedsiębiorstwa.

Przedstawione powyżej obszary wykorzystania wywiadu jawnoźródłowego w biznesie to ledwie inspiracja zasiana na konkretnych przykładach. Oczywistym natomiast powinno być, że OSINT to jeden z kluczowych elementów budowania strategii rozwoju przedsiębiorstw, wdrażania na rynek nowych produktów czy usług oraz budowania perspektyw internacjonalizacji biznesu. Wszystkie te działania wymagają pozyskania wiarygodnych informacji, a to z kolei narzuca na przedsiębiorców konieczność angażowania do działań pracowników elementów białego wywiadu nawet, jeśli ich stanowiska nie są wprost związane z OSINTem właśnie. Wówczas możemy mówić o po prostu zaawansowanych kompetencjach informacyjnych, by użyć słownictwa lżejszego kalibru.

**OSINT w bezpieczeństwie państwa**

Niekiedy mówi się, że strategiczne zarządzanie państwem nie różni się od zarządzania firmą: ma zapewniać bezpieczną ciągłość funkcjonowania, skuteczną realizację projektów i zadań oraz dostarczanie usług / produktów przy satysfakcjonującej współpracy z interesariuszami.

Jednym z elementów wpisanych w realizację takich działań jest efektywne zarządzanie zasobami informacyjnymi, a w konsekwencji także wiedzą i doświadczeniem. W tym obszarze nieocenionym elementem jest właśnie biały wywiad, którego możliwości wykorzystania i potencjał można rozpatrywać na wielu poziomach.

Wsparcie działań jednostek wywiadowczo-informacyjnych wydaje się być pierwszym z obszarów, gdzie OSINT może być skuteczny. Oczywistym jest, że takie jednostki w swej pracy mają do dyspozycji szeregu źródeł informacji o charakterze niejawnym, niemniej zasoby jawne mogą być ich uzupełnieniem. Komplementarne podejście do zasobów informacyjnych pozwala na zbudowanie szerszej, pełniejszej perspektywy koniecznej w procesie analizy informacji. Dobrze skrojona strategia OSINT to także skuteczne narzędzie służące monitoringowi informacji na skalę międzynarodową, gromadzenie i przetwarzanie publikowanych treści i wykorzystanie ich w budowaniu strategii we wszystkich obszarach funkcjonowania państwa. Przykładem takiego wykorzystania OSINT może bieżący monitoring trendów w zakresie innowacji i szerzej rozumianego obszaru R&D na potrzeby stworzenia krajowej strategii w tym zakresie. Można pokusić się o sformułowanie, że budowanie każdej strategii mającej definiować kierunki rozwoju państwa, tudzież wybranych obszarów jego funkcjonowania powinno być poprzedzone realizacją zaawansowanego projektu-rozpoznania pozwalającego na klasyczny benchmarking rozwiązań już na świecie funkcjonujących i – finalnie – łatwiejsze wypracowanie tych, które najlepiej sprawdzą się na naszym rodzimym gruncie.

OSINT w bezpieczeństwie państwa to nie tylko zagadnienie związane z szeroko rozumianym pozyskiwaniem informacji przez pracowników sektora publicznego. To zagadnienie – w szerokim ujęciu – dotykające także organizacji publicznych zasobów informacyjnych. Zasobów, które wymagają nie tylko dobrej organizacji, ale też „promocji", rozumianej jako zadbanie o to, by wszyscy pracownicy sektora publicznego pracujący z informacją byli dobrze obeznani z zasobami danych i informacji udostępnianymi przez szereg instytucji publicznych. Takie podejście prowadzić może nie tylko do zwiększenia produktywności pracowników, ale – przede wszystkim – rozwijania ich potenciału poprzez dostęp do danych  i informacji, które mogą wykorzystywać w swojej pracy.

To także moment, w którym wspomnieć należy o bezpieczeństwie informacji publicznej zamieszczonych w rządowych źródłach danych, ale nie tylko na szczeblu infrastrukturalnym. Idzie tu także o perspektywę zadbania o to, jakie dokładnie dane i informacje są publikowane w oficjalnych zasobach i jakie może to za sobą pociągać potencjalne konsekwencje. Jeden z przykładów zasobów, które powinny wzbudzać refleksję jest publikacja wzorów podpisów przedsiębiorców notowanych w KRS, która odbyła się przy okazji udostępniania do informacji publicznej sprawozdań finansowych spółek (co samo w sobie, w perspektywie transparentności życia publicznego jest jak najbardziej chwalebne).

