Przegląd wyzwań strategicznych

01. prof. Jacek Czaputowicz

Bezpieczeństwo niemilitarne - znaczenie i zakres

02. dr Paweł Turowski

Wyzwania dla polskiego bezpieczeństwa energetycznego

03. Przemysław Sypniewski

Bezpieczeństwo logistyki i nowa geografia bogactwa

04. dr Piotr Gontarczyk

W historii wojna trwa

05. dr Marek Dietl

Finansowa rewolucja u bram III RP

06. Paweł Wiszniewski

Cyberbezpieczeństwo państwa

07. dr Bolesław Piasecki

Bezpieczeństwo informacyjne Polski wobec rozwoju technologii

POLSKA WIELKI PROJEKT

Bezpieczeństwo niemilitarne Polski

Bezpieczeństwo niemilitarne – znaczenie i zakres

prof. Jacek Czaputowicz

W tradycyjnym rozumieniu bezpieczeństwo dotyczyło wolności od zagrożenia zewnętrznego i wojny. Po zakończeniu zimnej wojny obserwujemy „rozszerzenie" tego terminu na kwestie niemilitarne. Dostrzeżono, że wiele zagrożeń ma charakter transnarodowy, a przeciwstawienie się im wymaga współpracy międzynarodowej. Źródłem zagrożeń stały się konflikty o niskiej intensywności, konflikty wewnątrzpaństwowe i terroryzm. Na bezpieczeństwo wpływają kwestie gospodarcze, środowiskowe, niekontrolowane migracje i przestępczość zorganizowana.

Natura bezpieczeństwa

Bezpieczeństwo oznacza stan spokoju, pewności, który daje brak poczucia zagrożenia. Wymiar wewnętrzny odnosi się do zjawisk występujących w polityce wewnętrznej, gospodarczej i społecznej, natomiast wymiar zewnętrzny – do relacji z innymi państwami. Określanie bezpieczeństwa w kategoriach militarnych dotyczy zabezpieczenia narodu przed groźbą podboju przez zewnętrzną potęgę. Państwo oddziałuje na sferę wewnętrzną i otoczenie zewnętrzne, by oddalać zagrożenia dla bezpieczeństwa. Jest ono bezpieczne, kiedy nie musi poświęcać wyznawanych wartości, takich jak przetrwanie, integralność terytorialna, niezależność polityczna i jakość życia, oraz gdy jest w stanie wartości te obronić w walce zbrojnej.

Gdy mówimy, że bezpieczeństwo jest wartością brzegową, rozumiemy przez to, że jego wartość zależy od podaży i popytu. Wartość bezpieczeństwa dla poszczególnych państw zależy nie tylko od tego, jak dużo bezpieczeństwa potrzebują, ale także od tego, jak dużo bezpieczeństwa już mają. Im czujemy się bezpieczniejsi, tym mniej bezpieczeństwa pożądamy i tym mniejszą ma dla nas wartość. Bezpieczeństwo ma np. większą wartość dla Polski niż dla Niemiec, które nie czują się zagrożone w takim samym stopniu co my, przez co są skłonne przeznaczać relatywnie mniej środków na obronę.

Sektory bezpieczeństwa

Systematyzacji bezpieczeństwa jako pierwszy dokonał Barry Buzan. Poza bezpieczeństwem militarnym wyróżnił także bezpieczeństwo polityczne, społeczno-kulturowe, ekonomiczne i ekologiczne.

Bezpieczeństwo militarne odnosi się do zagrożeń dla integralności terytorialnej państwa, jego ludności i zasobów, czyli do agresji zbrojnej. Przedmiotem zainteresowania są tradycyjnie przyczyny wojen, znaczenie broni nuklearnej i strategie odstraszania. Po zakończeniu zimnej wojny ujawniły się zagrożenia o charakterze asymetrycznym, występujące wtedy, gdy słabsza strona konfliktu stosuje techniki i metody nieprzystające do sposobu prowadzenia walki przez silniejszego przeciwnika. Przeciwdziałanie zagrożeniom asymetrycznym wymaga ścisłej współpracy międzynarodowej oraz różnych rodzajów sił zbrojnych, dyplomacji, wywiadu, kontrwywiadu, policji i administracji.

Bezpieczeństwo polityczne odnosi się do zagrożeń dla stabilności społecznej państw i rządów. Dotyczy suwerenności wewnętrznej państwa, czyli sprawowania przez jego władze kontroli na określonym terytorium. Zagrożenia dla bezpieczeństwa politycznego stanowią takie niebezpieczeństwa jak międzynarodowy terroryzm, transnarodowa przestępczość zorganizowana czy wykorzystanie do ataku technologii informatycznych.

Terroryzm jest formą politycznej przemocy, ukierunkowaną na zabijanie niewinnych ludzi w celu realizacji postulatów politycz-

nych. Jest on godny potępienia na gruncie etycznym, ponieważ celowo wymierzony jest w przypadkowych ludzi i w ten sposób łamie normę immunitetu przynależnego osobom niebiorącym udziału w walce. Sposoby przeciwdziałania terroryzmowi zależą od tego, jakie ramy nadajemy temu zagrożeniu. Gdy określimy terroryzm jako wojnę, rozwiązaniem będą działania militarne, gdy jako działalność kryminalną, właściwym rozwiązaniem będzie wprowadzanie prawa za pomocą sił policyjnych.

Przestępczość zorganizowana to z kolei aktywność motywowana dążeniem do osiągnięcia nielegalnych dochodów. Różnica między terroryzmem a przestępczością zorganizowaną polega na tym, że terroryści dążą do zmiany politycznej, np. rewolucji lub secesji państwa, natomiast przestępcy mają interes w dobrze prosperującym społeczeństwie, a nie w obaleniu rządu. Przestępczość zorganizowaną cechują trwały charakter, duża ranga dokonywanych przestępstw oraz poważne skutki społeczne. Działalność przestępcza koncentruje się na handlu bronią, narkotykami i ludźmi, zwłaszcza kobietami w celu zmuszania ich do prostytucji.

Bezpieczeństwo społeczno-kulturowe dotyczy tożsamości społeczności narodowych i etnicznych. Źródłem tożsamości jest wspólnota, która różni się od innych wspólnot językiem i kulturą. Zagrożenia dla tożsamości mogą być wynikiem ograniczenia swobody wypowiadania się, używania języka ojczystego, ograniczenia edukacji czy kultu religijnego, a także zakazu pisowni nazwisk w języku ojczystym. W dłuższym czasie mogą one prowadzić do ograniczenia reprodukcji danej tożsamości narodowej lub etnicznej. Bezpieczeństwo dotyczy w tym przypadku grupy społecznej wewnątrz państwa, np. polskiej mniejszości na Białorusi czy na Litwie. Gdy granice państwa i wspólnoty są zbieżne, bezpieczeństwo państwa i bezpieczeństwo społeczno-kulturowe są tożsame. Natomiast kiedy te granice się nie pokrywają, a państwo dąży do asymilacji mniejszości narodowych, bezpieczeństwo państwa i bezpieczeństwo grupy kolidują ze sobą.

Zagrożenie dla bezpieczeństwa społeczno-kulturowego stanowi migracja, która może prowadzić do zmiany etnicznego, kultu-

rowego i językowego składu ludnościowego. Może ona też pobudzać konkurencję o rzadkie zasoby, takie jak edukacja i służba zdrowia. Z kolei spójność społeczna mniejszości etnicznej może podważać bezpieczeństwo państwa, na przykład litewskość państwa litewskiego może być postawiona pod znakiem zapytania przez istnienie silnej polskiej mniejszości narodowej. Zagrożenie dla tożsamości ma często charakter subiektywny, tworzone jest w procesie społecznym.

Pojęcie ***bezpieczeństwa ontologicznego*** dotyczy podmiotowości, posiadania odrębnej tożsamości, czyli subiektywnego poczucia kim się jest. Być ontologicznie bezpiecznym oznacza posiadać odpowiedzi na fundamentalne pytania egzystencjalne. Gdy bezpieczeństwo fizyczne państwa dotyczy jego suwerenności, bezpieczeństwo ontologiczne odnosi się do realizacji podmiotowości poprzez stabilizowanie tożsamości i rutynizowanie relacji z innymi państwami. Brak bezpieczeństwa ontologicznego prowadzi do zakłóceń w rozróżnieniu rzeczywistych zagrożeń.

Państwo może czuć się ontologicznie bezpieczne mimo występowania konfliktu. Dążenie do określenia swojej tożsamości i zapewnienia bezpieczeństwa ontologicznego mogą wręcz wymagać podtrzymywania konfliktu z innym państwem. Przedłużenie konfliktu może służyć podtrzymywaniu tożsamości państwa i w ten sposób umacniać bezpieczeństwo ontologiczne. Badacze wskazują, że dylemat bezpieczeństwa ontologicznego występuje w konfliktach na Bałkanach, na Kaukazie czy w relacjach między Izraelem a Palestyną.

Koncepcja bezpieczeństwa ontologicznego może być zastosowana do wyjaśnienia relacji Polski z naszymi sąsiadami, zwłaszcza z Ukrainą. Dążenie do umocnienia tożsamości zarówno Polski, jak i Ukrainy, które jest warunkiem bezpieczeństwa ontologicznego tych państw, stoi w sprzeczności z rozwiązaniem sporów historycznych i oparcia relacji na bazie pojednania i współpracy. Podobnie dyskusja o reparacjach po II wojnie światowej służyć może umocnieniu bezpieczeństwa ontologicznego Polski w relacjach z Niemcami.

Bezpieczeństwo ekonomiczne odnosi się do zagrożeń dla dobrobytu. Obejmuje ono takie zagadnienia jak bezpieczeństwo dostaw surowców i żywności, dostęp do rynków, bezpieczeństwo finansowe

i techniczno-przemysłowe oraz dotyczące utrzymania zdolności produkcyjnych na potrzeby militarne. W ostatnim czasie szczególne znaczenie ma zapewnienie dostaw minerałów rzadkich i półprzewodników. Częścią bezpieczeństwa ekonomicznego jest bezpieczeństwo energetyczne określane jako zdolność państwa do funkcjonowania bez poważnych zaburzeń. Chodzi o zapewnienie dostaw surowców energetycznych, takich jak gaz i ropa naftowa.

Bezpieczeństwo ekologiczne dotyczy z kolei zachowania środowiska naturalnego na poziomie koniecznym dla rozwoju ludzkości – powietrza, wody, gleby, wszystkich żywych organizmów oraz zasobów archeologicznych i kulturowych. Zmiany środowiskowe stanowią ryzyko dla ekosystemu i jakości życia ludzi. Zagrożenia dla środowiska obejmują klęski naturalne, takie jak powodzie, trzęsienia ziemi czy tsunami, oraz zagrożenia związane z działalnością człowieka, czyli katastrofy czy wyjaławianie gleby. Zagrożenia występują w postaci kwaśnych deszczy, powodzi, suszy, cofania się lasów, utraty biologicznej różnorodności, rozprzestrzeniania się produktów toksycznych i epidemii, takich jak COVID-19.

Sekurytyzacja

Sekurytyzacja oznacza zakwalifikowanie jakiejś dziedziny do sfery bezpieczeństwa w celu uzasadnienia podjęcia nadzwyczajnych środków. Zagrożenie jest aktem deklaratywnym, wynikiem dyskursu, narracji i oddziaływania państwa. Sekurytyzacja polega na wzbudzeniu przekonania, że tylko wyjątkowe środki zapobiegną tym zagrożeniom oraz że trzeba je podjąć teraz, zanim będzie za późno.

Przedmiotem badania jest wpływ na bezpieczeństwo takich kwestii jak migracje, polityka azylowa czy działania antyterrorystyczne. Część badaczy utrzymuje, że bezpieczeństwo jest „tworzone", by służyć określonym celom państw. Państwo staje się społecznością polityczną poprzez wprowadzanie podziału na swoich i obcych, zwykle kosztem bezpieczeństwa innych państw i wewnętrznych dysydentów. Bezpieczeństwo jest postrzegane jako stan naruszający normalny porządek polityczny, a jego rozszerzenie na nowe dziedziny niesie

za sobą potencjalnie negatywne konsekwencje w postaci ograniczania swobód demokratycznych.

Ujmowanie migracji w kategoriach bezpieczeństwa łączy izolowane heterogeniczne zjawiska, takie jak migracja, fundamentalizm religijny, terroryzm, narkotyki i europejski rynek wewnętrzny, w jedną całość, określaną mianem pola bezpieczeństwa. Język nie jest więc w tym przypadku tylko instrumentem komunikacji służącym opisowi świata rzeczywistego, jest także siłą łączącą określone praktyki w instytucjonalne ramy.

Występuje pewna prawidłowość – wraz ze wzrostem prawdopodobieństwa wystąpienia zagrożenia, spada jego destrukcyjność. Prawdopodobieństwo wybuchu wojny nuklearnej jest bardzo niskie. Gdyby jednak do niego doszło, skutek byłby bardzo destrukcyjny. Bardziej prawdopodobne jest wystąpienie zagrożeń dla sektora politycznego, takich jak terroryzm i konflikty etniczne, są one jednak mniej destrukcyjne niż konflikty militarne. Jeszcze bardziej prawdopodobne jest wystąpienie zagrożeń ekonomicznych i ekologicznych, które w krótkim okresie są jednak mniej destrukcyjne. Zagrożenia w sektorze społecznym, takie jak niekontrolowana migracja, przestępczość zorganizowana, handel narkotykami, są jeszcze bardziej prawdopodobne, lecz dla państwa relatywnie mniej destrukcyjne.

Strategia Bezpieczeństwa Narodowego RP

Uznanie zagrożeń niemilitarnych dla bezpieczeństwa Polski znajduje odzwierciedlenie w dokumentach strategicznych. Już w Strategii Bezpieczeństwa Narodowego RP z 2007 r. bezpieczeństwo narodowe zostało określone jako obejmujące zarówno kwestie militarne, jak i polityczne, społeczne oraz ekologiczne. Z kolei ostatnia Strategia Bezpieczeństwa Narodowego RP z 2020 r. obejmuje – obok kwestii militarnych i współpracy sojuszniczej – kwestie dotyczące bezpieczeństwa niemilitarnego. Postuluje się w niej prowadzenie działań na rzecz umacniania tożsamości narodowej i ochrony dziedzictwa narodowego, zakorzenionego w wartościach chrześcijańskich i uniwersalnych. Strategia przewiduje też prowadzenie skutecznej polityki

migracyjnej, skoordynowanej z polityką gospodarczą i społeczną, m.in. poprzez integrację migrantów ze społeczeństwem, co ma służyć zachowaniu spójności społecznej.

Inne cele określone w Strategii to zapewnienie rozwoju społecznego i gospodarczego, ochrona środowiska i przeciwdziałanie zagrożeniom epidemiologicznym. Wzmocnienie bezpieczeństwa ekonomicznego ma nastąpić poprzez wzmacnianie odporności na międzynarodowe kryzysy finansowe i prowadzenie działań prorozwojowych. Ważnym obszarem jest też bezpieczeństwo energetyczne, które ma być zapewnione poprzez zabezpieczenie dostaw tradycyjnych źródeł energii – ropy naftowej i gazu ziemnego – oraz rozwój źródeł alternatywnych. Zapewnienie bezpieczeństwa ekologicznego dotyczy natomiast m.in. działań na rzecz ochrony zasobów wodnych, koniecznych dla zapewnienia bezpieczeństwa żywnościowego, walki ze smogiem, wykorzystywania paliw alternatywnych i źródeł bezemisyjnych oraz rozwoju elektromobilności. Polska będzie też dążyć do realizacji celów klimatycznych uzgodnionych na forum organizacji międzynarodowych.

Można podsumować, że wraz ze spadkiem prawdopodobieństwa wybuchu tradycyjnej wojny międzypaństwowej rośnie znaczenie działań asymetrycznych i hybrydowych, które stanowią poważne wyzwanie dla bezpieczeństwa państwa. Bezpieczeństwo jest coraz częściej postrzegane w kategoriach niemilitarnych, obejmuje kwestie polityczne, społeczno-kulturowe, ekonomiczne i ekologiczne. Takie rozszerzenie rozumienia bezpieczeństwa znajduje odzwierciedlenie w dokumentach strategicznych, w tym w ostatniej Strategii Bezpieczeństwa Narodowego RP.

Wyzwania dla polskiego bezpieczeństwa energetycznego

dr Paweł Turowski

Najważniejsze wyzwania dla bezpieczeństwa energetycznego Polski wynikają z wywołanej polityką Unii Europejskiej transformacji polskiej energetyki oraz polityką Rosji wykorzystującą surowce energetyczne, w tym gaz, do dominacji nad Polską i państwami regionu Europy Środkowej.

Przebudowa polskiej energetyki w ciągu najbliższych trzydziestu lat została wywołana polityką transformacji energetycznej Unii Europejskiej. Wraz z objęciem stanowiska szefowej Komisji Europejskiej przez Ursulę von der Layen doszło do przekształcenia sektorowej polityki na rzecz klimatu i energii w Europejski Zielony Ład, czyli wielowymiarową strategię gospodarczą i przemysłową, której rdzeniem jest ochrona klimatu. Pochodną tych działań było podwyższenie skali redukcji gazów cieplarnianych do 55 proc. do 2030 r., co stanowi 15-procentowe podniesienie celu. Ma to bezpośredni wpływ na znaczące zwiększenie wydatków na technologie bezemisyjne. Tak zaprojektowana polityka wymusza zbliżanie się wielu sektorów gospodarki dotychczas luźno ze sobą powiązanych. Sektor energetyczny zacznie przenikać się z transportowym, hutniczym, stalowym czy nawet chemicznym. Nowa europejska polityka skutkuje przede wszystkim wielkoskalowym rozwojem odnawialnych źródeł energii oraz odchodzeniem od ropy naftowej w transporcie samochodowym, kolejowym, lotniczym, morskim, produkcją gazów syntetycznych m.in. wodoru

jako czystego paliwa dla transportu, przemysłu hutniczego, stalowego, nawozowego i chemicznego. Spowoduje to na masową skalę rozwój nowych technologii, których urynkowienie jest możliwe wyłącznie dzięki wsparciu finansów publicznych (dotacje, gwarancje, umarzane pożyczki etc.) na dotychczas niespotykaną skalę. Taką ścieżką będą rozwijały się morska i lądowa energetyka wiatrowa, technologie fotowoltaiczne, produkcja wodoru bez paliw kopalnych. Europejski Zielony Ład nie mógłby zostać wdrożony m.in. bez funduszy wspólnotowych, a jest to ok. 30 proc. najbliższego budżetu Unii Europejskiej (tzw. wieloletniej perspektywy finansowej na lata 2021-2027). Europejski Bank Inwestycyjny przekieruje na ten cel od połowy obecnej dekady połowę wszystkich udzielanych kredytów. To doprowadzi do strumienia 1 bln euro w ciągu najbliższych dziewięciu lat na transformację energetyczną.

