aut. Fundacja Instytut Bezpieczeństwa i Strategii
06.08.2019

WYWIAD 3.0, CZYLI SŁUŻBY WYWIADOWCZE W CZASACH GLOBALNEGO PRZYSPIESZENIA

Domeną wywiadu od zawsze była informacja. Traktowana jako „surowiec" wydobywany zazwyczaj z trudno dostępnych lub ściśle strzeżonych pokładów, w wyniku „obróbki" przybierała postać gotowego „produktu" dostarczającego wiedzy o wybranym fragmencie rzeczywistości. Tradycyjnie wywiad zorganizowany był wzdłuż „łańcucha wiedzy": od pierwotnych danych przez przetworzone informacje, całościową wiedzę, aż po mądrość decydentów wyznaczających cele wywiadu i korzystających z uzyskanej wiedzy. Zracjonalizowane, podlegające twierdzeniom logiki, procesy myślowe stanowiły podstawę nie tylko oglądu rzeczywistości, ale też przewidywania i prognozowania.

Dziś klasyczny łańcuch wiedzy rozpada się, a może bardziej zapętla, rozciąga i rozszczepia. Każdy z jego elementów ulega przeobrażeniu w wyniku działania trzech kluczowych czynników: tempa (prędkości), skali i złożoności. Dane jako kody odzwierciedlające strukturę rzeczywistości generowane są w stale rosnącym tempie w coraz bardziej sztucznym (zwirtualizowanym, symulowanym) środowisku. Informacja tworzona jest w coraz większym stopniu przez zmechanizowane systemy przetwarzania danych, sterowane za pomocą sztucznej inteligencji. Wiedza o rzeczywistości łączy elementy faktyczne i wymyślone (wyobrażone), na dodatek z pominięciem trybu weryfikacji z zastosowaniem obiektywnych kryteriów rozstrzygających o ich prawdziwości lub fałszywości. Mądrość decydentów ustępuje przesłankom ideologicznym i nakazom politycznym. Jeszcze częściej jest ofiarą bezradności w obliczu wymogu podjęcia decyzji na podstawie niepełnej lub niezweryfikowanej wiedzy. Tempo generowania informacji przez elektroniczne urządzenia telekomunikacyjnej, wprowadzania ich do globalnego obiegu za pośrednictwem Internetu i serwisów społecznościowych, a także dodawania informacji pokrewnych, oszałamia zwykłych użytkowników oraz przyprawia o ból głowy decydentów. Skala i zasięg informacji to istne cyfrowe tsunami. Co sekundę do Internetu wprowadzanych jest 90 GB danych. Nikt nie jest w stanie ocenić, jaki odsetek stanowią „fake news", czyli dane niesprawdzone, sfałszowane, lub spreparowane w celu dezinformacji.

Wywiad nowej generacji jako odpowiedź na wyzwania współczesności

Wizje roztaczane ponad pół wieku temu przez prekursorów cybernetyki, telekomunikacji digitalizacji i informatyki stają się rzeczywistością. Zawrotne tempo rozwoju technologii informacyjnych i komunikacyjnych wymusza głębokie przeobrażenia współczesnego państwa, społeczeństwa, gospodarki i kultury. Technologie nie rozwiązują problemów bezpieczeństwa – technologie mnożą te problemy wskutek rosnących wzajemnych powiązań i ograniczoności pojedyncznych rozwiązań. Co więcej, użytkownicy tych technologii, wskutek ignorancji lub specjalistycznych umiejętności, pogłębiają problemy i zagrożenia związane z transformacją cywilizacji w kierunku „wspólnoty infosferycznej".