Wszystko to sprowadzać nas powinno nie tylko do refleksji o tym, jak „robić OSINT", by zaadresować interesy państwa pozyskując informacje, ale też, jak zadbać o krajowe zasoby informacyjne.

## Zalety OSINT

OSINT opierany przede wszystkim na zasobach cyberprzestrzeni jest poważnym narzędziem w działaniu na skalę globalną. Jego dużą zaletą jest stosunkowo niski koszt prowadzenia działań, a przy odpowiedniej koordynacji i strategii tych działań, także prawdopodobieństwo wykrycia prowadzonych działań informacyjnych.

Działania opierające się na metodyce białego wywiadu cechuje także mała czasochłonność, a dzięki odpowiednio przygotowanej kadrze specjalistów informacji, także większa produktywność w realizacji zadań związanych z pozyskiwaniem informacji w praktyce.

W perspektywie długofalowej ważną zaletą w szerokim wykorzystywaniu OSINT, zarówno w biznesie jak i instytucjach rządowych, jest jego łatwa adaptowalność do zmieniających się realiów i dynamiki, która w cyberprzestrzeni jest tak intensywna.

## OSINT kontra dezinformacja

Jedną z narastających bolączek funkcjonowania w świecie on-line jest konieczność radzenia sobie z problemem dezinformacji, szumu informacyjnego i fake news. W praktyce oznacza to, że analityk OSINT, podobnie jak każdy internauta, narażony jest na ryzyko pracy przy wykorzystaniu zasobów zmanipulowanych. To także oznacza, że w szczególności osoby odpowiadające za pozyskiwanie i przetwarzanie informacji na potrzeby realizacji celów biznesowych, zadań realizowanych w ramach pracy w instytucjach publicznych (szeroko rozumianych) powinny być wyposażone w najwyższe kompetencje w zakresie analizy i weryfikacji informacji. To także oznacza konieczność wypracowania odpowiedniego poziomu uwrażliwienia na zagrożenia płynące z dezinformacji i możliwość codziennego spotykania się z nierzetelnymi treściami.

Pierwszym punktem wyjścia z sytuacji jest oczywiście zwrócenie uwagi na kluczowe elementy weryfikacji informacji, tj.:

- Autor i jego powiązania, wiarygodność, ekspertyza
- Aktualność treści
- Dokładność w prezentowaniu faktów
- Ocena obiektywizmu
- Ocena poziomu relewancji informacji

Nieodłącznym elementem weryfikacji informacji musi także być analiza kontekstowa pozwalająca na zrozumienie, jakie konsekwencje i dla kogo może mieć publikacja danego materiału, komu mogło zależeć na tym, by publikowane treści wywarły taki, a nie inny skutek. Taki model w podejściu do analizy i weryfikacji informacji wymaga odpowiednio rozwiniętej wrażliwości na potencjalne manipulacje, pewnej dozy sceptycyzmu badawczego i dążenia do konfrontowania ze sobą różnych stanowisk.

**System**

Kompletne, świadome, bezpieczne i strategiczne wykorzystanie dobrodziejstw białego wywiadu w budowaniu przewag konkurencyjnych przedsiębiorstw oraz mocowaniu pozycji państwa na arenie międzynarodowej wymaga szerokiej dyskusji i skoordynowanych działań. Całościowy system powinien odpowiadać nie tylko na pytanie o to, jak pozyskiwać informacje, ale też, jak je dystrybuować wśród interesariuszy, jak definiować wymagania poszczególnych grup odbiorców i zarządzać bezpieczeństwem.
Zasoby informacyjne

Jednym z kluczowych elementów budowania systemu pozyskiwania informacji są jego zasoby informacyjne. Mimo, iż na przestrzeni ostatnich lat organizacja zasobów informacji publicznej w Polsce mocno się poprawiła, wciąż jest wiele do zrobienia, aby praca osób na co dzień korzystających z nich była możliwie jak najbardziej efektywna. To z kolei wymaga precyzyjnego zdefiniowania, jakie są potrzeby poszczególnych grup odbiorców w zakresie dostępu do informacji, co samo w sobie nie jest zadaniem prostym, ale wartym wysiłku.