Kolejną dźwignią jest 30 proc. Funduszu Odbudowy (Next Generation EU przyjęty w 2022 r. dysponujący ponad 723 mld euro). Fundusz ustanowiono jako swego rodzaju dźwignię pobudzającą gospodarki państw Wspólnoty w kryzysie i recesji wywołanej pandemią COVID-19. Środki funduszu będą wydatkowane zgodnie z priorytetami Europejskiego Zielonego Ładu. Tak zaprojektowane ramy polityki transformacji energetycznej stanowią poważne wyzwanie dla nadrabiających dystans cywilizacyjny państw (takich jak Polska oraz pozostałe kraje Europy Środkowej) oraz budują strukturalną przewagę państw najsilniejszych. Trudno nie zauważyć, że polityki UE czynią największym beneficjentem Niemcy, w których przemysł odnawialnych źródeł energii stał się największym silnikiem wzrostu gospodarczego, daleko istotniejszym niż przemysł samochodowy czy elektrotechniczny.

Polskie priorytety – atom i energetyka gazowa

Otoczenie regulacyjne, prawne oraz finansowe wytycza granice, w jakich będzie przeprowadzona transformacja energetyczna w Polsce. Wyraźnie są widoczne dwa kluczowe założenia, jakie legły u podstaw nowo projektowanego systemu energetycznego państwa polskiego.

Pierwszy z nich odnosi się do kluczowego dylematu rozwojowego: jak zaprojektować transformację energetyczną, aby w długim horyzoncie czasowym nie zahamowała wysokiego tempa wzrostu gospodarczego (niezbędnego dla realizacji kluczowego celu, jakim jest wzrost zamożności i dobrobytu Polaków). Zagrożenie dla trwałego spowolnienia wzrostu zostało zaszyte w transformacji energetycznej. Uruchamia bowiem na niespotykaną dotychczas skalę strumień wydatków publicznych i prywatnych na cele niepriorytetowe dla nadrabiającego zapóźnienia cywilizacyjne państwa. Przyjęty przez rząd dokument strategiczny – Polityka energetyczna Polski do 2040 r. (PEP 2040) – szacuje, iż w ciągu najbliższych dwudziestu lat transformacja energetyczna będzie wymagała ok. 1,6 bln zł zaangażowania kapitałowego. W tej kwocie mieszczą się inwestycje w sektorach paliwowo-energetycznych w wysokości ok. 867-890 mld zł. Nakłady w nowe urządzenia do wytwarzania energii elektrycznej to 320-342 mld zł (ok. 80 proc. zostanie przeznaczonych na budowę odnawialnych źródeł energii oraz na energetyki jądrowe). Dokument wskazuje także, że na skutek wyżej wymienionych głębokich przekształceń sektora paliwowo-energetycznego nieuchronna będzie podwyżka cen energii. Wiele inwestycji uzyska wsparcie finansowe (operacyjne i inwestycyjne), co przyczyni się do szybszego tempa i większej skali. Jednocześnie wyraźnie sformułowano cel społeczny transformacji, że ceny energii mają być akceptowalne społecznie oraz nie mogą pogłębiać ubóstwa energetycznego obywateli. Co ilustrują przytoczone dane finansowe na temat kosztów transformacji? Że 1,6 bln zł na transformację energetyczną państwa do 2040 r. to prawie 69 proc. Produktu Krajowego Brutto Polski z 2020 r. (statystyczna wartość PKB wyniosła 2323,9 mld zł). To w uproszczeniu oznacza, że przez najbliższe niespełna dwadzieścia lat każdego roku uśrednione wydatki na transformację energetyczną państwa sięgną 3,5 proc. PKB państwa polskiego. Oznacza to roczne inwestycje w wielkości co najmniej 80 mld zł. Dla porównania w 2020 r. wydatki budżetowe to prawie 505 mld zł. Przytoczone dane wskazują, jak olbrzymi będzie wysiłek inwestycyjny państwa i społeczeństwa polskiego wywołany polityką Europejskiego Zielonego Ładu. Prezes Narodowego Banku

Polskiego Adam Glapiński wprost podkreśla, iż wysokie ceny prądu wywołane nakładaniem na nasze źródła energii ogromnych danin, mogą zdusić wzrost gospodarczy państwa polskiego. Dlatego władza państwowa i przedsiębiorcy muszą ten problem potraktować niezwykle poważnie. Pytany, czy nie można było się temu przeciwstawić, odpowiada, że gdyby Polska była tak silna gospodarczo jak Niemcy, nigdy taka polityka nie zostałaby wprowadzona w życie (Tygodnik „Sieci", 15.03.2021). Zobowiązania obligują nas do przeprowadzenia transformacji energetycznej. Wskazany wcześniej dylemat, jak zachować wysokie tempo rozwojowe, przy realizacji niezwykle kosztownej przebudowy energetyki, postanowiono rozwiązać aktywną polityką przemysłową. W skrócie nowe, wyśrubowane cele transformacji energetycznej potraktowano jako swego rodzaju dźwignię do głębokiej i wielowymiarowej modernizacji przemysłowej państwa, która ma zasadzać się na przechwytywaniu i rozwijaniu w krajowych przedsiębiorstwach jak największej liczby łańcuchów wartości nowo tworzonych gałęzi przemysłowych.

Priorytety transformacji energetycznej

Polityka Energetyczna Polski do 2040 r. oparta jest na trzech filarach. Pierwszym jest sprawiedliwa transformacja, drugim – zeroemisyjny system energetyczny, a trzecim – dobrej jakości powietrze. W każdym z nich znajdują się łańcuchy technologiczne, które mają być rozwijane przez krajowy przemysł. Pierwszy filar – sprawiedliwa transformacja – jest traktowany dwutorowo: jako polityka przemysłowa oraz swego rodzaju instrument negocjacyjny w relacjach z Unią Europejską. Skoro zależność od węgla brunatnego i kamiennego polskiej elektroenergetyki jest znacznie wyższa niż w pozostałych państwach członkowskich UE, to postulat sprawiedliwej transformacji ma zapewnić uwzględnienie gorszego punktu startowego Polski wynikającego z szerszego niż w pozostałych państwach wykorzystania węgla. To także przeciwdziałanie nierównomiernemu rozkładowi kosztów, bardziej obciążającego polską gospodarkę. Ma to pozwolić negocjować odstępstwa, wolniejsze wprowadzanie Europejskiego Zielone-

go Ładu lub zapewnić większe środki pomocowe na transformację czy też realizację obydwu wskazanych celów. Postulat sprawiedliwej transformacji zawiera także polityki przemysłowe – projektuje rozwój nowych gałęzi przemysłu związanych m.in. z energetyką jądrową oraz odnawialnymi źródłami energii. Wsparcie dla transformacji rejonów węglowych sięgnie gigantycznej kwoty 60 mld zł, z której gros będzie przeznaczone na rozwój nowych gałęzi przemysłowych. Polityka energetyczna szacuje, iż transformacja będzie opierała się na krajowych przewagach konkurencyjnych w takich branżach jak elektromobilność, infrastruktura sieciowa, cyfryzacja, termomodernizacja budynków, odnawialne źródła energii, energetyka atomowa i umożliwi stworzenie nawet 300 tysięcy nowych miejsc pracy w branżach o wysokim potencjale.

Atom to podstawa

Drugi cel polityki energetycznej państwa to wybudowanie zeroemisyjnego systemu energetycznego. Jego rdzeniem będą energetyka jądrowa oraz energetyka gazowa, niezbędna do stabilizacji odnawialnych źródeł energii, wtedy gdy wiatr przestaje wiać, a słońce świecić. Plany zakładają wybudowanie do 2043 roku sześciu bloków jądrowych o mocy całkowitej 6-9 GW. Budowa pierwszego bloku jądrowego ma rozpocząć się nie później niż w 2026 roku. Choć polski przemysł nie ma kompetencji w budowie całego łańcucha technologicznego elektrowni nuklearnych, to jednak szacuje się, iż do 70 proc. wartości całego projektu mogą je zrealizować polskie przedsiębiorstwa wspólnie z krajowymi ośrodkami naukowo-badawczymi. Szacunki wskazują, że ponad 60 polskich przedsiębiorstw ma doświadczenie w energetyce jądrowej, zaś prawie 300 kolejnych posiada kompetencje z branż pokrewnych, które przy określonych działaniach dostosowawczych można wykorzystać w przemyśle jądrowym. Dokument szacuje, że do 2040 r. energetyka jądrowa utworzy ok. 25-38 tys. nowych miejsc pracy bezpośrednio przy realizacji programu. Państwo polskie planuje, że energetyka jądrowa będzie rozwijać się w przemyślany sposób. Wybrana firma ma objąć 49 proc.

udziałów we wspólnym ze stroną polską przedsiębiorstwie budującym i zarządzającym krajowymi elektrowniami nuklearnymi. Obie strony podzielą się proporcjonalnie do udziałów zarówno kosztami, jak i przyszłymi zyskami. W ten sposób dostawca technologii zostanie partnerem biznesowym na długie lata. W naturalny sposób taka struktura udziałów wywołuje efekt polityczny. Zbliża na dziesiątki lat gospodarczo i politycznie dwóch partnerów realizujących projekt budowy elektrowni atomowych w Polsce. Obecnie strona polska zawarła najbliższe relacje we wzmiankowanej kwestii ze Stanami Zjednoczonymi, poważne oferty przedstawiają zarówno francuski koncern Électricité de France (EDF), jak i koreański podmiot Korea Hydro and Nuclear Power (KHNP). Harmonogram przyjętych prac zakłada, że z dużą dozą prawdopodobieństwa już w przyszłym roku powinien zostać wybrany zagraniczny partner dla polskiego programu energetyki jądrowej. Warto podkreślić, że w *de facto* od nowa projektowanym i budowanym systemie, energetyka jądrowa będzie odgrywała kluczową rolę, dostarczając prąd w tzw. podstawie systemu (czyli nieprzerwanie). Jej rola w zapewnieniu bezpieczeństwa energetycznego będzie zbliżona do tej, jaką obecnie odgrywa energetyka węglowa (zarówno węgla brunatnego, jak i kamiennego).

Gaz to stabilizator

Drugim filarem będzie energetyka gazowa, której rola wraz z rozwojem odnawialnych źródeł energii będzie znacząco rosła. Z tego powodu w ciągu najbliższych trzydziestu lat znacząco zwiększy się zapotrzebowanie na gaz ziemny. Jak wielki będzie to wzrost, ilustruje przygotowana przez Komisję Europejską prognoza wskazująca, iż obecna konsumpcja gazu ziemnego w naszym kraju to zaledwie 56 proc. prognozowanego zużycia gazu w 2050 r. Z czasem będzie ulegać zmianie zawartość koszyka paliwa gazowego przez domieszki gazów syntetycznych (przede wszystkim wodoru). Za dwadzieścia lat energetyka gazowa dostarczy ponad 18 proc. wyprodukowanej energii, podczas gdy energetyka jądrowa niewiele mniej – 16,5 proc. Choć statystycznie planowana produkcja energii z gazu zbliżona jest

do prognozy dla energetyki nuklearnej, to jednak jej rola w systemie będzie zupełnie inna. O ile prąd z elektrowni atomowych będzie stanowił podstawę systemu, o tyle prąd z gazu będzie stabilizował system i przeciwdziałał nieplanowanym wyłączeniom (*blackout*), gdy odnawialne źródła energii będą gwałtownie zmniejszać produkcję. System elektroenergetyczny musi być przygotowany na kompensowanie spadków dostaw energii w amplitudach dobowych. Z tej przyczyny energetyka gazowa jest kluczowym instrumentem dla zastępowania niestabilnych źródeł odnawialnych w pikach, które będą się pojawiać zaledwie co kilka, kilkanaście godzin.

OZE to zmienność

Kolejnym filarem będą odnawialne źródła energii, które na przestrzeni najbliższych dwudziestu lat będą rozwijane bardzo dynamicznie. W 2040 r. morskie i lądowe farmy wiatrowe oraz energetyka fotowoltaiczna wyprodukują ponad 40 proc. krajowej energii elektrycznej (prawie 79 TWh). Dla porównania w 2020 r. OZE dostarczyły ok. 11 proc. energii (trochę ponad 16 TWh). Priorytetem będzie rozwój morskiej energetyki wiatrowej, która nie dość że jest najbardziej produktywna (wiatr na morzu wieje ciągle, w odróżnieniu od lądu), to jeszcze z racji wielkiej skali inwestycji da szansę na rozwój wielu tradycyjnym i nowym gałęziom krajowego przemysłu (stocznie, huty, stalownie, przemysł elektrotechniczny, chemiczny, lakierniczy i farbiarski itd.). Dlaczego tak się stanie? Wystarczy spojrzeć na dane techniczne. Pojedyncza morska turbina wiatrowa o mocy 5 MW jest posadowiona na prawie 80-metrowym stalowym maszcie wbitym w dno morskie. Turbinę napędza śmigło wyposażone w trzy łopaty (każde o długości 62 metrów, takie jak dwudziestopiętrowy blok mieszkalny). Całość o wadze ok. 1700 ton, wraz z obracającym się śmigłem, od podstawy do szczytu będzie wysoka na 185 metrów, czyli prawie tyle co warszawski Pałac Kultury do linii dachu (bez iglicy). Z prostego obliczenia wynika, że dla jednej farmy wiatrowej o mocy 1000 MW potrzeba aż 200 turbin posadowionych na ogromnych masztach – wszystko będzie ważyć co najmniej 370 tys. ton. Jeśli chcemy sprawdzić, jak

duża będzie skala morskich farm wiatrowych na polskim wybrzeżu, to wskazane wyżej 370 tys. ton i 200 turbin na wielkich masztach należy pomnożyć przez dziewięć (ponieważ zgodnie z planami w 2040 r. morskie farmy wiatrowe na polskim wybrzeżu będą miały moc powyżej 9 tys. MW, sześć razy więcej niż moc opalanej węglem brunatnym elektrowni w Turowie u zbiegu polsko-niemiecko-czeskiej granicy).

Wodór to przyszłość

Transformacja energetyczna to także produkcja nowych syntetycznych paliw. Ważną rolę ma ogrywać wodór, wytwarzany z energii elektrycznej uzyskanej z odnawialnych źródeł energii, w przebudowie sektora gazowego, zapewniając zmniejszenie redukcji emisji CO_2. W tym celu infrastruktura przemysłu gazowego będzie zasilana bezemisyjnym wodorem, mieszanym w coraz większych proporcjach z gazem ziemnym – rządowa polityka energetyczna postuluje, aby w 2030 r. sieci umożliwiały transport gazu ziemnego z domieszką 10 proc. gazów zdekarbonizowanych (przede wszystkim wodoru). Wodór, oprócz kluczowej roli mieszanki dla gazu ziemnego, ma znaleźć szerokie zastosowanie jako czyste paliwo dla ciężkiego transportu kołowego, dla flot pojazdów miejskich (już w 2025 r. flota autobusów wodorowych sięgnie 500 pojazdów, pięć lat później zwiększy się do 2000 sztuk), dla transportu kolejowego, morskiego, a nawet lotniczego. Jednak większość wodorowych technologii transportowych jest dopiero rozwijana i dlatego planuje się szersze zastosowanie nowego paliwa dopiero pod koniec lat 30. XXI wieku. Wydaje się, że rola wodoru będzie w nieodległej przyszłości rosła, skoro polityka energetyczna wskazuje, iż to paliwo przyczyni się do obniżenia importu paliw i zmniejszania zależności od dostaw z zagranicy, zastępując importowaną ropę naftową i paliwa ropopochodne. Widać wyraźnie, iż wyzwania energetyczne traktowane są jako szansa na rozwinięcie nowych sektorów gospodarczych, m.in. produkcji autobusów i pociągów, ogniw wodorowych, jednostek pływających oraz elektrolizerów – najdroższych urządzeń do produkcji wodoru z energii elektrycznej.

Zagrożenia ze Wschodu

Kluczowe zagrożenia dla bezpieczeństwa energetycznego Polski z kierunku wschodniego wiążą się z używaniem surowców energetycznych jako instrumentu dla realizacji strategicznych celów politycznych państwa rosyjskiego. Z tej perspektywy prowadzona przez nasze państwo dywersyfikacja dostaw i rezygnacja z długoterminowych kontraktów na rosyjski gaz skutecznie ogranicza zależność. Polska realizuje szereg projektów infrastrukturalnych zapewniających dostawy gazu od nowych dostawców (m.in. ze Stanów Zjednoczonych, Kataru, Norwegii) w miejsce surowca z Rosji. Temu celowi służy m.in. rozbudowa możliwości odbiorczych terminala LNG w Świnoujściu (do 8,3 mld m^3 gazu rocznie z początkowych 5 mld m^3), budowa podmorskiego gazociągu Baltic Pipe (umożliwiającego przesłanie od jesieni 2022 r. po dnie Morza Bałtyckiego do Polski 10 mld m^3 gazu ziemnego wydobywanego na Szelfie Norweskim) oraz decyzja o postawieniu do 2028 r. kolejnego morskiego terminala LNG w Gdańsku jako jednostki pływającej (Floating Storage and Regasification Unit-FSRU). Zdolność odbiorcza nowego terminala jest szacowana w widełkach 4,5-8 mld m^3 gazu rocznie. Wszystkie wymienione działania, powiązane z rozbudową oraz budową nowych połączeń gazowych z Litwą, Słowacją, Czechami i Niemcami, poprawią bezpieczeństwo regionu, a Polska ma szansę stać się eksporterem w regionie gazu od innych niż Rosja producentów do państw Europy Środkowej. Prowadzone są także działania mające na celu zmniejszenie zależności od dostaw ropy naftowej z kierunku wschodniego. Zawierane na przestrzeni ostatnich lat kontrakty redukują import ropy z Rosji, wprowadzając w to miejsce dostawy z innych kierunków.

Eliminacja zależności od Rosji i modernizacja gospodarki

Dla bezpieczeństwa Polski rysują się dwa kluczowe wyzwania związane z zachodzącymi zmianami w energetyce. Trudniejsze jest wywołane transformacją energetyczną oraz polityką ochrony klimatu

Unii Europejskiej. Wymusza przekierowanie przez państwo polskie dużych środków finansowych na przebudowę sektora energetycznego, znacząco ograniczając zdolności inwestycyjne w innych sektorach gospodarczych i społecznych. Plan przeciwdziałania trwałemu spowolnieniu gospodarczemu (w bezpośrednim skutku bardzo kosztownych inwestycji w energetykę) oparty jest na aktywnej polityce przemysłowej oraz przechwytywaniu i rozwijaniu w kraju nowych technologii tych części łańcuchów produkcyjnych, które mają największą wartość. W tym ujęciu polityka transformacji energetycznej została potraktowana jako szansa na znaczące przyspieszenie tempa wzrostu gospodarczego państwa. Fundusze wspólnotowe, krajowe oraz środki zebrane od konsumentów mają w jak największym stopniu zasilać rozwój nowych sektorów gospodarczych i branż przemysłowych w kraju, w jak najmniejszym – finansować import produktów gotowych. Drugie wyzwanie, jakim jest neutralizacja oddziaływania Rosji na politykę państwa polskiego za pośrednictwem surowców energetycznych, jest bliska sukcesu. Szereg oddanych już do użytku inwestycji, realizowanych obecnie oraz zaplanowanych do wdrożenia w najbliższych latach, uniezależni Polskę od rosyjskiego szantażu groźbą odcięcia dostaw gazu lub ropy naftowej. W średnim horyzoncie czasowym ta polityka powinna skutkować przejęciem przez Polskę roli dostawcy energii umożliwiającym działania wolnego rynku i konkurencji w energetyce.