Czytaj też: Emerytura po 25 latach, płatne nadgodziny i związkowy pluralizm. Senat za zmianami w służbach mundurowych

Przedmiotem transformacji są także służby wywiadowcze, nawet jeśli nie dostrzegają dokonujących się zmian w otaczającej je rzeczywistości, albo − mając tego świadomość – liczą na gładkie i bezbolesne dopasowanie się do nowych warunków. Tymczasem przed funcjonariuszami władzy państwowej piętrzą się wyzwania, w przeważającej mierze dotyczące różnych aspektów bezpieczeństwa: socjalnych, zdrowotnych, gospodarczych, informatycznych, by wymienić te najbliższe przeciętnemu obywatelowi. Rośnie ryzyko ataków cybernetycznych, zwiększa się skala zagrożeń ze strony przestępczości, także tej o zorganizowanym charakterze i międzynarodowym zasięgu. Nie ustała groźba zamachów terrorystycznych, mimo spadku ich częstotliwości. Świat w całej złożoności staje się coraz trudniejszy do obserwacji, analizy i oceny pod kątem czynników stabilności i destabilizacji, rodzącej zagrożenia i problemy bezpieczeństwa. Służby wywiadowcze w obliczu tych wyzwań muszą dokonać poważnej przebudowy w kierunku wywiadu nowej generacji.

W związku z tym muszą uwzględnić następujące wyzwania:

1. Wzrastającą złożoność współczesnego środowiska bezpieczeństwa ułatwiającą rozprzestrzenianie się zagrożeń.
2. „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.
3. Rozwój technologii wytwarzania, pozyskiwania, przetwarzania i analizy danych, tworzenie algorytmów generujących przekaz treściowy, ekspansję systemów sztucznej inteligencji i uczenia maszynowego w oparciu o sieci neuronowe, masowe wykorzystanie botów, inteligentnych asystentów, crowdsourcingu.
4. Rosnącą rolę technologii wspierających procesy tworzenia wiedzy w oparciu o zastosowania sztucznej inteligencji, zwłaszcza w zakresie drążenia danych wielkoskalowych (big data), przetwarzania informacji oraz generowania syntetycznej wiedzy stanowiącej podstawę analiz wywiadowczych.
5. Ekspansję sieci głębokiej (deep web) i ukrytej (dark net) powiązaną ze wzrostem przestępczości i bezpośrednich zagrożeń dla państwa i jego obywateli.
6. Wielopoziomowość struktur decyzyjnych (w wymiarze wewnętrznym i międzypaństwowym); zwiększającą 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).
7. Komercjalizację bezpieczeństwa; rosnącą ofertę usług analityczno-rozpoznawczych ze strony firm prywatnych; outsourcing, czyli zlecanie pewnych czynności analitycznych podmiotom prywatnym.

Podobnie jak w przypadku kolejnych generacji wojen, które zastępując poprzednie przejmowały wiele ich cech, wywiad trzeciej generacji łączy dotychczasowe funkcje, cele i rozwiązania organizacyjne z nowymi technologiami i innowacjami społecznymi, gospodarczymi, kulturowymi i świadomościowymi. Pierwsza generacja skupiała się na zdobywaniu tajnych informacji przez siatki szpiegowskie, dostarczanych wąskiemu kręgowi decydentów. Wywiad drugiej generacji opierał się na rozbudowanej strukturze instytucjonalnej oraz różnorodnych zracjonalizowanych narzędziach i metodach pozyskiwania i przetwarzania informacji i danych. Wywiad 3.0 to złożony system zarządzania danymi angażujący technologie sztucznej inteligencji w celu opanowania chaosu komunikacyjnego poprzez minimalizację prawdopodobieństwa błędu w ocenie rzeczywistości. Łączy tradycyjne metody zdobywania informacji ukrytych (niejawnych) z wielkoskalowym pozyskiwaniem i przetwarzaniem danych i informacji jawnoźródłowych. Wiąże zadania i działania wywiadowcze z kontrwywiadem skupionym na ochronie infrastruktury krytycznej i kluczowych zbiorów danych leżących w gestii

zarówno organów administracji publicznej, w szczególności państwowej, jak i podmiotów prywatnych (gospodarczych, socjalnych, zdrowotnych). Funkcjonuje w stałym związku z rynkiem usług informacyjnych, w szczególności firmami oferującymi informacje pozyskiwane w oparciu o własne zasoby ludzkie i techniczne (tzw. prywatne wywiadownie), jak też produkty analityczne tworzone w oparciu o otwarte zbiory danych i informacje jawne. Podstawowym celem wywiadu 3.0 jest doskonalenie umiejętności przewidywania zachowań podmiotów indywidualnych i zbiorowych pod kątem wykrywania potencjalnych, możliwych i prawdopodobnych zagrożeń bezpieczeństwa.