**Kompetencje**

Naturalnym elementem budowania systemu pozyskiwania informacji jako elementu w infrastrukturze skutecznego zarządzania państwem i kluczowymi podmiotami polskiej gospodarki powinna być edukacja. Szeroko zakrojony, system budowania kompetencji cyfrowych wśród kadr podmiotów ulicznych, pomyślany tak, by gwarantował adekwatny do wykonywanych zadań poziom zaawansowania. Nie każdy pracownik administracji publicznej musi być zobligowany do posiadania zaawansowanej wiedzy i umiejętności z zakresu OSINT, ale każdemu przydadzą się skuteczne techniki wyszukiwania informacji i zrozumienie specyfiki określonych rodzajów zasobów on-line. Odpowiedzią na to zapotrzebowanie może być wdrożenie standardu kompetencji informacyjnych urzędników państwowych (zarówno na szczeblu centralnym jak i samorządowym), uzależnianego od zakresu odpowiedzialności i realizowanych zadań.

**Bezpieczeństwo**

Budowanie kompetencji informacyjnych może być celem samym w sobie, choć nie powinno, Ważne, by konsekwencją nabywania tych kompetencji stała się także większa wrażliwość na cyber-ryzyka, z którymi możemy się spotykać, nie zawsze to sobie uświadamiając. To najbardziej podstawowy, choć niewystarczający wątek zadbania o bezpieczeństwo w systemie OSINT wykorzystywanym w państwie.

**Infrastruktura**

Nie jest tajemnicą, że skuteczny OSINT wymaga wykorzystania technologii. Na skalę globalną dostępne są setki skromniejszych i bardziej rozbudowanych systemów wspierających OSINT. Wciąż jednak brakuje rozwiązania, które pozwalałoby na automatyzację działań OSINTowych w warunkach polskich, przy sprawnej integracji z polskimi zasobami informacyjnymi. Stworzenie modułowego oprogramowania dedykowanego różnym grupom odbiorców-specjalistów informacji funkcjonujących w ramach różnych organów instytucji publicznych byłoby niewątpliwym sukcesem.

**Rekomendacje**

- Konieczne jest zapewnienie wysokiego poziomu kompetencji informacyjnych na wszystkich szczeblach administracji publicznej, będących kluczem do efektywnego wykorzystania OSINT
- Należy uwzględniać OSINT na poziomie państwa i poszczególnych sektorów gospodarki to konieczny etap budowania przez nie strategii rozwoju
- Wykorzystanie pełni potencjału OSINT i jego automa-

tyzacji wymaga zagwarantowania stosowania dedykowanego oprogramowania, dostosowanego do realiów Polski

- Celem skutecznego działania OSINT należy wdrożyć odpowiednie zabezpieczenia przed cyberatakami i dekonspiracją, a tym samym także świadomości specjalistów zajmujących się pozyskiwaniem i monitoringiem informacji.

## Informacje o autorach

**Prof. dr hab. Artur Gruszczak** – Ekspert Fundacji Instytut Bezpieczeństwa i Strategii. Zajmuje się problematyką przestrzeni wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej, współpracy wywiadowczej w Unii Europejskiej, ewolucji współczesnych wojen. Jest pracownikiem naukowym Uniwersytetu Jagiellońskiego, kierownikiem Zakładu Bezpieczeństwa Narodowego. Jest także wykładowcą European Online Academy z siedzibą w Nicei, gdzie prowadzi wykłady na temat „Justice and Home Affairs, migrants and refugees in times of crisis".

**Dr Artur Jagnieża** – Przewodniczący Rady Fundacji Instytut Bezpieczeństwa i Strategii, absolwent Akademii Obrony Narodowej (2003); ukończył studia historyczne na Wydziale Historycznym Uniwersytetu Warszawskiego (1996), studia nauk politycznych na Wydziale Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego (1997) oraz studia podyplomowe obronności państwa na Wydziale Strategiczno- Obronnym AON (1998). Specjalista w dziedzinie obronności, strategii i bezpieczeństwa państwa oraz problematyki zarządzania ciągłością działania, ochrony infrastruktury krytycznej oraz zarządzania kryzysowego.