Bezpieczeństwo logistyki i nowa geografia bogactwa

Przemysław Sypniewski

19 września 1775 r. I Rzeczpospolita zawarła traktat handlowy z Królestwem Pruskim. Był on właściwe pruskim dyktatem, który nałożył śluzy celne na wszystkie ciągi logistyczne I Rzeczpospolitej, za pomocą których prowadziła ona handel. Prusom chodziło wówczas o osiągnięcie trzech celów: zdławienie polskiego handlu, uderzenie w interesy ekonomiczne Gdańska (po pierwszym rozbiorze Polski nie został on wcielony do Prus) i przekierowanie ciągów logistycznych do portów pruskich, głównie Elbląga. Traktat z 1775 r. przewidywał nałożenie asymetrycznych ceł na eksport. Z Polski były one drastycznie wysokie, z Prus do Rzeczpospolitej skrajnie niskie. Dodatkowo opodatkowany był tranzyt polskich towarów przez pruskie terytorium. Zapisy traktatu przewidywały również zakaz polskiego eksportu na Śląsk oraz produktów rolnych do Brandenburgii. Monarchia pruska z pełną konsekwencją wykorzystała nie tylko siłę swojego państwa, ale również geograficzną możliwość nałożenia na szlaki handlowe I Rzeczpospolitej śluz logistycznych. Ówczesna polska gospodarka została całkowicie wydrenowana finansowo. Traktat doprowadził również do tego, że nowo powstałe ciągi logistyczne rozbijały spójność Rzeczpospolitej, a cementowały państwo pruskie.

W 2007 r. udział całej Unii Europejskiej w światowym PKB wynosił 25 proc., w 2020 spadł do 18 proc. W 2007 r. 81 proc. światowych inwestycji dokonywano na Zachodzie lub Zachód inwestował na Wschodzie, a tylko 17 proc. pochodziło ze Wschodu. W 2019 r. ten podział wyglądał już tak: Zachód – 32 proc., Wschód – 66 proc. Punkt ciężkości świata przesunął się z rejonu Atlantyku w region Azji i Pacy-

fiku. Tendencja ta przyspieszyła po wybuchu epidemii COVID-19. Nie należy jednak zapominać, że Wschód to nie tylko Chiny. To również Japonia, Korea, Indonezja, Malezja czy Tajlandia. Nowe szlaki handlowe powstają w Azerbejdżanie, Kazachstanie, Kirgistanie, Uzbekistanie i Turcji. Tam tworzą się nowe potężne centra logistyczne. Procesy te przebiegały od kilkudziesięciu lat, ale jak wszystko w historii przez długi czas nie były zauważalne. Przełomem była wizyta prezydenta Chin Xi Jinpinga w Kazachstanie we wrześniu 2013 r. Wówczas ogłosił on wielki chiński projekt na XXI wiek. Chodzi o strategię Jeden Pas, Jedna Droga, czyli Nowy Jedwabny Szlak. Od tamtej pory jest ona realizowana konsekwentnie i już przebudowała cały system wymiany towarowej.

Chińczycy uważają, że świat to nie tylko wschód, zachód, północ, południe. Jest również piąta strona świata, a jest nią środek, czyli państwo chińskie. Dlatego Chiny chcą być centrum, z którego mają wychodzić i do którego mają przychodzić wszystkie współczesne ciągi logistyczne. Ważnym punktem końcowym tego szlaku jest Europa. Polska ze względu na swoje położenie geograficzne jest istotnym miejscem przepływów strategicznych. Najważniejszym „portem" końcowym Jedwabnego Szlaku jest Centrum Logistyczne w Duisburgu, najważniejszą bramą do Europy jest polska wschodnia granica, a najważniejszym dziś do niej kluczem jest terminal w Małaszewiczach. W ostatnich latach mamy do czynienia ze zmianą szlaków handlowych. Mając bramę i klucz, Polska powinna wykorzystać każde „prawo sprzyjających okoliczności", aby nie tylko mieć kontrolę i czerpać zyski z przepływu towarów, ale mieć zdolność „zwrotnicy", która może zmienić kierunki i otworzyć nowe szlaki gospodarcze.

Dziś nowoczesna gospodarka działa dzięki logistyce. Logistyka to obszar działalności firmy odnoszący się do przepływu produktów oraz powiązanych z nimi pieniędzy i informacji od ich źródła pochodzenia poprzez wszystkie firmy i instytucje pośrednie (producentów, firmy transportowe, magazynowe, ubezpieczycieli, banki itp.) aż do ostatecznego klienta. Dobra i nowoczesna logistyka zapewnia dostarczenie do adresata, magazynowanie na szlaku lub czasowe przechowanie, przygotowanie do użycia oraz pozbycie się elemen-

tów pozostałych po konsumpcji dostarczonego towaru lub produktu. Podstawowym pojęciem w logistyce jest łańcuch. Jest to zespół następujących po sobie miejsc przeładunkowych (port, magazyn, lotnisko) i środków transportu (statki, samoloty, pociągi, samochody), przez które przepływają produkty, informacje i pieniądze. Podobnym pojęciem jest sieć logistyczna. Określiłbym ją jako zbiór firm współpracujących w zarządzaniu danym łańcuchem. Do sieci należą właściciele miejsc przeładunkowych, właściciele środków transportu, producenci i klienci. W dzisiejszym świecie należą również do niej te firmy, które nie stanowią bezpośrednio łańcucha logistycznego, ale budują system zamówień lub rozwiązania informatyczne. Logistyka stwarza miejsca pracy, przyciąga zakłady produkcyjne, sprzyja industrializacji i buduje nową geografię bogactwa.

Transport zapewnia przemieszczanie towarów od przedsiębiorcy do ostatecznego klienta. W ten sposób wpływa na rozwój nie tylko firmy, ale również całej gospodarki. Jednak, aby przemieszczenie towarów było maksymalnie efektywne, potrzebne są również spedycja oraz magazynowanie. To dzięki spedycji firmy nieposiadające własnych środków transportu mogą przemieszczać towary do odbiorców. Przedsiębiorcy zajmujący się produkcją, a nieposiadający magazynów, mogą korzystać z takich usług. W ten sposób ograniczają swoje koszty i więcej środków mogą inwestować w rozwój. Transport, spedycja i magazynowanie to procesy skomplikowane i czasochłonne. Dziś ulegają one znacznemu uproszczeniu dzięki nowoczesnym technologiom.

Dobrze zaprojektowana logistyka przyspiesza rozwój kraju, zwiększa efektywność inwestycji infrastrukturalnych i buduje konkurencyjność gospodarki. Możemy obserwować dwa równolegle zachodzące modele. Pierwszym jest model, w którym różnego rodzaju koncerny integrują procesy produkcyjne w jednolity łańcuch towarowy z udziałem dziesiątków podmiotów, przy czym integracja nie wynika z kapitałowej zależności, lecz z chęci realizacji w sposób bardziej konkurencyjny wspólnego przedsięwzięcia. Ten sposób tworzenia biznesu staje się też strategią obronną przed drugim modelem. Ten z kolei jest odwrotny, to model przejmowania wszystkich ogniw zwią-

zanych z potrzebami konsumenckimi w handlu, przy jednoczesnym stopniowym przejmowaniu całego łańcucha dostaw logistycznych. Skutkuje to kontrolą nad całym procesem gospodarczym obejmującym produkcję towarów, magazynowanie, dostarczanie do klientów aż do pełnego zaspokojenia potrzeb konsumenckich, nie wykluczając nawet tych, które są inspirowane i tworzone.

Rozwój modelu drugiego stanowi zagrożenie dla obecnie funkcjonującego modelu gospodarczego. Staje się on bardzo konkurencyjny dla funkcjonujących sieci handlowych, przejmuje produkcję skupioną dotychczas w innych przedsiębiorstwach oraz ma zdolność do narzucania nowych reguł gospodarczych. Wielkim sojusznikiem tego modelu działania są zmiany technologiczne i powstające dzięki nim logistyczne łańcuchy dostaw nowej generacji. Zbieranie informacji, ich przekaz, sprzedaż, analiza i dedukcja dzięki sztucznej inteligencji. Kable podmorskie, sieci światłowodowe, połączone z nimi szlaki komunikacyjne, technologie 5G i 6G. Komunikacja w przestrzeni kosmicznej, nowe systemy mikrosatelitarne, kanały na YouTube, portale społecznościowe, telewizyjne platformy serialowe – wszystko to tworzy nowe szlaki logistyczne, o których opanowanie toczy się walka pomiędzy państwami, globalnymi firmami, starą gospodarką a nową. Wszystko, co można scyfryzować, zostanie w tym świecie nowej rywalizacji scyfryzowane. Przemiany są już tak rozległe, że trudno przewidzieć przyszłość. Rozbudowa sieci, wydajność komputerów, dostępność informacji, satelitarna nawigacja, duże zbiory danych, samouczące się systemy, autonomiczne pojazdy. To, co jeszcze dwadzieścia lat temu wydawało się fantastyką, dziś jest rzeczywistością.

Zadaniem dla firm logistycznych jest sprawne i konsekwentne wprowadzenie koniecznych zmian. Bez tego znikną z rynku, tracąc możliwość konkurencji. Na razie w dziedzinie cyfryzacji przemysł wyprzedza logistykę. Oczekuje on od logistyków tworzenia takich łańcuchów dostaw, które zapewnią ich widoczność w czasie rzeczywistym. Dobrym przykładem nowych modeli biznesowych jest rozwój technologii druku 3D. Dla firm logistycznych to nowe możliwości rynkowe w zakresie zaopatrzenia w części zapasowe. W połączeniu z kopalnią danych, jaką jest na przykład ciężarówka albo pociąg

(zbierające w czasie rzeczywistym wszelkiego rodzaju informacje w terenie, przez który przejeżdża), daje możliwość realizacji zadań związanych z dostarczaniem potrzebnych produktów w czasie rzeczywistym. Gdy firma logistyczna będzie dysponować danymi z całkowicie scyfryzowanej floty (nie tylko swoich pojazdów, lecz także od współpracujących podwykonawców i przewoźników czarterowych), będzie mogła nie tylko wyeliminować zbędne koszty i poprawić swoją konkurencyjność, ale również proponować określone towary dedykowane miejscom i klientom. Będzie również mogła handlować tymi danymi na olbrzymią skalę. Z technicznego punktu widzenia dzisiaj jest możliwe prawie wszystko. Zarządzanie oknami czasowymi ze sterowaniem pojazdem w czasie rzeczywistym, zarządzanie procesami logistycznymi na terenie zakładu zdalnie, zautomatyzowane zawieranie umów itp. W ten sposób powstaje łańcuch dostaw 4.0. Pojęcie to odnosi się do zastosowania nowoczesnych technologii cyfrowych w tradycyjnych łańcuchach dostaw. Cyfryzacja umożliwia integrację przepływu ładunków i danych szybko, niezawodnie i elastyczniej. Dzięki tej technologii jest też możliwe sprawniejsze zarządzanie nie tylko stanem magazynowania, ale całą siecią magazynów, które już dziś wypierają dotychczasowy model handlu oparty na sieciach handlowych. Nowy trend w logistyce to korzystanie z takich technologii jak blockchain, cyfryzacja operacji, automatyzacja magazynów, Big Data, samouczenie maszyn i przemysłowy Internet rzeczy. Logistyczny łańcuch 4.0 umożliwia dostarczenie zamówionego towaru maksymalnie w 24 godziny i praktycznie eliminuje zwroty. Łańcuch dostaw 4.0 korzysta z osiągnięć sztucznej inteligencji, aby przewidzieć przyszłe scenariusze. Umożliwia lokalizowanie obszarów o niższej wydajności pracy, obszarów, gdzie wzrasta lub spada konsumpcja. Wprowadzanie łańcucha logistycznego 4.0 wiąże się z wysokimi kosztami. Wymaga też skoordynowanych i szybkich działań ze strony wszystkich podmiotów będących jego ogniwami. W ten sposób automatyzacja i cyfryzacja całego procesu logistycznego uwzględniająca magazynowanie stają się we współczesnym świecie fundamentem przemysłu i ponownej industrializacji, ale tym razem opartej na automatach.

Jednocześnie wśród klientów rozpowszechniane są nowe trendy konsumpcyjne. Obserwując rzeczywistość gospodarczą, można zauważyć, że trendy te bywają już skutecznie inspirowane i wzmacniane przez dostawców. Klienci chcą kupować i ewentualnie zwracać produkty różnymi kanałami handlowymi, oczekując realizacji usług maksymalnie w ciągu 24 godzin. Cyfryzacja jest jedną z dwóch kluczowych osi dostaw 4.0. Druga to automatyzacja. Potrzeby rynku logistycznego kreują w tej dziedzinie nowy przemysł. Proponowane w tej dziedzinie rozwiązania muszą być bowiem bardzo zróżnicowane i odpowiadać konkretnym potrzebom każdej firmy. To powoduje duże potrzeby kapitałowe i w związku z tym sprzyja dużym podmiotom logistycznym prowadzącym ekspansję globalnie i mającym własne ośrodki badawcze. Warto wiedzieć, że w Europie na badania najwięcej przeznacza największa firma logistyczna świata, jaką jest DHL. Łańcuch dostaw 4.0 powstał na skutek upowszechniania się przemysłu 4.0. Koncepcja ta, wywodząca się z niemieckiego sektora przemysłowego, powstała w odpowiedzi na wprowadzanie nowych technologii cyfrowych pozwalających zautomatyzować procesy produkcyjne i ograniczyć liczbę błędów mogących pojawiać się w całym procesie. Każda firma, która chciałaby tworzyć łańcuch dostaw, powinna stopniowo wprowadzać cyfrowe technologie i sztuczną inteligencję.

Zjawiska zachodzące w tym obszarze gospodarczym zmieniają proces. Tak naprawdę gospodarka i przemysł XXI wieku zasadniczo różnić się będą od tego, co dotychczas znamy. Już widzimy, że największymi podmiotami o globalnym zasięgu stają się przede wszystkim firmy, które opanowują cały łańcuch logistyczny – od produkcji (a nawet od kreacji potrzeb) do dostawy. Wpływa to nie tylko na gospodarkę, ale na całe państwo i społeczeństwo. Wpływ ten ma charakter dwojaki. Bezpośrednio dążąc do swoich celów biznesowych, jak i pośrednio poprzez efekt skali. Rodzi to niebezpieczeństwo powstawania dużych międzynarodowych „śluz" na państwowych ciągach infrastrukturalnych. Może to skutkować utratą nie tylko całych gospodarek, ale również wpływem na model rynku pracy, system podatkowy i wykorzystywanie funduszy publicznych. Bezpieczeństwo

własnej logistyki staje się kluczowe dla państwa. Jest on zjawiskiem dynamicznym, zmieniającym się w czasie, przestrzeni i wymiarze. Dziś w Polsce rozumiemy już, co to znaczy bezpieczeństwo w energetyce, sektorze bankowym czy infrastrukturze gazowej. Najwyższy czas zdać sobie sprawę z wagi bezpieczeństwa w logistyce. Musimy mieć zdolność zapewnienia potrzebnych dla rozwoju kraju przepływów towaru z możliwością ich zatrzymania.

Optymizm nie zastąpi nam firm logistycznych

Polska leży nie tylko w centrum Europy, leży również na przecięciu głównych szlaków logistycznych zmieniającego się i wędrującego świata. Niezależnie, czy stanowić będzie część Nowego Jedwabnego Szlaku, czy część Projektu Trójmorza, stanowi centrum logistyki na końcach łańcuchów dostaw. Dobrze, że obok wcześniejszych inwestycji na osi wschód – zachód, inwestycje infrastrukturalne powstające w ostatnich latach uwzględniają oś północ – południe. Obecnie realizujemy wielkie, wręcz przełomowe inwestycje logistyczne i dziesiątki mniejszych. Wszystkie – drogi kołowe, kolejowe, szlaki wodne, Centralny Port Komunikacyjny, przekop Mierzei Wiślanej, autostrady – złożą się w jednolity zintegrowany system logistyczny. Inwestycje te są kapitałochłonne i charakteryzują się długą stopą zwrotu. W polskich warunkach nie można sobie wyobrazić, że mogłyby być realizowane bez udziału państwa. Całe społeczeństwo ponosi ich koszt i to społeczeństwo powinno być ich beneficjentem. Dziś jednak istnieje zagrożenie, że te kosztowne budowle będą głównie wykorzystywane przez międzynarodowe koncerny, które mogą nam założyć podobny rodzaj „śluz gospodarczych" jak te w XVIII w. założone przez Fryderyka II. Może wystąpić nacjonalizacja kosztów, a prywatyzacja zysków. Polskie państwo powinno wspierać rozwój polskich firm logistycznych (dziś także poprzez zapisy ustawowe wspierające polskie przedsiębiorstwa transportowe, które dominują rynek samochodowy w Europie), jutro poprzez budowę od początku, jeśli taka będzie potrzeba własnych firm logistycznych. Bez sprawnej logistyki nie powiedzie się żaden program reindustrializacji Polski. Bez udziału

polskich przedsiębiorstw w międzynarodowych łańcuchach dostaw nie uda się zwiększyć eksportu ani rozwijać technologii. Nie jest przypadkiem, że dwie firmy, które w ostatnich latach odniosły największe sukcesy giełdowe w Polsce, związane są z branżą logistyczną. In Post i Allegro, podmioty, które mają największą wycenę giełdową, powstały jako polskie pomysły i polskie firmy, ale dziś już są w rękach międzynarodowych. Należy więc stworzyć Projekt Rozwoju Logistyki. Ma on zawierać koncepcję, jak i gdzie wydawać pieniądze na państwową infrastrukturę logistyczną i określić sposoby wspierania polskich przedsiębiorców. Należy stworzyć program, który – opisując całość koncepcji logistycznej Polski i powiązanie z systemem społeczno-gospodarczym – określi też sposoby zapewnienia bezpieczeństwa. Taka strategia jest niezbędna dla zapewnienia trzech podstawowych funkcji logistyki: integracji kraju, obsługi wszystkich procesów społecznych i gospodarczych oraz sprawności mobilizacyjnych zasobów również w kontekście militarnym.

Polska jako centrum logistyki, z własnymi portami, firmami spedycyjnymi, portami multimodalnymi wewnątrz kraju i na granicach, ze szlakami wschód – zachód, północ – południe, z możliwościami szybkiego przekierowywania strumieni przepływu towarów i informacji, będzie silnym i pożądanym partnerem w geopolitycznej rozgrywce. Życie (także to gospodarcze) zawsze znajdzie sposób.