Zadania stojące przed aparatem wywiadowczym RP

W obliczu zarysowanych powyżej cech rzeczywistości oraz wyzwań, przed którymi stoją współczesne państwa i społeczeństwa, służby wywiadowcze każdego państwa muszą podjąć zadanie gruntownej przebudowy w sferze organizacyjnej, mentalnej i technicznej zgodnie z kluczowymi interesami państwa i narodu określonymi w strategii bezpieczeństwa narodowego. W odniesieniu do Rzeczypospolitej Polskiej, wiąże się to z kilkoma obszarami działań.

Określenie strategicznych priorytetów i podstawowych obszarów działań służb wywiadowczych, 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.

Budowa systemu zintegrowanej krajowej oceny sytuacyjnej.

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.

Rozbudowa zdolności identyfikowania zewnętrznych źródeł ryzyka i zagrożeń.

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.

Czytaj też: Służby mundurowe finansowane jak wojsko? NIK o modernizacji formacji podległych MSWIA

Rozwój, zastosowanie 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.

Czytaj też: Kto pilnuje naszej prywatności? Podsłuchy bez kontroli

Kształtowanie świadomej odpowiedzialności decydentów za bezpieczeństwo narodowe.

Aparat wywiadowczy służy narodowi reprezentowanemu przez najwyższe organy prawomocnej władzy państwowej. Na najwyższych przedstawicielach tych organów, zwłaszcza władzy wykonawczej, spoczywa odpowiedzialność nie tylko za rzetelne, zgodne z prawem wykonywanie przyznanych im uprawnień, ale i za kompetentne korzystanie z ocen, analiz i innych zasobów wiedzy dostarczanych przez aparat wywiadowczy. Nawet najdokładniejsze analizy wywiadowcze i raporty sytuacyjne mogą pozostać bezużyteczne, jeżeli zostaną zlekceważone, opacznie zrozumiane lub zmanipulowane przez decydentów. Brak szacunku decydentów dla wysiłku włożonego przez służby wywiadowcze, oczekiwanie uproszczonego obrazu sytuacji i łatwego przełożenia wiedzy analitycznej na decyzje, a także konformizm ze strony kierownictwa wywiadu i kontrwywiadu w stosunku do zwierzchnika reprezentującego państwo polskie mogą zrujnować wysiłki włożone w przebudowę służb w kierunku modelu wywiadu 3.0. Prawidłowa współpraca między decydentami a służbami wywiadowczymi musi opierać się na wzajemnym szacunku i zrozumieniu oraz odrzuceniu pokusy narzucania swego zdania, bezkompromisowego wzajemnego traktowania i – co najgorsze – wzajemnego rozgrywania ze szkodą dla interesów bezpieczeństwa narodowego. Kluczowym warunkiem jest odpolitycznienie systemu kierowania aparatem wywiadowczym oraz uznanie nadrzędności interesów narodowych nad interesem partyjnym.

Perspektywa powstania wywiadu 3.0 jest sprawą bieżącą. Proces ten toczy się w różnych wymiarach, skali i tempie w wielu państwach, zarówno mocarstwach światowych, jak też państwach pretendujących do roli mocarstw regionalnych. Polska jako kraj średni nie może zlekceważyć tego procesu. Przeciwnie – musi jak najszybciej włączyć się w nurt przeobrażeń poświęcając im znacznie więcej uwagi, woli politycznej, a także – a może przede wszystkim – nakładów materialnych i finansowych. Globalne przyspieszenie preferuje dużych, aktywnych graczy i łatwo degraduje pozostałych do roli outsiderów. Bierność i impas decyzyjny prowadzi do marginalizacji państwa i przekształcenia go w instrument w rękach światowych mocarstw.

Prof. dr hab. Artur Gruszczak jest ekspertem Fundacji Instytut Bezpieczeństwa i Strategii