**Dr Milo Jones** – Ekspert Fundacji Instytut Bezpieczeństwa i Strategii. Jest profesorem wizytującym na Uniwersytecie IE w Madrycie. Prowadzi wykłady z przedmiotów "Narzędzia wywiadowcze dla profesjonalistów z branży finansowej", "Geopolityka" i "Sposoby podejścia do złożonych problemów" w programach MBA, Masters in Advanced Finance, Masters in Cybersecurity i Executive Education. Jest członkiem Centrum Studiów nad Cyfrowym Życiem, amerykańskiej strategicznej grupy badawczej o charakterze non-profit, zajmującej się zrozumieniem wpływu technologii cyfrowych na cywilizację.

**Dr Mateusz Kolaszyński** – Ekspert Fundacji Instytut Bezpieczeństwa i Strategii. Jest absolwentem, Uniwersytetu Jagiellońskiego. W 2015 r. obronił pracę doktorską pt. „Status ustrojowy polskich służb specjalnych po 1989 roku". Jest pracownikiem naukowym w Zakładzie Bezpieczeństwa Narodowego UJ. Jego zainteresowania naukowe koncentrują się wokół miejsca i roli służb specjalnych w państwach demokratycznych.

**Płk (rez.) Grzegorz Małecki** – Prezes Zarządu i jeden z twórców Fundacji Instytut Bezpieczeństwa i Strategii. Dysponuje rozległą i wszechstronną wiedzą oraz bogatym doświadczeniem w dziedzinie bezpieczeństwa narodowego. Jest absolwentem Instytutu Historii na Uniwersytecie Wrocławskim (mgr 1991). W latach 1991 – 2017 (z przerwami) płk Małecki służył w UOP, ABW i AW, obejmując w nich kolejne stanowiska kierownicze. W latach 2015 – 2016 pełnił funkcję szefa Agencji Wywiadu. W okresie 2005 – 2008, jako Sekretarz Kolegium ds. Służb Specjalnych w Kancelarii Prezesa rady Ministrów, organizował i kierował pracami tego organu nadzorującego działalność polskiej wspólnoty wywiadowczej. Wykładowca akademicki, autor licznych publikacji, uczestnikiem szeregu krajowych i zagranicznych konferencji poświęconych zagadnieniom wywiadu, bezpieczeństwa narodowego, cyberbezpieczeństwa, zarządzania systemami wywiadowczymi, bezpieczeństwa energetycznego, stosunków międzynarodowych, kontroli i audytu.

**Grzegorz Matyasik** – Zastępca Dyrektora Departamentu Analiz Przygotowań Obronnych Administracji w KPRM. W latach 2017  - 2018 w MON jako m.in. koordynator projektu Legia Akademicka – ochotniczego szkolenia studentów. Od jest 1992 członkiem jednej z ogólnopolskich organizacji strzeleckich, a od 2011 do 2017 roku Prezes Zarządu stowarzyszenia  ObronaNarodowa.pl Ruch na Rzecz Obrony Terytorialnej. Redaktor Naczelny portalu ObronaNarodowa.pl.

**Ppłk rezerwy Czesław Rybak** – Ekspert Fundacji Instytut Bezpieczeństwa i Strategii. Specjalista w zakresie bezpieczeństwa narodowego, ze szczególnym uwzględnieniem bezpieczeństwa energetycznego. Z uwagi okres dwudziestoletniej służby w UOP, SG i ABW (1993-2014), oraz sprawowanie w przeszłości funkcji dyrektora Departamentu Bezpieczeństwa w PGNiG S.A. i prowadzenie obecnie Biura Bezpieczeństwa Informacji dysponuje rozległą wiedzą i doświadczeniem w zakresie ochrony informacji niejawnych.

**Justyna Trzeciakowska** – Ekspert Fundacji Instytut Bezpieczeństwa i Strategii. Specjalista i trener z zakresu OSINT, infobroker. Współwłaścicielka agencji Infobrokerska.pl, szkoleniowiec Krajowej Szkoły Administracji Publicznej, współpracuje jako wykładowca z Uniwersytetem Pedagogicznym w Krakowie, Uniwersytetem Jagiellońskim i Uniwersytetem im. Marii Curie-Skłodowskiej w Lublinie. Realizuje specjalistyczne szkolenia z zakresu OSINT dla sektora prywatnego i instytucji rządowych. Doświadczenie w zakresie OSINT buduje i rozwija od lat, realizując projekty doradcze i rozwojowe dla biznesu.