W historii wojna trwa

dr Piotr Gontarczyk

Historia zawsze była istotna w przestrzeni publicznej, a jej znaczenie wykraczało poza wyłącznie sferę opisu minionych faktów. W starożytnym Egipcie byli władcy, którzy nakazywali usuwać ślady niektórych swoich poprzedników, insygnia ich władzy oraz wyznawane przez nich systemy wierzeń. Aleksander Macedoński w 334 r. p.n.e. oficjalnie wybrał się na wielką wyprawę przeciwko Persji, żeby uwolnić Greków Anatolijskich, pomścić ich krzywdy, a także zrewanżować się za najazdy Persów z poprzednich stuleci. Kto dzisiaj pamięta, że wielu owych Greków „wyzwalanych" w Anatolii, którzy byli lojalni wobec władców Persji, masowo mordował lub zsyłał do kopalni jako niewolników?

Jedni chcieli do historii przejść choćby i barbarzyńskimi czynami, jak Herostrates z Efezu, który spalił Artemizjon, inni chcieli go za to wymazać z przeszłości, a udało mu się w niej przetrwać dzięki bodaj jednej nieopatrznej wzmiance w kronice. Inni, dzięki swoim pomysłom, jak król Karii Mauzolos sprzed 2,5 tys. lat, pozostali do dziś obecni w naszej kulturze, przestrzeni, symbolice. Inni, jak Juliusz Cezar po kampanii w Galii, pisali źródła, sami doskonale wiedząc, jaka będzie waga ich memuarów w historii, a wcześniej w polityce.

Wojna o polityczne rozumienie współczesności często oparta na wątkach religijnych, historycznych toczyła się od zawsze: w budowaniu pomników, w niszczeniu prawdziwych i wytwarzaniu fałszywych dokumentów, w każdym rodzaju piśmiennictwa i używanej w nich nawet tytulaturze, w inskrypcjach zamieszczanych na wznoszonych budowlach, w budowaniu genealogii najpierw rodowej, a potem politycznej, heraldyce, na monetach i na igrzyskach. Polityka

i historia są tak nierozerwalne, że doprawdy naiwnością byłoby uważanie, że historia może być apolityczna. Naturalnie, niezwykle ważne i cenne jest akademickie oderwanie się od politycznych potrzeb i rzetelna rekonstrukcja skomplikowanych niekiedy i wielowątkowych zjawisk i wydarzeń. Złudna jednak wydaje się nadzieja – zwłaszcza w dzisiejszych czasach – że historia nagle po wszystkich doświadczeniach ludzkiej cywilizacji zostanie pozostawiona wyłącznie jako obszar odtwarzania przeszłości. Przeciwnie: historia zawsze tłumaczyła współczesny świat i jako taka była obszarem poszukiwania legitymacji władzy, uzasadnienia systemu politycznego i społecznego, uprzywilejowanej pozycji osób, grup społecznych i narodów. Co tu jest prawdą, co fikcją, co argumentem prawdziwym, a co zwykłą blagą, nie zawsze jest łatwe do rozstrzygnięcia, a nawet jego wyjątkowa merytorycznie jakość nie zawsze miała i często nie ma dla wagi używania owych argumentów historycznych większego znaczenia. Ważniejsze, że zawsze używano ich do atakowania państw, religii czy wręcz cywilizacji zarówno na potrzeby wewnętrzne, jak i polityki międzynarodowej czasem z bardzo daleko idącymi konsekwencjami. Mowy Marka Porcjusza Katona na temat Kartaginy (sam kiedyś żołnierz w wojnie z tym państwem) odwoływały się do argumentów politycznych, ale także do historii. Mimo oporu wielu Rzymian ostatecznie doprowadziły do zniszczenia Kartaginy. Swoją rolę odegrało także niefortunne posługiwanie się przez niefortunnie wybranych na tron Polski królów z dynastii Wazów tytułem „królów Szwecji". Formalno-prawna i historyczna uzurpacja, która przyczyniła się do popchnięcia Rzeczypospolitej na skraj historycznej przepaści.

Polska i Niemcy

Taka wycieczka w przeszłość (*historia magistra vitae est*) wskazuje na czynniki od zawsze pokazujące nieusuwalną symbiotyczność związku historii i polityki. Dobrze widać to na przykładzie Polski włącznie z faktem, że tradycyjnie jest ona polem (historycznej) bitwy mocarstw, takich jak Niemcy, które w przeszłości robiły bardzo wiele, by unikać odpowiedzialności za zbrodnie z czasów II wojny świa-

towej. Rzekome niemieckie rozliczenie przeszłości to historyczna mistyfikacja. Konstytucja, na bazie której ufundowano RFN, wykluczyła możliwość wydania w ręce innych państw zbrodniarzy hitlerowskich. Ci podlegali w późniejszym okresie ochronie prawnej także przed niemieckimi sądami. Sami swoi: ci hitlerowcy, którzy te prawa tworzyli, i ci hitlerowcy, którzy mogliby im podlegać. W większości zapadające wyroki w sprawach zbrodni hitlerowskich na Żydach i Polakach były uniewinniające. Liczni mordercy, zbrodniarze, funkcyjni machiny Holocaustu i organizacji systemu mordowania ocalałych żydowskich uciekinierów pozostawali bezkarni. Za typowy można tu wskazać przykład wicestarosty powiatu miechowskiego Friedricha Schmidta. Organizował on eksterminację Żydów, a w czasie jednej z masowych ich egzekucji został raniony w szyję przez mordowanego Żyda. Z rąk hitlerowskich władz za bohaterstwo w „rozwiązywaniu kwestii żydowskiej" dostał wówczas odznaczenie, a po wojnie, w latach 70. XX w. (jako znany prawnik i wpływowa postać) uniewinnienie w postępowaniu za udział w Holocauście. Dość powiedzieć, że żaden z podobnych urzędników cywilnych czy sędziów niemieckiego aparatu w okupowanej Polsce nie poniósł żadnej odpowiedzialności za dokonane w czasie wojny zbrodnie.

Niemieckie działania w przestrzeni historycznej poszły w kierunku „odniemczenia" zbrodni na rzecz bliżej niezdefiniowanych nazistów, ale także czegoś, co można zdefiniować jako „uwspólnianie" Holocaustu. Chodzi głównie o przedstawianie niechęci do Żydów jako „projektu europejskiego", którego Niemcy byli tylko wykonawcami. To sposób na „rozdzielanie" tej niemieckiej zbrodni na inne narody Europy, w tym także na Polaków.

Metodologia tego ataku jest różna i nie można jej traktować jako całości, bowiem media i rynek naukowy w Niemczech nie są sterowane tak jak w Rosji. Można tu jedynie próbować opisać problem sumowania się wielu czynników: konsekwentnej polityki władz RFN w sprawie „wybielania" hitlerowskich zbrodni, wywodzenia się całego systemu prawnego Niemiec z generaliów III Rzeszy, pochodzenie części mediów z hitlerowskich korzeni, a także klasycznie antypolskie resentymenty i uprzedzenia. W tworzeniu i promowaniu „pedagogiki

wstydu" istotną rolę zawsze odgrywały należące do naszych zachodnich sąsiadów media.

Powyższe działania w przestrzeni publicznej bynajmniej nie wyczerpują zagadnienia. Przeciwnie, są tylko fragmentem systemu przywilejów, orderów i stypendiów, który za pomocą najprostszych narzędzi w postaci środków finansowych, dostępu do dóbr i możliwości, będzie generował postawy „co najmniej miękkie" do ośrodków, z których będą płynęły pieniądze. Nie wolno zapominać o tym, że prace naukowców chociażby z Niemieckiego Instytutu Historycznego w Warszawie prezentują niekiedy w sprawach historii Polski klimat niemal tożsamy z III Rzeszą. Wyrósł tam na przykład historyk opisujący odrodzenie się Polski jako historyczne nieporozumienie i akt orgii, zbrodni i przemocy (Jochen Böhler, *Wojna domowa. Nowe spojrzenie na odrodzenie Polski w latach 1918-1921*, Kraków 2018). Powstanie Wielkopolskie zostało przedstawione tam jako bunt mniejszości, która wykorzystała „dobroduszność niemieckiej większości" (tymczasem to Polacy stanowili w Wielkopolsce większość), a generalnie przyznanie Polsce Pomorza było wtedy stworzeniem „polskiego korytarza" wyrąbanego w „Prusach Zachodnich". Poza jednak tego rodzaju pracami dominują metody bardziej subtelnego oddziaływania na publikacje ukazujące się o Polsce. Klasycznym przykładem może tu być sprawa ostatniej książki o „granatowej" policji w Generalnym Gubernatorstwie pióra Jana Grabowskiego. Autor ów, którego pisarstwo znane jest w Polsce jako pozbawione elementarnych cech wiarygodności naukowej (braku poważniejszego kontaktu intelektualnego pomiędzy budowaną narracją i treścią materiału źródłowego, ustawiczne posługiwanie się zmienionymi lub fałszywymi cytatami itp.), spróbował stworzyć obraz, w którym tzw. „granatowa" policja (składająca się przecież przede wszystkim z Polaków) była odpowiedzialna za śmierć „setek tysięcy" żydowskich uciekinierów i była ważnym elementem niemieckiej machiny Holocaustu. Wszystko to oczywiście jest mistyfikacją budowaną klasycznymi dla tego autora metodami w postaci konfabulacji i fałszywego relacjonowania źródeł (szerzej pisałem o tym w Tygodniku „Sieci" 1.06.2020). Charakterystyczne w tym wszystkim jest to, że w czasie przygotowywania książki

autor był afiliowany przy *Zentrum für Holocaust-Studien* przy *Institut für Zeitgeschichte* w Monachium.

Warto wspomnieć o szerszej działalności tego autora w Polsce. Jest on mianowicie współredaktorem (obok Barbary Engelking) dwutomowego wydawnictwa na temat losów Żydów w czasie Holocaustu (*Dalej jest noc. Losy Żydów w wybranych powiatach okupowanej Polski*, Warszawa 2018), w którym w sposób ciągły, niezgodny z treścią wykorzystywanych źródeł, dopuszczając się systemowych falsyfikacji relacji ze źródeł (albo wprost ich treści), dokonywana jest operacja (na dużą skalę metodami niedozwolonymi w nauce) możliwie jak najszerszego obarczenia rzekomym „współudziałem" Polaków w Zagładzie Żydów. To proces, który dzieje się na naszych oczach. W interesie państwa polskiego jest kwestia zaprezentowania solidnych badań naukowych w obronie zarówno prawdy historycznej na temat historii Polski, jak i prawdy o Holocauście. Tu konsekwencje braku obrony prawdy o minionej historii mogą mieć ogromne znaczenie dla naszego kraju zarówno w wymiarze wizerunkowym, jak i politycznym. Za operacją „historycznego przesunięcia" Polaków ze statusu ofiar ostatniej wojny do kategorii współsprawców Zagłady Żydów mogą stać także ogromne pieniądze. Jak to ładnie wyłożył kiedyś w jednym z artykułów były już dyrektor Muzeum Polin, obecnie trudno będzie od Polski oczekiwać zaspokojenia roszczeń, bowiem Polacy uważają się za ofiary II wojny światowej. Sytuacja powinna zmienić się, kiedy do opinii publicznej dotrą odpowiednie informacje o polskich przestępstwach na Żydach i Holocauście. To już będzie pod względem historycznym (i moralnym) sytuacja, która „może ułatwić rozwiązanie kwestii własności".

Nowa stara Rosja

Próbami przedstawiania historii Polski jako kraju agresywnego, wojowniczego (takie głosy pojawiają się w Niemczech), a ostatnio także dezawuowania Polski jako kraju antysemickiego zainteresowana jest Rosja. Dla niej samo odrodzenie się państwa polskiego (tak jak dla historyka spod znaku NIH) to geopolityczne nieszczęście zakończo-

ne podpisaniem w 1921 r. Traktatu Ryskiego. Sam prezydent Putin określił ówczesną Polskę jako agresora, a sam pokój jako niesprawiedliwy, bo przyznający Polsce część ziem białoruskich i ukraińskich, które ZSRS (a więc z historycznego punktu widzenia: słusznie) odebrała w 1939 r. Swego rodzaju *novum* (w postaci tego rodzaju wywodów i ciągłego powtarzania, że zbrodnia katyńska była należytą „odpłatą" za mordowanie sowieckich jeńców w 1920 r., którego nigdy nie było) kremlowska propaganda w ostatnich latach wzmocniła akcenty przedstawiające Polskę jako kraj antysemicki i współodpowiedzialny za Holocaust. Ta operacja, w przeciwieństwie do tego, co dzieje się w Niemczech, jest zaplanowaną kampanią wymierzoną w Polskę i prezentowaną tak przez oficjalne wystąpienia („publikacje dokumentów") rosyjskich ministerstw obrony narodowej czy spraw zagranicznych, a także pozostających w gestii rosyjskich władz placówek naukowych i archiwalnych. Tu w sposób programowy powrócono do wizji historii Związku Sowieckiego wytyczonej osobiście przez Józefa Stalina w redagowanej przez niego broszurze *Fałszerze historii* z 1946 r. Mamy więc do czynienia z pełną rehabilitacją w czasach Władimira Putina paktu Ribbentrop-Mołotow i polityki sowieckich podbojów dokonywanych w sojuszu z Hitlerem w latach 1939-1941. Słuchając i czytając czołowych polityków rosyjskich odnoszących się do kwestii agresji sowieckiej z września 1939 r., nie sposób nie zauważyć pełnego powrotu do sowieckiej propagandy z lat stalinowskich. Były szef administracji i bliski współpracownik prezydenta Władimira Putina w związku z kolejną rocznicą sowieckiego najazdu powiedział: „Twierdzenia, iż ZSRS jesienią 1939 r. okupował Polskę są niezgodne z faktami historycznymi. Wyraził też ocenę, że przed wkroczeniem Armii Czerwonej we wrześniu 1939 r. Polska jako państwo przestała faktycznie istnieć, a jej władze polityczne i wojskowe rozpierzchły się pod uderzeniem armii niemieckiej" (S. Iwanow, *Oceny, że ZSRS kupował Polskę w 1939, są niezgodne z faktami*, „Dzieje.pl", 17.09.2019).

Obok podobnych kłamliwych twierdzeń o wkroczeniu Armii Czerwonej do Polski, kiedy Wojsko Polskie zostało już rozbite, a władze uciekły do Rumunii (w rzeczywistości walki jeszcze trwały,

a władze polskie opuściły teren kraju już po agresji sowieckiej), pojawiły się te rzadziej wykorzystywane lub całkiem nowe. Agresywna propaganda rosyjska i podporządkowani władzom „dyżurni historycy" przedstawiają Polskę jako kraj ściśle współpracujący z III Rzeszą względnie wprost z „nazistami". To informacja oczywiście nieprawdziwa: przez całe dwudziestolecie międzywojenne II Rzeczpospolita prowadziła politykę równego dystansu, wykluczając jakiekolwiek porozumienia czy sojusze wojskowe zarówno z Niemcami, jak i z Rosją. Odmowa współpracy z Niemcami była jednym z powodów niemieckiej agresji na sprzymierzoną z zachodnimi demokracjami Polskę. Propaganda rosyjska jako dowód współpracy z hitlerowską III Rzeszą wskazuje również zajęcie Zaolzia przez Polskę w październiku 1938 r., po konferencji w Monachium, kiedy los Czechosłowacji został już przesądzony. W istocie władze polskie działały tu bez porozumienia z Niemcami, choć sam fakt skorzystania z okazji i wystosowania do władz w Pradze ultimatum i przyłączenie do Polski ziem z etnicznie polską większością większość polskich historyków traktuje jako polityczny błąd polegający na wpisaniu się w niemiecką politykę roszczeń terytorialnych bez względu na to, że zostały one zaakceptowane przez władze Czechosłowacji i przez zachodnie mocarstwa na konferencji w Monachium. W świetle propagandy rosyjskiej Monachium jest ważnym elementem polityki Anglii i Francji, które miały pchać Hitlera na wschód i wspierać jego podboje. W rzeczywistości konferencja w Monachium była próbą – prawda, że całkowicie nieudaną – ratowania pokoju w Europie. Ale polityka polska w najmniejszym stopniu nie odpowiada ani za wyniki konferencji monachijskiej, ani za późniejszy wybuch II wojny światowej. Ta zaczęła się dlatego, że chcieli jej Adolf Hitler i Józef Stalin.

W tym kontekście, a także w kwestii szukania odpowiedzialnych za eksterminację polskich Żydów i tej tragedii, współodpowiedzialnych trzeba szukać właśnie w Moskwie. Póki bowiem trwał porządek wersalski, którego elementem było istnienie niepodległej Polski i szeregu innych niepodległych krajów w tej części Europy, Żydzi byli bezpieczni. Zburzenie tego systemu przez III Rzeszę i jego najbliższego sojusznika – Związek Sowiecki – było pierwszym krokiem w kierun-

ku urzeczywistnienia planów Hitlera wobec Żydów. Bez współpracy niemiecko-sowieckiej z lat 1939-1931 nie byłoby Holocaustu.

Małym (o ile w ogóle) pocieszeniem może być fakt, że Rosja stale używa broni historycznej wobec krajów bałtyckich, przedstawiając światu Litwinów, Łotyszy i Estończyków jako generalnie (bez wyjaśnienia kontekstu historycznego i nieadekwatnie co do skali zjawisk) hitlerowskich kolaborantów i zbrodniarzy. Najdalej posuniętą „historyczną wojnę hybrydową" rosyjskie media i historycy prowadzą z Ukrainą. Traktują ten kraj jako fragment Rosji i używają historycznych argumentów do stałego kwestionowania jej niepodległości.

IPN, czyli element infrastruktury krytycznej państwa

Zadania Instytutu Pamięci Narodowej zawsze wykraczały poza sferę klasycznej działalności naukowej. Opisanie czasów komunizmu z mechanizmami działania systemu, które uznano za istotne przy tworzeniu Ustawy o IPN, wcale nie jest najważniejsze. Niezwykle ważne stało się odtworzenie losów wielu mniej znaczących ludzi „Solidarności", a także tych, którzy walczyli zbrojnie z komunistami w początkach PRL-u. W tym zakresie podjęto szereg działań nie tylko naukowych, ale także edukacyjnych w różnych obszarach przestrzeni publicznej. Dziś, głównie dzięki działalności IPN-u, osoby takie jak rtm. Witold Pilecki, gen. August Fieldorf „Nil" czy Danuta Siedzikówna „Inka" są powszechnie znane i zajmują należne im miejsce w polskim Panteonie. Ale to tylko jeden wymiar działalności IPN-u. Dziś, po tym niemal ćwierćwieczu, trudno byłoby wskazać placówkę z chociażby zbliżonym dorobkiem badań naukowych XX wieku i zasług w budowaniu narodowej wspólnoty.

Dziś IPN odgrywa w szybko zmieniającym się świecie także inną, zupełnie fundamentalną dla Polski rolę. Ostateczne zwycięstwo pokoju i liberalnej demokracji, które przed laty zapowiadał Francis Fukuyama, okazało się głównie pokazem arogancji i ślepoty. Rywalizacja cywilizacji, imperialnych mocarstw i narodowych interesów toczy się w najlepsze i nic nie wskazuje na to, by ten stan miał w najbliż-

szym czasie ulec zmianie. Przeciwnie: rywalizacja odbywa się na coraz to nowych polach. Już dziś toczy się niemal otwarta walka między światem Zachodu a „państwami zbójeckimi", chociażby w obszarze środków masowej informacji czy cyberprzestrzeni. Chiny na skalę globalną szpiegują i kradną technologie, Rosja atakuje infrastrukturę cyfrową Stanów Zjednoczonych, państw NATO i Ukrainy. Kwestią strategiczną i narzędziem polityki jest dziś budowa rurociągów i sprawa dostępu do surowców energetycznych. Nie inaczej jest z kwestią posiadania własnych mediów. Państwa, które pozwalają kontrolować ośrodki kształtowania opinii publicznej przez obce podmioty, z góry skazują się na utratę suwerenności. Nadto żadne normalne państwo nie będzie w stanie należycie funkcjonować w czasie kryzysów, nie posiadając własnych środków informacji, takich jak telewizja. Pandemia koronawirusa spowoduje zapewne kolejne zmiany definicji infrastruktury krytycznej, którą powinien posiadać kraj wielkości Polski, by zapewnić bezpieczeństwo obywateli. Przepychanki przy imporcie z Chin respiratorów i maseczek zapewne wywołają refleksję, czy zasadne było prywatyzowanie, a jeszcze częściej likwidowanie w Polsce produkcji podstawowych środków ochronnych, sprzętu medycznego i leków. Trzeba też mieć nadzieję, że w przyszłości będziemy dysponować stosowną linią produkcyjną do produkcji szczepionek na wirusy, które mogą pojawić się w przyszłości tak samoczynnie, jak i w wyniku działań państw zbójeckich. Następny wirus może być znacznie bardziej śmiertelny niż atakujący obecnie koronawirus.

Właściwa infrastruktura gazowa czy jednostki do walki z atakiem cyfrowym, a także zaplecze techniczno-medyczne na wypadek pandemii są dziś oczywistymi elementami bezpieczeństwa, tak jak regularna armia i służby bezpieczeństwa państwa. Nie można zapominać, że przestrzenią walki o różne interesy, zwłaszcza ostatnio, stała się także historia.

Być albo nie być

Na działania Rosji, „polskie obozy koncentracyjne" i inne szkalujące wypowiedzi mediów na świecie o Polsce, a także na działania

oszustów udających naukowców w obszarze Holocaustu Polska musi dawać odpowiedź. Tak jak szkolimy żołnierzy i kupujemy samoloty, budujemy gazoporty, trzeba zadbać o wizerunek Polski w świecie i świadomość historyczną własnych obywateli. Inaczej za kilka lat ockniemy się w Polsce, w której młode pokolenie będzie prezentowało wiedzę z serialu *Nasze matki, nasi ojcowie* i będzie się wzruszać przy artykułach Onetu o smutnych świętach niemieckich żołnierzy w okupowanej Polsce. Jak pozwolimy na takie medialne operacje, za chwilę zrobią z nami, co zechcą. Zobaczymy Polskę zbrukaną, upodloną kłamstwami o masowym udziale Polaków w mordowaniu Żydów i współodpowiedzialnością za Holocaust. Katastrofalnie ucierpi na tym międzynarodowa pozycja Polski. Mogą pojawić się znów ostrzej artykułowane roszczenia na dziesiątki miliardów dolarów. Dlatego prawdy historycznej trzeba bronić, a działania IPN-u w tym zakresie – jedynej instytucji, która stanowi solidne zaplecze do takich debat i obrony racji stanu – są dziś i będą w przyszłości nie do zastąpienia.

Wspomniany już tu kilkakrotnie Jan Grabowski z tzw. nowej polskiej szkoły badań Holocaustu (a raczej jego mistyfikacji) stale nawołuje do likwidacji IPN-u i dobrze wie, co robi. Polska przegra wszystko i z każdym, nie tylko z Rosją czy Niemcami, ale naprawdę z byle kim. Nawet z różnej maści naukowymi oszustami.

Ostatnio w mediach pojawia się krytyka wielu działań IPN-u, a także krytyka niektórych luminarzy polskich nauk historycznych. Rytualnie pojawiają się wynurzenia o zmarnowanych pieniądzach i IPN-ie jako „marginesie świata polskiej nauki", który otrzymuje więcej środków finansowych niż inne placówki naukowe. Krytyka ta jest chybiona. Pieniądze idą tu na dużo więcej zadań niż nauka. Większość środków pochłaniają edukacja, poszukiwania szczątków ofiar komunizmu i ich upamiętnianie. Jeszcze więcej kosztuje działalność dwóch (niezależnych od władz IPN-u) prokuratur: Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu i Biura Lustracyjnego, których działalność jest kulą u nogi Instytutu. Podniesiona przez prof. Wnuka sprawa braku wymogu dla naukowców IPN-u systematycznego zdobywania stopni naukowych i uzyskiwania publikacjami

punktów może być traktowana nie jako wada, a błogosławieństwo. Praca przy ogólnopolskim, ambitnym projekcie wymaga czegoś więcej niż pogoń za stopniami i punktami, która po reformie ministra Gowina stała się katastrofą polskiej humanistki.

Słowa o „marginalnej" roli IPN-u w polskiej nauce można skwitować odesłaniem do listy nominacji i zwycięzców konkursów na książki historyczne w ostatnim dziesięcioleciu. Życzyłbym takich sukcesów każdej placówce naukowej w Polsce.

W każdej krytyce zawsze tkwi jakieś ziarno prawdy. Ale nie ma poważniejszych wątpliwości, że bez względu na ilość przekazanych pieniędzy żadna inna placówka naukowa nie zastąpi IPN-u. Jak widać, bez słowa sprzeciwu „główny nurt" polskiej nauki pozwala na funkcjonowanie Centrum Badań nad Zagładą Żydów IFIS PAN, których jak dotąd nikt nie zobligował nawet do odpowiedzi na artykuły, gdzie zilustrowano konkretnymi przykładami zarzuty manipulacji źródeł metodami na miarę i skalę KC PZPR z lat 50. XX w. Może dlatego, że autorzy tych machinacji „wyrabiają punkty"?

Niech Bóg ochroni Polskę przed sytuacją, kiedy w dziedzinie podstawowych interesów państwa będzie ona zdana wyłącznie na polskie uniwersytety i PAN. Pasują one do obrony prawdy historycznej i interesów państwa jak – sięgając do klasyka – przysłowiowa krowa pod siodło. Z tej perspektywy sytuacja jest prosta. Albo 40-milionowy kraj leżący pomiędzy dwoma historycznie umiarkowanie sympatycznymi sąsiadami, w miejscu krzyżowania się potężnych interesów politycznych i finansowych, będzie prowadził własną politykę historyczną, albo stanie się postawą sukna, które będzie rwał kto żyw naokoło.

Historyk może pomstować na takie instrumentalne traktowanie historii, gdzie każdy próbuje wykorzystać ją do swoich nie zawsze nobliwych celów lub wręcz – jak dziś na przykład Rosja wobec Ukrainy – do uzasadnienia planowanej agresji i likwidacji sąsiedniego państwa. Wojna interesów w przestrzeni historycznej trwa i w świecie błyskawicznego rozwoju mediów coraz bardziej oderwanym od treści wiarygodnych badań naukowych raczej będzie przybierała na sile. Nieobecni nie będą mieli racji i za brak właściwej polityki

informacyjnej, umiejętności, a przede wszystkim woli ukazywania swojej prawdziwej historii i zapłacą wysoką cenę. Jestem zwolennikiem wyrzeczenia się prowadzenia własnej polityki historycznej, tak jak pełnego światowego rozbrojenia, także w obszarze historii. Pod warunkiem wszakże, że zrobimy to jako ostatni.

Fragment powyższego tekstu został opublikowany w 2021 roku w postaci artykułu w tygodniku „Sieci".

Finansowa rewolucja u bram III RP

dr Marek Dietl

Historia Polski uczy nas, że utrata zdolności do kontrolowania pieniądza i podatków, czyli sfery monetarnej oraz fiskalnej, zawsze na końcu skutkowała utratą niepodległości lub pogorszeniem się międzynarodowej pozycji Polski. Musimy mieć pełną kontrolę nad naszą walutą, by reagować na kryzysy, i jednocześnie musimy kontrolować naszą sferę fiskalną, żeby budować sprawne państwo. Dzisiaj dodatkowym wymiarem jest konieczność wprowadzenia cyfrowego złotego (CBDC), inaczej możemy utracić kontrolę nad sferą monetarną, ponieważ cyfrowe waluty innych krajów okażą się bardziej atrakcyjne dla naszych obywateli niż pieniądz tradycyjny.

Rys historyczny

W czasach, w których traciliśmy kontrolę nad naszym pieniądzem, jako państwo przeważnie popadaliśmy w kłopoty. Tak było w okresie rozbicia dzielnicowego czy w epoce rozkwitu państwa krzyżackiego u naszych granic. Później, za czasów kanclerza Jana Zamoyskiego, nastąpiła, tak byśmy to dzisiaj określili, konsolidacja finansów publicznych. Uporządkowania finansów domagał się wówczas także ruch egzekucyjny. Średnia szlachta żądała zwrotu dóbr królewskich bezprawnie przekazanych magnatom i realizacji uprzednio ustalonych praw. Choć realizacja postulatów, wskutek rezerwy króla i oporu możnowładztwa, udała się jedynie połowicznie, to jednak uzyskane fundusze pozwoliły wzmocnić obronność poprzez ustanowienie wojsk kwarcianych, a pokłosiem reform było też wprowadzenie jed-

nolitej waluty – florena polskiego, zwanego już wtedy złotym. Następnie znowu musieliśmy się odbudowywać po szwedzkiej grabieży w XVII w. Za rządów Sasów to, co dzisiaj nazywamy Skarbem Państwa, uległo *de facto* rozpadowi – nastąpiła jego oligarchiczna prywatyzacja (podobnie jak w niektórych krajach naszego regionu w latach 90.), bo rody magnackie przy zagranicznym wsparciu stawały się rozproszonymi ośrodkami władzy. Doprowadziło to do dekompozycji tego fiskalnego układu. Stanisław August Poniatowski próbował zreformować mennicę królewską i narzucić pieniądz centralny, ale z różnych powodów nie udało się już tego przeprowadzić.

Z historii Polski płynie wniosek, że niezdolność do kontrolowania pieniądza i podatków, czyli sfery fiskalnej oraz monetarnej, zawsze kończyła się utratą niepodległości lub pogorszeniem się naszej pozycji w Europie. Można się oczywiście zastanawiać, co było przyczyną, a co skutkiem. Nie możemy z pewnością stwierdzić, czy rozkład polityczny państwa powodował, że waluta się osłabiała, czy ta zależność przebiegała w drugą stronę. Te doświadczenia wywołały jednak pewną traumę wśród elit politycznych. Gdy po zaborach i odzyskaniu niepodległości wkraczaliśmy w nową rzeczywistość, a nasza pierwsza waluta, marka polska, ze względu na zaburzenia gospodarcze była bardzo słaba, to w 1924 r. zwalczaliśmy ten problem niezwykle agresywnie poprzez wprowadzenie polskiego złotego oraz bardzo restrykcyjną politykę monetarną i fiskalną po reformach Władysława Grabskiego. Po traumie z okresu tuż po I wojnie światowej utożsamiano powszechnie potęgę Rzeczypospolitej z siłą pieniądza. Jak zauważył na XI Kongresie Polska Wielki Projekt członek zarządu Narodowego Banku Polskiego Paweł Szałamacha, ówczesna nadostrożność decydentów w polityce monetarnej wynikała wprost z doświadczenia powojennej hiperinflacji. Jednak decyzja marszałka Józefa Piłsudskiego o tym, aby powiązać polską walutę ze złotem, a następnie utrzymać unię walutową m.in. z Francją w ramach Złotego Bloku, okazała się wręcz zabójcza dla naszej gospodarki, szczególnie po 1929 r. Jak wyliczyli Stefan Kawalec i Ernest Pytlarczyk w książce *Paradoks euro*, produkcja przemysłowa w Polsce mogłaby być o 50 proc. wyższa, gdyby nie deflacyjna polityka mone-

tarna II RP. W odróżnieniu od naszego zachodniego sąsiada bardzo późno weszliśmy na etap aktywnego kreowania polityki monetarnej. Z tego powodu realne przygotowania do wojny i prawdziwa ekspansja gospodarcza rozpoczęły się w Polsce dopiero w 1936 r. Utworzono wówczas fundusz na dozbrojenie, na rzecz którego chętni obywatele oddawali złoto – niestety, nie zdążyliśmy zrealizować wydatków z tego funduszu. Razem z zasobami Banku Polskiego został on bohatersko ewakuowany z kraju w 1939 r. Zatem przed II wojną światową byliśmy przywiązani do standardu złota i pozostawaliśmy w pewnego rodzaju unii monetarnej m.in. z Francją. Zamiast tak jak Niemcy prowadzić ekspansywną politykę gospodarczą, czy tak jak Amerykanie w ramach New Deal podejmować próby wypełnienia luki popytowej, skupialiśmy się na tym, aby utrzymać wartość pieniądza o zbyt wysokim dla nas kursie walutowym, podobnie jak obecnie Hiszpania, Włochy czy Grecja. Ogólny wniosek z naszej historii jest zatem taki, że musimy zawsze mieć pełną kontrolę nad naszą walutą, reagować na kryzysy i jednocześnie powinniśmy kontrolować naszą sferę fiskalną, żeby budować sprawne państwo.

I. LIMIT DŁUGU PUBLICZNEGO Jeżeli dla bezpieczeństwa i suwerenności naszego państwa kluczowe jest, żebyśmy posiadali pełną kontrolę nad sferą monetarną i fiskalną, to jednocześnie musimy się zastanowić, czy dysponujemy w nich także pełną swobodą. Otóż nie mamy jej w zakresie kształtowania polityki fiskalnej. Naszym sukcesem są skonsolidowane finanse i rosnące wpływy podatkowe, ale z drugiej strony jesteśmy związani nieszczęsnym konstytucyjnym limitem długu publicznego. Po pierwsze, ten limit jest bardzo restrykcyjny, bo nikt w Europie już takiego nie ma – dla przykładu Niemcy mają limit na poziomie 85 proc. Po drugie, nie niuansuje tego, czy to jest dług w walutach obcych, czy w walucie krajowej. Dług w walucie krajowej jest oczywiście dużo mniej ryzykowny, bo zawsze możemy ją dodrukować. Sami sobie jednak narzuciliśmy w 1997 r. ograniczenie, które dzisiaj, przy ultraniskich stopach procentowych, bardzo nam doskwiera. Powinniśmy zadłużyć się na dwadzieścia, trzydzieści lat według stałej stopy procentowej i zbudować dzięki temu całą

infrastrukturę, ale nie możemy tego zrobić. Zamiast konstytucyjnego limitu, dbając o stan finansów państwa w długim okresie, moglibyśmy powołać Radę Polityki Fiskalnej, która określałaby maksymalny deficyt budżetowy na dany rok fiskalny, biorąc pod uwagę czynniki zewnętrzne, poziom luki popytowej, długoterminowe prognozy gospodarcze, potrzeby infrastrukturalne itd. Zyskalibyśmy elastyczność, jednocześnie dbając o stan finansów publicznych. Obecnie jest wyjątkowo dobry czas do taniego zadłużania się i rozwijania kraju. Powinniśmy więc wytworzyć przestrzeń fiskalną do dalszych inwestycji.

II. INFLACJA Drugi filar naszego bezpieczeństwa dotyczy polityki monetarnej. Z jednej strony mamy bardzo atrakcyjny kurs złotego dla naszych eksporterów, co sprzyja rozwojowi gospodarczemu kraju. Z drugiej strony rosną oczekiwania inflacyjne – rośnie inflacja producencka, nie tylko konsumpcyjna. Naszym wyzwaniem jest, by znaleźć w tej sytuacji równowagę i wspierać nasz eksport, a równocześnie mieć pod kontrolą oczekiwania inflacyjne. Dzisiaj inflacja utrzymuje się na poziomie poniżej 5 proc., natomiast jeśli miałaby dalej rosnąć, to byłoby to pewne zagrożenie, gdyż gwałtowne korekty w cyklu gospodarczym w postaci istotnych podwyżek stóp procentowych są bardzo niewskazane.

III. KREDYTY FRANKOWE Według raportu NBP z 16 czerwca br. kredyty frankowe są obecnie największym zagrożeniem dla systemu finansowego Polski. Przez to, że się zadłużamy w walutach obcych – czy jako państwo, czy jako obywatele, czy przedsiębiorstwa – tracimy kontrolę nad sferą monetarną. Powinny obowiązywać ostrożnościowe bariery dotyczące zadłużania się w walutach innych niż polski złoty. Warto jak najszerzej promować złotego poprzez zawieranie tzw. *masters agreements* z innymi krajami, gwarantując im, że zawsze do określonej ilości wymienimy ich lokalną walutę na polskiego złotego. Każdemu bankowi centralnemu powinno na tym zależeć. Każdy kraj chce emitować swoją walutę, bo to najtańszy sposób finansowania gospodarki. Dodatkowo jednym z elementów ostrożności związanej z kredytami walutowymi dla przedsiębiorstw oraz konsumentów

powinno być to, że Narodowy Bank Polski zawierałby umowę swap, żeby móc wymienić nasze polskie złote na euro lub dolary z rezerw walutowych.

IV. STREFA ZŁOTEGO Wstępując do Unii Europejskiej, Polska zobowiązała się do przyjęcia waluty euro, lecz bez podania konkretnego terminu. Zawieranie terminu wstąpienia do strefy euro w dokumentach akcesyjnych byłoby niewłaściwe, gdyż przyjęcie wspólnej waluty jest obwarowane szeregiem kryteriów. To daje Polsce możliwość wybrania dogodnego terminu zmiany waluty z gospodarczego i społecznego punktu widzenia. Perspektywa przyjęcia euro jest więc odległa i niepewna, dlatego też należy określić strategie rozwoju polskiego złotego. Obecnie Polska jest dwudziestą drugą czy dwudziestą trzecią największą gospodarką świata. Jednocześnie, jakość otoczenia instytucjonalnego jest wysoka, a polityka monetarna przewidywalna, czego nie można powiedzieć o większych od Polski gospodarkach wschodzących. To oznacza, że Polska powinna zacząć dążyć do popularyzacji polskiego złotego w obrocie gospodarczym oraz w rezerwach walutowych innych krajów. Proces zwiększania popularności naszej waluty mógłby być połączony z podobnym procesem dla krajów naszego regionu (z uwagi na spełnianie warunków jakościowych), czyli z Czechami i Węgrami. Umożliwiłoby to naszemu regionowi uniezależnienie się w pewnym horyzoncie od finansowania w walutach obcych, co doprowadziłoby do wyższych ratingów kredytowych i jeszcze korzystniejszych warunków finansowania.

V. INTELIGENTNE FINANSOWANIE WYDATKÓW ZBROJNYCH Kolejnym filarem bezpieczeństwa finansowego jest odpowiedzialne zarządzanie wydatkami na obronność, np. wykorzystanie instrumentów rynku finansowego, żeby dokonywać zakupów sprzętu dla armii. Jeśli ze środków budżetowych kupimy uzbrojenie o wartości 100 mld zł, to wpiszemy w deficyt i w dług publiczny 100 mld, chociaż ten sprzęt będziemy użytkować przez kilkadziesiąt lat. W budżecie nie działa mechanizm amortyzacji. Dlatego warto zbudować wehikuł specjalnego przeznaczenia, który dokonywałby zakupu i potem leasingował

sprzęt armii. Wtedy płaci się co roku ratę leasingową, która kosztuje Skarb Państwa kilka miliardów złotych rocznie. To konieczny warunek, by w inteligentny sposób zapewnić finansowanie wydatków zbrojnych, bo obecnie niepotrzebnie zabieramy sobie przestrzeń fiskalną.

VI. BEZPIECZEŃSTWO CYFROWE Nowym wymiarem bezpieczeństwa finansowego jest sfera cyfrowa. System finansowy kraju musi być bezpieczny w sensie cyberbezpieczeństwa, nie może być podatny na ataki hakerskie. Stąd przypomnienie postulatu PiS z 2015 r., żeby w policji i w wojsku znieść widełki płacowe dla pracowników informatycznych, żeby specjalistów do pilnowania naszego systemu finansowego zatrudniać po stawkach rynkowych. Nie potrzeba do tej pracy wielu osób, ale muszą być to najlepsi z najlepszych.

VII. WALUTA CYFROWA Na powyższe filary nakłada się jeszcze zmiana paradygmatu myślenia o finansach, którą wprowadzają waluty cyfrowe banku centralnego (CBDC). Prace nad tą walutą w różnych krajach są już bardzo zaawansowane. Na początku czerwca Bank Anglii zainaugurował debatę na temat stablecoinów i waluty cyfrowej. Z kolei banki centralne Francji i Szwajcarii będą współpracować z bankami komercyjnymi w celu przetestowania płatności transgranicznych w walucie cyfrowej. Latem swój raport na temat CBDC opublikuje amerykański Fed. Natomiast Chiny planują wdrożyć u siebie CBDC już w 2022 r.

Waluty cyfrowe będą oznaczać rewolucję w światowych finansach. Tak jak kiedyś nastąpiło odejście od funta na rzecz dolara, tak teraz może nastąpić odejście od walut tradycyjnych. CBDC oferuje bardzo dużą wygodę użytkownikom i doprowadzi do przetasowania na rynku finansowym, zmieniając dotychczasową rolę banków. Jeśli każdy obywatel będzie miał wirtualny rachunek w banku centralnym świata, oznacza to, że będzie mógł ze swoim partnerem biznesowym np. z Malezji rozliczyć się w czasie rzeczywistym w dowolnej walucie: w walucie Malezji czy w walucie polskiej, albo w dolarze, albo w prywatnej walucie lub w meta-walucie. Co więcej, cyfrowe waluty oferują

nowe instrumenty zarządzania gospodarką poprzez dokładniejsze kształtowanie polityki monetarnej i jej większą synergię z polityką fiskalną. Możliwości w tym obszarze są ogromne. Jeżeli nie wprowadzimy cyfrowego złotego, to może się zdarzyć, że stracimy kontrolę monetarną, ponieważ inne waluty będą bardziej atrakcyjne dla biznesu. Musimy aktywnie działać, by – jak zauważył prezes Ramp Network Szymon Sypniewicz podczas tegorocznego Kongresu Polska Wielki Projekt – polski złoty nie podzielił losu Naszej Klasy w konkurencji z Facebookiem: „Czy w obliczu nowego świata finansów, w którym wszystko jest cyfrowe i nie wymaga zakotwiczenia w państwach narodowych, nie wymaga fizycznych placówek banków (...) nowe aktywa nie zaczną wypierać polskiego złotego? (...) Państwa, które pozostaną bierne i nie będą reagować na cyfrową rewolucję, przegrają. Ich suwerenność będzie powoli erodować pod naporem walut, które będą emitowane przez podmioty pozapaństwowe, mogą to być korporacje takie jak Facebook, albo rozproszone sieci emitentów kryptoaktywów". Często pojawia się zarzut, że przecież możemy wszędzie płacić kartą, ale tutaj chodzi przede wszystkim o rozliczenia biznesowe. Najwięcej transakcji na świecie wykonuje się w związku z inwestycjami finansowymi i transakcjami biznesowymi.

W każdym rankingu informatycznym polscy specjaliści IT zajmują pierwsze miejsce, mamy więc wysoko wykwalifikowany kapitał ludzki. Odpowiednio wczesny start w wyścigu po cyfrową walutę da nam możliwość stania się dostawcą technologii do emitowania cyfrowego pieniądza dla innych krajów. Nie jest przypadkiem, że giełdy kryptowalut czy różne inne rozwiązania wokół cyfrowych walut pochodzą z Polski, ponieważ mamy w tym obszarze bardzo wysokie kompetencje. Dla Polski najważniejsze jest to, żeby przygotować technologię do obsługi cyfrowego złotego. Jako Giełda Papierów Wartościowych pracujemy nad rozwiązaniami opartymi o blockchain i jesteśmy gotowi udostępnić nasze zaplecze informatyczne. Widzimy, że nasi koledzy z giełd z innych krajów pracują ze swoimi bankami centralnymi nad integracją swoich cyfrowych walut do transakcji na rynkach kapitałowych. My jesteśmy do tego przygotowani – jak tylko Narodowy Bank Polski będzie zainteresowany, to bardzo chętnie pomożemy.

Cyberbezpieczeństwo państwa

Paweł Wiszniewski

Krajobraz cyberbezpieczeństwa

Technologie są nowe nie tylko dlatego, że są odmienne od poprzednich, ale dlatego, że **dogłębnie zmieniają samo nasze doświadczanie, nasz aparat pojęciowy, nasz język.** Trzeba uniknąć naiwnej wiary, że technologie teleinformatyczne[1] pozostają do naszej dyspozycji i nie zmieniają o jotę naszego sposobu postrzegania rzeczywistości. Doświadczamy nowego egzystencjalnego kontekstu wytworzonego w cyberprzestrzeni przez nowe media, w tym media społecznościowe i – w konsekwencji – „mutacji antropologicznej". O zjawisku wirtualności i życiu w hałasie oraz wśród stałych przekazów audiowizualnych, doprowadzających do „mutacji antropologicznej", mówił w 2011 r. Papież Benedykt XVI[2].

Czy „cyberbezpieczeństwo" dotyczy jedynie zagrożeń pochodzących z „cyberprzestrzeni" i czy uwzględnia jedynie ochronę wirtu-

[1] Pod pojęciem technologii informacyjnych i komunikacyjnych (w skrócie ICT, ang. *Information and Communication Technologies*, nazywanych zamiennie technologiami informacyjno-telekomunikacyjnymi, teleinformatycznymi lub technikami informacyjnymi) kryje się rodzina technologii przetwarzających, gromadzących i przesyłających informacje w formie elektronicznej.

[2] Papież Benedykt XVI składał wizytę w Kalabrii, w Serra San Bruno, gdzie odwiedził klasztor mnichów kartuzów, założony ponad 900 lat temu przez świętego Brunona z Kolonii. W homilii podczas nieszporów papież powiedział, zwracając się do mnichów: „Rozwój mediów w ostatnich latach rozszerzył i wzmocnił zjawisko, które już zarysowało się w latach 1960 – wirtualność, która grozi tym, że zdominuje rzeczywistość. Coraz bardziej, także nie dostrzegając tego, ludzie pogrążeni są w wymiarze wirtualnym, z powodu przekazów audiowizualnych, które towarzyszą im w życiu od rana do wieczora. Najmłodsi, którzy już urodzili się w tych realiach, wydają się chcieć wypełnić muzyką i obrazem każdy pusty moment, niemal, jakby ze strachu przed tą pustką" – zauważył papież. Wyraził opinię, że tendencja ta, zwłaszcza wśród młodzieży w wielkich miastach, „osiągnęła dzisiaj poziom, który skłania do tego, by mówić o mutacji antropologicznej".

alnych zasobów w ramach „cyberprzestrzeni"? Czy „cyberbezpieczeństwo" stosuje się również do zasobów fizycznych, takich jak systemy kontroli przemysłowej, linie produkcyjne, elektrownie itp., chociaż nie są one elementem „cyberprzestrzeni", lecz świata realnego? Wypada już na wstępie stwierdzić, że cyberbezpieczeństwo będzie się przenikać wzajemnie z innymi obszarami działań, w tym z fizycznym bezpieczeństwem infrastruktury sieciowej.

System cyberbezpieczeństwa obejmuje trzy poziomy: a) **techniczny system cyberbezpieczeństwa**, opisujący organizację w kategoriach przepływu komunikatów, działań związanych z bezpiecznym przetwarzaniem danych, politykę ochrony systemów, infrastruktury teleinformatycznej, wskazanie organizacyjnych i technicznych zabezpieczeń zasobów informacyjnych i systemów; b) **formalny system cyberbezpieczeństwa** – prawne zabezpieczenie zasobów informacyjnych, regulacji prawnych, jawne nakazy dotyczące zachowań: zasady, regulaminy, polityka ochrony samych informacji, ochrony danych osobowych, informacji niejawnych, tajemnic ustawowo chronionych, dostępu do informacji publicznej i procedur, cyberobronę, tj. formalna kultura cyberbezpieczeństwa; c) **nieformalny system cyberbezpieczeństwa**, czyli zbiór wzorców zachowań, kodeksy dobrych praktyk z tego zakresu, tj. nieformalna kultura cyberbezpieczeństwa.

Struktury bezpieczeństwa narodowego przewidziane w XX w. okazały się nieadekwatne do zagrożeń cyberbezpieczeństwa, przed którymi stoi Polska w XXI w. Dawny porządek i strategie, stworzone w celu przeciwdziałania zewnętrznym zagrożeniom z jednej strony, a kryzysom bezpieczeństwa wewnętrznego z drugiej, nie mogły ochronić nas przed otaczającymi zewsząd konfliktami w cyberprzestrzeni, ponieważ zostały zaprojektowane z myślą o różnych czasach i zagrożeniach.

Rządy państw, które mają za zadanie chronić dane obywateli i poufne informacje, stały się popularnym celem ataków. Dzisiejszy krajobraz cyberzagrożeń obejmuje coraz większą liczbę wyrafinowanych wrogich aktorów, zaawansowanych ukierunkowanych naruszeń bezpieczeństwa. Hakerzy, cyberprzestępcy, wrodzy aktorzy państwowi i niepaństwowi używają szerokiej gamy zaawansowanych

metod kradzieży danych, włamywania się do systemów rządowych, powszechnej manipulacji i dezinformacji.

Dodatkowo, żyjąc w cyfrowej epoce, jesteśmy bardzo niewinni i naiwni zarazem, nie rozumiejąc, co obserwujemy – nowy porządek gospodarczy. Jak pisze Shoshana Zuboff[3], jest to „pasożytnicza logika ekonomiczna, w której produkcja towarów i usług jest podporządkowana nowej globalnej architekturze modyfikacji zachowań", swoisty ruch, który ma na celu narzucenie nowego porządku zbiorowego opartego na całkowitej pewności – uwarunkowany danymi z osobowych cyfrowych ewidencji i czerpiący zyski z masowego inwigilowania ludzi. To wszystko dzięki naszej aktywności na urządzeniach cyfrowych, podłączonych do Internetu i pozostawiających cyfrowe dowody i znaki.

Firmy kapitalizmu inwigilacji i/lub nadzoru reprezentują takie molochy globalne jak Google, Amazon, Facebook, Apple i Microsoft. Jeden z tych cyfrowych gigantów – Facebook – dokonał aktualizacji algorytmu głównej strony serwisu społecznościowego z postami znajomych oraz udostępnionych przez polubione strony. Po zmianie algorytmu łatwiej można było rozpowszechniać dezinformację i skandalizujące posty. Celem było wywołanie internetowej „społecznościowej wojny domowej", a jako przykład kraju, który miał paść ofiarą tej strategii, podano Polskę podczas kampanii wyborczej w 2019 r. Informacje ujawniono w ramach przecieku wewnętrznej korespondencji największego serwisu społecznościowego świata. Amerykańskie media pisały o „Facebook Papers"[4] w 2018 r.

Prefiks ***cyber***- jest szeroko stosowany od ok. 2000 r. w odniesieniu do wszelkich zagadnień bezpośrednio lub pośrednio związanych z korzystaniem z Internetu, telekomunikacji, różnych działań cyfrowych i automatycznego przetwarzania informacji. Obecnie ob-

---

[3] S. Zuboff, *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, tłum. A. Unterschuetz, Poznań 2020.

[4] Inaczej *The Facebook Files: A Wall Street Journal Investigation* – seria doniesień prasowych „The Wall Street Journal" opublikowanych po raz pierwszy w połowie września 2021 r., opartych na wewnętrznych dokumentach z Facebook Inc. (obecnie Meta Platforms), które wyciekły dzięki sygnalistce Frances Haugen.

serwujemy olbrzymią dynamikę w dziedzinie słowotwórstwa, wytworzoną niespotykanymi wcześniej usprawnieniami technologicznymi w obrębie zarówno narzędzi komunikowania, jak i – niestety – samych treści, tj. dezinformowania, manipulowania czy sterowania zachowaniami konsumpcyjnymi i wyborczymi znacznej liczby odbiorców. Dzisiejszy i przyszły rozwój technologii dodatkowo wymusza zajęcie stanowiska wobec nowego wymiaru bezpieczeństwa i potencjalnego konfliktu w cyberprzestrzeni, używania broni informacyjnej do dyskredytowania i delegitymizacji rywali, przeciwników i wrogów, co także radykalnie zmienia i uzupełnia istniejące normy i doktryny odnoszące się do współczesnej wojny.

Wszystko staje się ***cyber-*** i umożliwia popularyzację niekiedy trudnych dyscyplin technicznych (bezpieczeństwo systemów informatycznych, architektura sieci, procesy przetwarzania przemysłowego). Mówimy więc o cyberprzestępczości, aby odnieść się do wykorzystywania nowych technologii informatycznych do popełniania przestępstw, cyberoperacji (operacji w cyberprzestrzeni), cyberobrony, cyberprzemocy etc. Rosnącemu używaniu przedrostka ***cyber-*** towarzyszy niekiedy zjawisko odrzucenia ze strony ekspertów technicznych (teleinformatyków), którzy postrzegają go jedynie jako wyraz ignorancji i sposób na udawanie „modnego" słownictwa.

W literaturze wojskowej termin ***cyber*** jest używany w szerszym znaczeniu, odnosi się do wykorzystania Internetu i technologii komputerowych do operacji w tzw. piątej domenie. NATO w lipcu 2016 r. uznało, że cyberprzestrzeń jest domeną operacji, w których NATO musi bronić się równie skutecznie jak w powietrzu, na lądzie i na morzu (a nawet w kosmosie). Przykładami takich operacji są „cyberoperacje", „cyberwojna" i „cyberataki", w zależności od ich intensywności.

Wielowymiarowe bezpieczeństwo narodowe

Nasze społeczeństwo – rząd, siły zbrojne i służby, władze regionalne i lokalne, firmy sektora prywatnego, operatorzy infrastruktury krytycznej, organizacje non-profit i uniwersytety, a nawet życie prywatne

obywateli – jest nieustannie atakowane przez ogromną liczbę cyberprzestępców o coraz większych możliwościach. Zespoły zajmujące się wieloaspektowym bezpieczeństwem narodowym, m.in. bezpieczeństwem informacyjnym, cyberbezpieczeństwem i cyberobroną, wymagają ciągłej edukacji, szkoleń, kolektywnego doświadczenia i kreatywnego myślenia, które pozwolą im nieustannie się rozwijać. Muszą także tworzyć wielodziedzinowe zespoły reagowania w wielu obszarach i budować zdolności do błyskawicznej wymiany danych i stałej współpracy.

Wymiar „cyber" odgrywa dziś wyjątkową i bardzo specyficzną rolę także w odniesieniu do zagrożeń hybrydowych, gdyż to, co dzieje się w świecie rzeczywistym – w tym każdy konflikt polityczny i militarny – ma również miejsce w cyberprzestrzeni (cyberprzestępczość, szpiegostwo, wywieranie wpływu, manipulacja informacją, dezinformacja, propaganda, terroryzm, a nawet działania sił zbrojnych). Charakter zagrożeń dla bezpieczeństwa narodowego nie uległ zmianie, ale cyberprzestrzeń pozwala na zwiększenie szybkości, rozproszenia i siły ataku, jego sprawcom zapewniając anonimowość i niewykrywalność[5]. W aspekcie technologicznym w najbliższych dekadach dominującym trendem będzie rosnący poziom zaawansowania technologicznego. Wśród technologii o najwyższym potencjale wzrostu i znaczeniu dla środowiska bezpieczeństwa można wskazać: **sztuczną inteligencję**, **systemy autonomiczne**, **systemy biomechaniczne**, **technologie 6G i 7G**, **technologię wielkobazodanową** (ang. *Big Data*), **informatykę kwantową**, **robotykę**, **nanotechnologię**, **technologię wytwarzania przestrzennego 3D i 4D**, **biotechnologię** oraz **technologię humanoidalną** i **inżynierię genetyczną**. Istotnym zagrożeniem w kontekście bezpieczeństwa, stanowiącym konsekwencję rosnącej powszechnej dostępności do nowoczesnych technologii, będzie również **utrata przewagi technologicznej podmiotów pań-**

[5] Dotyczy to zwłaszcza *Deep Web* (wszelkie informacje lub dane internetowe, celowo i/lub nieumyślnie ukryte, niewidoczne lub niedostępne dla wyszukiwarek), *Darknet* (celowo ukryte zasoby Internetu zapewniające anonimową łączność sieciową i usługi), *Dark Web* (strony internetowe, hostowane w sieciach nakładkowych i zwykle nie są dostępne bez specjalnego oprogramowania, takiego jak przeglądarka TOR).

stwowych nad podmiotami niepaństwowymi czy potencjalnym przeciwnikiem. Szczególną kwestią pozostanie dalsze „podłączanie się" do sieci przez wszystkie państwa świata – mimo że obywatele niektórych rządzonych autokratycznie krajów mają ograniczenia w dostępie do Internetu – co będzie sprzyjać dalszemu rozwojowi sieci globalnej.

Niska cena, anonimowość i asymetria oznaczają, że mniejsi aktorzy mają większą zdolność sprawowania władzy w cyberprzestrzeni niż w wielu bardziej tradycyjnych dziedzinach polityki globalnej. Narzędzia, które może zastosować wrogi podmiot, mają na celu spowodowanie degradacji, zakłócenia lub zniszczenia sieci bądź też uzyskanie dostępu do danych i informacji. Dostęp do informacji może być również celem wrogiego podmiotu w celu zbierania danych wywiadowczych i ograniczenia wykrywalności.

Cyberbezpieczeństwo to bezpieczeństwo narodowe

Ponieważ skala i złożoność cyberzagrożeń i cyberprzestępstw rosną, państwo polskie stara się ulepszyć potencjał reagowania i chronić integralność, bezpieczeństwo i odporność infrastruktury cyfrowej oraz sieci i usług komunikacyjnych. Większe cyberbezpieczeństwo to większe zaufanie do technologii cyfrowych i bezpieczna oraz otwarta cyberprzestrzeń. Jeszcze kilka lat temu idea cyberbezpieczeństwa i infrastruktury państwa – zarządzania cyberryzykami w wielu dziedzinach – w każdym ministerstwie była realizowana osobno. Obecnie widać, że **cyberbezpieczeństwo stało się istotnym elementem koncepcji bezpieczeństwa państwa**. Znalazło to wyraz w nowej **Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej** zatwierdzonej, w drodze postanowienia, przez Prezydenta Rzeczypospolitej Polskiej Andrzeja Dudę, 12 maja 2020 r.

Strategia Bezpieczeństwa Narodowego 2020 określa kompleksową wizję kształtowania bezpieczeństwa narodowego Rzeczypospolitej Polskiej we wszystkich jego wymiarach. Główna treść strategii została oparta na czterech filarach. **Pierwszy filar to bez-**

pieczeństwo państwa i obywateli; **drugi filar stanowi o bezpieczeństwie międzynarodowym Polski**, **trzeci o tożsamości i dziedzictwie narodowym**, a **czwarty odnosi się do rozwoju społecznego, gospodarczego i ochrony środowiska**. Dotyczą one strzeżenia niepodległości, nienaruszalności terytorialnej, suwerenności oraz zapewnienia bezpieczeństwa państwa i obywateli. W tym celu należy między innymi zintegrować zarządzanie bezpieczeństwem narodowym oraz dostosować krajowy system zarządzania kryzysowego do systemu reagowania kryzysowego NATO, tak aby obejmował również obszar konfliktu polityczno-militarnego i umożliwiał płynne przechodzenie od stanu pokoju do stanu kryzysu i stanu wojny, a także tworzył skuteczne narzędzia do przeciwdziałania i zwalczania zagrożeń, również hybrydowych. **Odporność państwa na zagrożenia** zostaje podniesiona przez tworzenie systemu obrony powszechnej, opartej na wysiłku całego narodu, oraz budowanie zrozumienia dla tych spraw.

W Strategii Bezpieczeństwa Narodowego 2020 wiele uwagi poświęcono kwestii cyberbezpieczeństwa. Przypomina się o **kontekście rewolucji cyfrowej, w której należy uwzględnić szczególną rolę cyberprzestrzeni oraz przestrzeni informacyjnej**, co również stwarza pole do dezinformacji i manipulacji informacją i wymaga prowadzenia skutecznych działań z zakresu komunikacji strategicznej. Dziś, by sparaliżować kierownictwo państwa, pracę pojedynczego urzędu, biura, całego miasta czy samorządu lokalnego, wystarczą tak naprawdę komputer i dostęp do sieci.

Podkreślono konieczność **uzyskania zdolności operacyjnej do prowadzenia działań militarnych w cyberprzestrzeni oraz rozwijania wojsk obrony cyberprzestrzeni**. Postanowiono podnieść poziom odporności na cyberzagrożenia oraz zwiększyć poziom ochrony informacji w sektorze militarnym, promując jednocześnie wiedzę i dobre praktyki umożliwiające obywatelom lepszą ochronę ich informacji. Dostrzeżono konieczność zapewnienia bezpiecznego funkcjonowania państwa i obywateli w przestrzeni informacyjnej.

Zbudowanie odpowiedniej cyberodporności

W cyberbezpieczeństwie liczy się nie tylko umiejętność wykrywania i zwalczania pojawiających się ataków, zdolność reagowania na incydenty i przywracania funkcjonalności zainfekowanych systemów. Kluczowe znaczenie dla skuteczności działań w zakresie cyberbezpieczeństwa ma zbudowanie odpowiedniej cyberodporności (ang. *cyber-resilience*). Cyberodporność koncentruje się na tym, co dzieje się, gdy środki cyberbezpieczeństwa zawodzą, gdy systemy są zakłócane przez np. ludzki błąd albo przerwy w dostawie prądu czy pogodę. Odporność uwzględnia to, gdzie operacje są uzależnione od technologii, gdzie przechowywane są krytyczne dane oraz jaki wpływ na te obszary mogą mieć zakłócenia. Następnie obejmuje wprowadzenie środków w celu zminimalizowania wpływu tych zakłóceń. Cyberodporności, według Francesco Chiariniego, Dyrektora ds. Projektów Międzynarodowych ISSA (and. *International Security Systems Association*), nie można utożsamiać bezpośrednio z ochroną danych i systemów przed atakami. Chodzi bardziej o budowę odpowiedniej architektury cyberbezpieczeństwa i funkcji pozwalających na ochronę kluczowych zasobów. Ważne są także odpowiedni stopień dojrzałości i kultura organizacji w zakresie cyberbezpieczeństwa. Ich znaczenie – z definicji – odnosi się nie tylko do wymiaru technologii, ale i określonych idei, norm oraz zasad, które kształtują egzystencję współczesnego człowieka i pozwalają mu funkcjonować w rzeczywistości wirtualnej.

Cyberfakty i cybermity

Trwa żywa publiczna dyskusja na temat cyberbezpieczeństwa. Czasami jednak ta **dyskusja nie jest tak przemyślana, jak można by mieć nadzieję**. Punktem wyjścia analizy nie powinny być artefakty ze strategicznego myślenia zimnej wojny lub hipotetyczne scenariusze, które są ewidentnie nieprawdopodobne (teraz, gdy mamy ponad dwadzieścia pięć lat doświadczeń z cyberkonfliktami), ale **obserwowane fakty**. Kierując się obserwacjami i doświadczeniem, możemy poprawić analizę i kształtowanie polityki w tej dziedzinie.

Odstraszanie działa dobrze w domenach, dla których zostało zaprojektowane, ale jest wyjątkowo nieskuteczne w cyberprzestrzeni. Strategiczna debata na pewnym etapie koncentrowała się na paraleli między odstraszaniem nuklearnym a koncepcją cyberwojny. Przywołując widmo cyfrowej Hiroszimy, a nawet opracowując scenariusze katastrof, w których całe kraje pogrążyłyby się w chaosie fali cyberataków, myślenie strategiczne najpierw uwierzyło w pojawienie się nowej formy wojny opartej na cyfrowej broni, której potężne skutki byłyby porównywalne z wybuchem nuklearnym. Widać wyraźnie, że pojawia się nowa forma w postaci cyberodstraszania, zwłaszcza w dyskursie o zdolnościach ofensywnych i defensywnych, ale można wątpić w jej skuteczność w obliczu niektórych przeciwników mniej wrażliwych na cyfrowe formy odwetu. Co więcej, problem atrybucji pozostaje centralnym elementem mechanizmu odstraszania. Te ostatnie muszą być zastosowane do zidentyfikowanej struktury (państwa, grupy, a nawet jednostek). Model cyberodstraszania jako prostej transpozycji klasycznej teorii odstraszania nuklearnego wydaje się zatem wadliwy. Rosja nie wysłała swojej armii w celu inwazji na Europę, ale nie została odstraszona od wykorzystywania manipulacji informacją i operacji dezinformacyjnych, korupcji, przestępczości zorganizowanej, wywierania wpływu, szantażu energetycznego, szpiegostwa i zabójstw w celu promowania swoich interesów w Europie. Jest wielce prawdopodobne, że państwo Putina zbadało, jak obejść amerykańskie i natowskie środki odstraszające, i wie, jak pokierować swoimi cyberoperacjami i cyberstrategią. Nie odstraszamy naszych przeciwników w cyberprzestrzeni. Być może istnieje sposób na wskrzeszenie cyberodstraszania i innych nowych form zwalczania konfliktów w cyberprzestrzeni, ale to, co teraz robią kraje NATO, nie działa. Ukrytym celem odstraszania jest stabilność, a ponieważ nasi przeciwnicy nie chcą stabilności, jest to nieskuteczne jako strategia. Z drugiej strony nie możemy ignorować wkładu cyberdomeny w ogólne odstraszanie. Posiadanie zdolności (ofensywnych i defensywnych) w tym obszarze pomaga wzmocnić ogólną postawę obronną państwa.

Mając na uwadze, że nie istnieją międzynarodowa podstawa prawna i instytucje regulujące sferę relacji między różnymi aktora-

mi różnych szczebli w globalnej przestrzeni informacyjnej, a stawki polityczne w tradycyjnej sferze bezpieczeństwa euroatlantyckiego i skomplikowane relacje między NATO i Rosją są wysokie, warto zbadać polityczny wymiar cyberbezpieczeństwa wewnątrz Sojuszu oraz zastosowanie zasady bezpieczeństwa zbiorowego dla tej sfery z perspektywy relacji NATO – Rosja.

Aktywna obrona cyberprzestrzeni

Obecnie raptownie wzrasta ryzyko ataków i wrogiego wykorzystania systemów komputerowych, sieci i cyfrowych zasobów. Działalność aktorów państwowych i niepaństwowych coraz częściej jest skierowana przeciwko strukturom administracyjnym państwa. Może być jednak również ukierunkowana na zakłócenie ładu społecznego, prowadząc do podważenia zaufania obywateli do państwa i demokratycznego porządku. Szczególnie szkodliwe mogą być ataki hybrydowe, wywołujące chaos i niepewność, które łączą m.in. ataki i dezinformację w cyberprzestrzeni i przemoc fizyczną. Struktury aktywnej obrony cyberprzestrzeni powinny zawierać zarówno zdolności ofensywne, jak i defensywne. Ich zadaniem powinno być m.in. monitorowanie zagrożeń w cyberprzestrzeni i reagowanie na nie zarówno na terytorium Polski, jak i przy okazji działań polskich placówek dyplomatycznych oraz sił zbrojnych poza granicami kraju. Zadania te w dużej mierze są już realizowane – oraz wciąż rozwijane – w ramach utworzonego Krajowego Systemu Cyberbezpieczeństwa. W projekcie ustawy o Obronie Ojczyzny zawarto zapisy o utworzeniu Komponentu Wojsk Obrony Cyberprzestrzeni[6], które będą podlegały Dowódcy Komponentu WOC. Mają one realizować działania reaktywne, proaktywnej ochrony i aktywnej obrony w cyberprzestrzeni. Zgodnie z nim, ustawa miałaby wejść w życie 1 lipca 2022 r. Zakłada ona usankcjonowanie na poziomie ustawowym Wojsk Obrony Cyberprzestrzeni.

[6] https://legislacja.rcl.gov.pl/projekt/12353254 [dostęp: 1.12.2021].

Krajowa i międzynarodowa wspólna cyberobrona

Polem problemowym cyberbezpieczeństwa jest ocena charakteru i destrukcyjnego potencjału cyberzagrożeń, takich jak m.in. hakowanie, zorganizowana cyberprzestępczość, ekstremizm ideologiczny i polityczny w cyberprzestrzeni oraz sponsorowana przez wrogie państwa cyberagresja.

Musimy podążać w kierunku wspólnej cyberobrony – na poziomie krajowym i międzynarodowym – i wzmocnionej analizy struktury zagrożeń. Nadszedł czas na opracowanie zintegrowanego, sieciowego podejścia do współpracy w zakresie analiz obronnych i wywiadowczych w cyberprzestrzeni. Z pewnością istnieją kulturowe, organizacyjne, prawne i technologiczne bariery dla wspólnej obrony i wymiany informacji wywiadowczych między sektorem publicznym (centralnym, samorządowym) i prywatnym (biznes, infrastruktura krytyczna, organizacje non-profit). Podstawowym wyzwaniem jest brak struktur i bodźców, a istniejące relacje są w dużej mierze doraźne i punktowe. Co więcej, nie ma jasnego operacyjnego krajobrazu zagrożeń ani krajowego, strategicznego podejścia do nich. Brakuje nam wszechstronnego zrozumienia, ponieważ nie gromadzimy, nie przetwarzamy i nie udostępniamy dostępnych danych w skoordynowany i trwały sposób.

Dodatkowo cyberbezpieczeństwo krajowe jest utrudnione przez ograniczone zasoby (utalentowanych informatyków, finansowanie) i – ciągle jeszcze obecne – podejście „silosowe" do zarządzania kryzysowego w obliczu rosnących zagrożeń.

Powinniśmy być w stanie określić priorytety w narodowym krajobrazie cyberbezpieczeństwa. Podział między sektorem prywatnym i publicznym jest często punktowy i oparty na incydentach, z wyjątkiem ograniczonej, dobrowolnej koordynacji między sektorowym zarządzaniem ryzykiem a podmiotami. Ponadto klauzule umowne uniemożliwiają wymianę niektórych informacji między sektorem publicznym i prywatnym. A te nowe zagrożenia różnią się od historycznych zagrożeń z przeszłości wobec naszej ojczyzny i są szczególnie pilne i wyjątkowe w porównaniu z wcześniejszymi wyzwaniami,

przed którymi stoi dziś Polska. Nasz kraj i jego mieszkańcy, przedsiębiorcy i rząd są już atakowani, ale są źle przygotowani do walki z nieuchronnymi obecnymi i przyszłymi atakami, i tak było przez większą część ostatniej dekady.

Traktowanie cyberzagrożeń jako czegoś mniej ważnego błędnie diagnozuje naturę wyzwania, przed którym stoimy, i błędnie umiejscawia potrzebę stworzenia systemu, który odpowiednio zareagowałby we właściwym czasie. Te operacje w cyberprzestrzeni, dokonywane przez wrogie podmioty państwowe lub grupy przestępcze, charakteryzują się trwałym rozprzestrzenianiem się sieci wrogich. A reakcje zarządzania w sytuacjach kryzysowych są niewystarczające. **Wymagana jest trwała, skoordynowana reakcja systemowa**. Musimy określić cele, które mają nas poprowadzić w kierunku strategicznej współpracy w zakresie obrony i wzmocnienia podejścia wywiadu o zagrożeniach między rządem, samorządem i sektorem prywatnym. Bierzemy pod uwagę kwestie kulturowe, organizacyjne, prawne i technologiczne. Nie znamy wszystkich odpowiedzi, a wiele decyzji budżetowych i operacyjnych należy pozostawić w gestii liderów i decydentów posiadających wiedzę na temat środowiska. Dalsza analiza operacjonalizacji[7] informacji o cyberzagrożeniach przez poszczególne instytucje i organizacje oraz wyzwań współpracy na poziomie taktycznym jest konieczna, biorąc pod uwagę złożoność zagrożeń i środowiska operacyjnego.

W 2016 r., podczas Szczytu NATO w Warszawie, w ramach Zobowiązania w zakresie Cyberobrony (ang. *Cyber Defence Pledge*), państwa członkowskie NATO potwierdziły swoje zobowiązania wynikające z art. 3 Traktatu Waszyngtońskiego, a więc tworzenia własnych skutecznych zdolności obronnych, w tym w zakresie cyberobrony. Podkreślono również konieczność poprawy świadomości w zakresie cyberzagrożeń, a w szczególności ich oceny i wymiany informacji. W tym kontekście istnieje konieczność stworzenia spójnej i wszechstronnej strategii cyberobrony państwa, obejmującej wszystkie sek-

[7] Operacjonalizacja zmiennych teoretycznych, założeń itp. to nadanie im określonego sensu empirycznego, czyli ich sprawdzenie w praktycznych procesach.

tory, ogniwa militarne i pozamilitarne, a także ustanawiającej jeden organ decyzyjny, władny uruchomić wszystkie zasoby cyberobrony państwa w sytuacji najpoważniejszych zagrożeń.

Strategiczne cele cyberbezpieczeństwa państwa

Przy budowie zdolności w zakresie cyberbezpieczeństwa Polska i państwa sojusznicze muszą mierzyć się z wieloma wyzwaniami, zwłaszcza jeżeli chodzi o zapewnienie, aby zdolności te zawsze nadążały za zachodzącymi zmianami. Priorytetowymi celami strategicznymi cyberpezpieczeństwa państwa polskiego powinny być: a) utrwalenie odporności instytucji demokratycznych i instytucji spoza władzy wykonawczej, w tym integralności wyborów, b) odbudowanie i lepsze reagowanie w celu wzmocnienia ochrony cywilnych sieci rządowych, c) poprawa cyberbezpieczeństwa w łańcuchu dostaw i badanie nowych technologii w celu zwiększenia odporności, d) przygotowanie do strategicznych, horyzontalnych wyzwań cywilizacji cyfrowej i pojawiających się nowych i przełomowych technologii (*Emerging Dissruptive Technologies – EDT*[8]), takich jak np. przejście na algorytmy szyfrowania postkwantowego oraz e) ochrona tożsamości elektronicznej i budowanie zaufania do cyfrowych usług publicznych.

Odporność instytucji demokratycznych, uczciwych i wolnych wyborów jest znakiem rozpoznawczym polskiej demokracji. Zaufanie do wartości głosu obywateli zależy przede wszystkim od bezpieczeństwa i odporności infrastruktury, która umożliwia proces wyborczy. Najwyższym priorytetem jest zaangażowanie we współpracę z instytucjami znajdującymi się na pierwszej linii wyborów – Państwową Komisją Wyborczą i jej organem wykonawczym Krajowym Biurem Wyborczym, władzami lokalnymi[9], urzędnikami wyborczymi – w celu zarządzania ryzykiem krajowej infrastruktury wyborczej przed nowymi i ewoluującymi zagrożeniami.

---

[8] W lutym 2021 r. ministrowie obrony NATO zatwierdzili strategię dotyczącą nowych i przełomowych technologii (*Emerging Dissruptive Technologies* – EDT).

[9] W procedurze wyborczej na organach gminy spoczywa wiele obowiązków. Wójt, burmistrz, prezydent miasta odpowiada za techniczno-organizacyjne przygotowanie lokali wyborczych, ma też inne zadania.

Politolog Joseph S. Nye Jr. twierdzi, że „w klasycznym dualizmie wojny i pokoju cyberataki zwykle wpadają w «szarą strefę»”[10]. Rozwój rynków cyfrowych i zsieciowanych społeczeństw idzie w parze z wyzwaniami w zakresie bezpieczeństwa i obrony. Rzeczywiście, innowacje cyfrowe są coraz bardziej narażone na napięcia i rywalizacje geopolityczne. Aspekty te są szczególnie widoczne w nadchodzącym wyścigu o przełomy technologiczne między rządami i biznesem – cyfrowym wyścigu zbrojeń.

Nowe i przełomowe technologie (EDT) są w coraz większym stopniu wykorzystywane zarówno przez podmioty państwowe, jak i niepaństwowe w szarej strefie, kwestionując istniejące normy, prawa i instytucje, które zazwyczaj działają poniżej progu konfliktu zbrojnego. Coraz lepiej rozumie się, że w sferze cyfrowej coraz częściej rozgrywa się konkurencja strategiczna.

Pomimo tego, że w cyfrowym repozytorium – cyberprzestrzeni – znajduje się niemal wszystko, od danych osobowych po infrastrukturę krytyczną, rządy nie potrafiły jej bronić, „żaden kraj ani organizacja nie były *cyber ready*”[11] – „gotowe do cyberbezpieczeństwa”, co potwierdziło potrzebę wspólnej, globalnej współpracy w dziedzinie cyberbezpieczeństwa.

Chociaż ustalono, że prawo międzynarodowe ma zastosowanie do cyberprzestrzeni, państwa nadal nie zgadzają się, jakie ma ono zastosowanie w przypadkach takich jak samoobrona, przyjmowanie środków zaradczych i sytuacje objęte międzynarodowym prawem humanitarnym[12]. Podejście UE opiera się w takim samym stopniu na środkach cyberdyplomacji, jak i na cyberobronie i odstraszaniu. UE i jej państwa członkowskie uznają znaczenie inwestowania w solidną obronę na szczeblu krajowym i w całej Europie, aby chronić aktywa i zniechęcać potencjalnych sprawców. Jednocześnie traktują

---

[10] J.S. Nye Jr., *Deterrence and Dissuasion in Cyberspace*, International Security, Vol. 41, No. 3 (Winter 2016/17), s. 44-71.

[11] *Cyber Readiness Index 2.0. A Plan for Cyber Readiness: a Baseline and an Index*, Potomac Institute, 2015.

[12] F. Delerue, J. Kulesza, P. Pawlak, *The Application of International Law in Cyberspace: Is There a European Way?*, April 2019.

priorytetowo współpracę międzynarodową w zakresie norm w domenie „cyber", odporności i odpowiedzialnego zachowania. Takie podejście jest zgodne z zasadą: łańcuch jest tak mocny, jak jego najsłabsze ogniwo.

Polska – posiadając niemały potencjał w dziedzinie cyberbezpieczeństwa – powinna budować i rozwijać z sojusznikami[13] odporność instytucji zdolnych do reagowania na cyberzagrożenia i wychodzenia z nich, zapewnić zobowiązania do utrzymania otwartej, wolnej i bezpiecznej cyberprzestrzeni, promować wzrost sprzyjający włączeniu społecznego i zrównoważonego rozwoju infrastruktury cyfrowej, poprawę rynków cyfrowych i zapewnienie bezpiecznej gospodarki internetowej; stworzyć strategię cyberobrony w celu ochrony sieci wojskowych, zasobów i instytucji obronnych.

[13] *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building*, European Commission, 2018.

Bezpieczeństwo informacyjne Polski wobec rozwoju technologii

dr Bolesław Piasecki

Bezpieczeństwo informacyjne jako kategoria bezpieczeństwa jest szeroko opisywane w literaturze przedmiotu. Nie brakuje tekstów przybliżających definicyjne ujęcia, różnice w doktrynach czy skupiających się na generalnym porządku tych rzeczy. Truizmem jest twierdzenie, że bezpieczeństwo informacyjne jest coraz ważniejsze, a w dobie rosnącej rywalizacji w Europie i na świecie duża część rywalizacji odbywa się w sferze informacyjnej. Współczesny człowiek jest w niej wprost zanurzony, choć nie w taki sposób, jak miało to miejsce w przeszłości. Celem niniejszego tekstu jest próba nie tyle teoretycznego opisu rzeczywistości, co spojrzenia na praktyczne aspekty funkcjonowania środowiska informacyjnego, zwłaszcza wobec rozwoju nowych technologii i tego jak człowiek, społeczeństwo czy państwo dostosowuje się do niej. Refleksja ta ma charakter bardziej ogólny niż szczegółowy. Drugi cel to próba odpowiedzi na pytanie, co Polska powinna z tym zrobić, jak odnieść się do rzeczywistości, która w sposób pozornie niewinny zmienia się nie do poznania. Próbą taką jest przedstawiona koncepcja powołania pełnomocnika Prezesa Pady Ministrów ds. przeciwdziałania dezinformacji wraz z jego zadaniami i obszarem zainteresowania.

Bezpieczeństwo informacyjne można rozumieć jako stan (lub zdolność państwa do jego zapewnienia) płynnego oraz auten-

tycznego, tj. zgodnego z założeniami, funkcjonowania infosfery społecznej i państwowej. Dla niektórych obszarów działalności państwa atrybutem autentyczności będzie niejawność informacji, dla innych np. wolność słowa. Zagrożeniem wobec tego będzie działanie niszczące ten stan poprzez na przykład manipulacje, dezinformacje, ingerencje, tajny wpływ, przeciążenie informacyjne itd. Co ważne, bezpieczeństwo informacyjne państwa ulega istotnym przemianom, gdyż obszar ataku na sferę informacyjną niebywale się poszerza. W zasadzie z roku na rok tworzone są nowe miejsca, gdzie informacja ma kluczowe znaczenie, a zarówno państwo, jak i obywatele muszą mierzyć się z nowymi zagrożeniami. W tym sensie pole starcia ulega bezprecedensowemu poszerzeniu, walka jest permanentna i coraz szybsza. Wszystko to umożliwia technologia, która może być pozornie neutralna lub wręcz pożyteczna, a realnie szkodzić bezpieczeństwu informacyjnemu jednostek, społeczeństwa czy państwa. W tym aspekcie podmioty państwowe są zazwyczaj opóźnione, rozpoznanie istoty zagrożenia ułomne, a reakcje niedokładne. Dotyczy to zwłaszcza obrony bezpieczeństwa informacyjnego. W istocie ostatecznym celem ataku jest umysł obywatela. To dzięki atakowi na sferę poznawczą milionów można wpływać na zachowania społeczne czy politykę państwa demokratycznego. Nie jest to nic nowego, niemniej jednak ewolucja, czy wręcz rewolucja informacyjna, sprawia, że wadliwa natura i poznanie człowieka są pod ciągłym obstrzałem informacyjnym. Co więcej, wiele z tych ataków na sferę informacyjną choć ma charakter masowy, to wciąż jest dzięki technologii dobrze dopasowanych do specyfiki danego obywatela. Dla państwa stanowi to potężne wyzwanie. Konsumpcja i adaptacja nowoczesnych technologii zmieniających życie społeczności ludzkich odbywa się bez żadnych „badań klinicznych", to działanie na żywym i wciąż słabo znanym organizmie społecznym. Na naszych oczach zmienia się cywilizacyjny wzorzec podejścia do informacji, jest ona przeżywana, nie zaś konsumowana. Wykorzystywane są różne ludzkie podatności i ułomności, w skali znacznie szerszej i lepiej sprofilowanej. Sami tworzymy jeszcze większą powierzchnię ataku, sami wystawiamy społeczeństwo i państwo na ataki informacyjne, a technologia w dużej mierze utrudnia, a nie

ułatwia zadanie zapewniania płynnego i autentycznego funkcjonowania infosfery. Trzeba przy tym jasno zaznaczyć, że świat manipulacji, dezinformacji i zwodzenia milionów nie jest nowy. Cel zakłócenia bezpieczeństwa informacyjnego adwersarza, wpływ na jego percepcję i działania od wieków jest jednym z podstawowych w kontekście władzy, niezależnie od tego, czy mówimy o relacjach międzyludzkich, czy strategicznych starciach cywilizacji.

Można stwierdzić, że ujęcie to jest w pewien sposób ponadczasowe. Od zawsze ludzie szukali okazji do zdobycia władzy podstępem, oszustwem czy manipulacją. Nie ma w tym nic dziwnego, a sfera informacyjna od sceny w Edenie jest polem nieustannej bitwy. Bitwy odbywającej się wewnątrz człowieka czy na polu społecznym. Nie byłoby jednak prawdą podsumowanie obecnego stanu stwierdzeniem, że to wszystko już było, a to, co obecnie obserwujemy, jest jedynie większym nasileniem lub wzmocnioną percepcją. Nastąpiły bowiem jakościowe zmiany w otoczeniu człowieka, które powodują, że choć natura pozostaje niezmienna, to narzędzia walki informacyjnej i nastawania na bezpieczeństwo informacyjne ulegały znacznej zmianie. Trudno rozstrzygać, na ile jest to zmiana ewolucyjna, jest natomiast pewne, że jej skutki są rewolucyjne dla zasad, w ramach, których funkcjonuje ludzkie poznanie. Nowe technologie zmieniły zasady walki, zagrożenia dla bezpieczeństwa informacyjnego ewoluowały. Zmiana ta odbywa się na różnych poziomach i z pewnością zaczyna się od jednostki. Dzisiejszy obywatel jest wprost zasypywany wiadomościami i danymi, których nie jest w stanie analizować, ani na dobrą sprawę ich nie potrzebuje. Jest on wystawiony na działanie informacyjne przez większą część doby, a dobór kanałów komunikacji jest tylko pozorny. W rzeczywistości chcąc funkcjonować w społeczeństwie informacyjnym, obywatel jest zmuszony wykorzystywać szereg destrukcyjnych technologii. Dla znaczącej większości zwłaszcza ludzi młodych nie jest to świadomy wybór, a domyślna opcja wymuszana przez realia życia społecznego. Jest to ceną za uczestnictwo w życiu społecznym. Sprawia to, że potencjalne pole ataku informacyjnego i zagrożenia dla bezpieczeństwa ulegało bezprecedensowemu poszerzeniu. Każdy może być nadawcą masowym i odbiorcą. Dodatkowym,

a być może fundamentalnym czynnikiem będącym swoistym dopalaczem jest technologia mediów społecznościowych, które są na granicy stworzenia zupełnie cyfrowej rzeczywistości. Co ważne, nie jest to rzeczywistość alternatywna, w tym sensie nie ma już pomiędzy nimi rozdźwięku. Jedna z drugą się przenikają w sposób trudny do rozdzielenia, a życie społeczne czy polityczne jest podobnie zanurzone w tych dwóch obszarach. To rewers i awers tej samej monety. Wystarczy spojrzeć, jak wiele z konsumowanych przez społeczeństwo szeroko rozumianych informacji i relacji odbywa się za pomocą Internetu. Nie jest to jedynie medium, a obszar formujący zarówno relacje, jak i informacje. Dzieje się tak, ponieważ użytkownik funkcjonujący w tym świecie zostawia po sobie swój cyfrowy ślad mówiący bardzo wiele o nim i jego osobowości. Wszystko to jest w sposób ciągły analizowane, przetwarzane i wykorzystywane niejako przeciwko niemu, zachęcając do jeszcze większej interakcji. Ma to bardzo istotne konsekwencje społeczne związane z uzależnieniami, osamotnieniem, radykalizacją, znieczulicą i innymi dość powszechnie badanymi zjawiskami. Sprawia to, że jedno z najważniejszych zagrożeń bezpieczeństwa informacyjnego Polski jest faktycznie immanentną cechą modelu biznesowego wielkich korporacji technologicznych. Angielska fraza *disruptive technologies* tłumaczona jako technologie dysruptywne czy też zakłócające, zmieniające bieg i zasady ruchu w całym rynku, miała mieć pozytywne konotacje. Przeciwstawiano to tradycyjnemu modelowi, pewnemu zastojowi. Domena założyciela Facebooka „ruszaj się szybko, psuj rzeczy" także miała być pozytywna. Okazało się po czasie, że podstawowym pytaniem jest to, co jest zakłócane przez technologie dysruptywne. Otóż nie rynek, a społeczeństwo, rodziny, dobrostan jednostek.

Z punktu widzenia bezpieczeństwa państwa odbywa się tutaj jeszcze jeden bardzo istotny proces. Wszystko to w skali mikro systemowo przekłada się na skalę marko. Podmioty zewnętrzne posiadają bezprecedensowy wgląd w polskie społeczeństwo, w czasie zbliżonym do rzeczywistego pozyskują wiedzę, której żaden rząd ani pracownia badawcza nie posiadają. Wynika to z faktu, że ludzie są szczersi z wyszukiwarką Google niż z własnymi przyjaciółmi. To

oferuje prawdziwy wgląd, ale także możliwości wpływania na procesy społeczne i postawy Polaków. Te same narzędzia, które mogą być wykorzystywane do niwelowania nierówności, w rzeczywistości powiększają asymetrie informacji. Ten sam proces dotyczył innych wynalazków, takich jak telewizja czy radio. Z tego powodu zagrożenia dla bezpieczeństwa państwa związane ze sferą informacyjną, takie jak operacje wpływu, niszczenie zaufania do państwa, poczucia wspólnoty, kapitału społecznego, wzmacnianie znieczulicy, kreowanie skrajnego indywidualizmu połączonego z całkowitą relatywizacją dobra i zła, mogą być skutecznie rozsiewane za pomocą nowych technologii. Jeżeli zostaniemy na etapie obserwacji sfery informacyjnej przez media czy tradycyjne badania społeczne, to procesów tych nie zauważymy albo zrobimy to zbyt późno, zbyt pobieżnie. Jak pokazała agresja organizowana przez reżim Łukaszenki, polskie społeczeństwo i media są zupełnie niegotowe na sytuację kryzysową. Sytuacja na granicy jest naprawdę oczywista, a mimo to powszechne są opinie o tym, że granica to tylko linia na mapie. Tego typu uwagi padać mogą na podatny grunt części społeczeństwa właśnie dlatego, że w strategicznym zakresie nie ma prowadzonej walki z dezinformacją. Trzeba tu podkreślić, że walka ta nie może odbywać się za pomocą prostowania tzw. *fake newsów*, to znacznie poważniejsze i głębsze procesy, które muszą być rozpatrywane w kontekście strategicznym.

Wszystko to zdaje się sugerować, że państwo musi walczyć o swoją suwerenność informacyjną, o zdolność do obrony przestrzeni informacyjnej Polaków przed niszczącym wpływem innych aktorów. Nie sposób tutaj nie zauważyć, że polem walki jest przede wszystkim obszar nowych technologii. Obszar, na którym państwo nie jest gospodarzem, obszar, który się szybko zmienia, i w końcu obszar, który wciąż rozumiemy niewystarczająco dobrze.

Niniejszy tekst nie ma ambicji być tylko częściowym opisem rzeczywistości, ale także ma przedstawiać konkretne działania strategiczne, które można podjąć w celu zwiększenia bezpieczeństwa Polski. Mimo licznych diagnoz i imponującej pracy ośrodków analitycznych, brakuje praktycznego przełożenia zgromadzonej wiedzy i doświadczenia na praktykę funkcjonowania państwa. Było wiele

inicjatyw zarówno sektorowych, jak i próby koordynacji działań różnych resortów w obszarze informacyjnym. Mimo powszechnie identyfikowanej potrzeby stworzenia jednolitej komunikacji strategicznej czy walki z dezinformacją, podejmowane działania nigdy na szerszą skalę nie okazały się skuteczne. Funkcjonują jedynie wąskie, resortowe komórki, próbujące mierzyć się z przedmiotową tematyką. Są one w kontekście strategicznym skazane na porażkę, co wynika nie z braku woli czy kompetencji, ale z rozległości zagadnienia. Bez skutecznej koordynacji i pracowania w szerokim spektrum zagadnień nie ma możliwości odniesienia sukcesu w walce informacyjnej. Wydaje się to jeszcze trudniejsze, gdy podsumujemy zakres działania adwersarzy oraz wielość kierunków, z których atakują. To zaś wymaga pewnej specjalizacji oraz dostosowania narzędzi do specyfiki działania drugiej strony.

Działanie mające na celu odpowiedzenie na wyzwania zarysowane w niniejszym tekście bez wątpienia musi wyjść ze strony rządu. System ten należy budować z jednolitym zamysłem i od razu jako konkretne tryby w maszynie informacyjnej państwa. Oznacza to, że rozpocząć należy od koordynacji centralnej i stworzenia modelu pracy. Najmniejszym możliwym kalibrem takiego działania jest pełnomocnik Prezesa Rady Ministrów ds. przeciwdziałania dezinformacji. Nie powinniśmy mówić tylko o zwalczaniu dezinformacji, to działanie reaktywne, a w tak szybko fungującym świecie szybkość dostarczenia informacji jest kluczowa. W związku z tym strona broniąca się reaktywnie, jedynie demaskująca kłamstwa, musi przegrać. Przeciwdziałanie zakłada także działania proaktywne, zwalczanie zagrożenia, nim się pojawi, przygotowywanie systemu na atak. To bardzo ważny element całości systemy bezpieczeństwa, bez którego trudno mówić o sukcesie na polu informacyjnym. Osoba ta powinna być co najmniej w randze podsekretarza stanu Kancelarii Prezesa Rady Ministrów. Drugim ważnym elementem jest pełne poświęcenie obowiązkom pełnomocnika. Tematyka bezpieczeństwa informacyjnego jest tak rozległa, że w zasadzie łączenie jej z jakąkolwiek inną odpowiedzialną funkcją jest z gruntu bardzo trudne i nierekomendowane, jeżeli celem jest skuteczna obrona Polski, jej interesu i oby-

wateli przed zagrożeniami informacyjnymi. Istnieje pokusa, aby taką rolę sprowadzić do funkcji rzecznika prasowego czy też działań Centrum Informacyjnego Rządu. W rzeczywistości mówimy tutaj o dużo poważniejszym wyzwaniu, które wykracza poza bieżącą funkcję informacyjną, a obejmuje swoim działaniem bardzo szeroki wachlarz strategicznej aktywności państwa. Nie chodzi bowiem jedynie o rolę komunikacyjną, a o prawdziwe działanie w dwóch obszarach: pierwszy dotyczy agregacji wiedzy, drugi zaś oddziaływania sieciowego.

Pierwszym zadaniem pełnomocnika powinno być stworzenie centrum agregacji wiedzy w obszarze infosfery. Nie chodzi tutaj o centralizację całości władzy w tym obszarze, jest to niemożliwe i przeciwskuteczne. Przy takiej wielości komunikacji, specyfiki i przy ważnym aspekcie *stricte* politycznym pełnomocnik nie może być główną postacią komunikacyjną rządu. Chodzi o stworzenie jednego miejsca, które zbierałoby w jeden spójny obszar dane dotyczące środowiska informacyjnego z bardzo różnych obszarów działalności politycznej, społecznej, kulturowej czy historycznej. W tym ujęciu pełnomocnik ma za zadanie stworzenie jednolitego obrazu świadomości sytuacyjnej na podstawie licznych danych płynących z bardzo różnych obszarów informacyjnych, od różnych instytucji. Dzięki temu w jednym miejscu zbiegać się będą nie tylko informacje, ale i perspektywy działania, które często są niezauważane. Pozwoli to na całościowe działania analityczne i możliwie skuteczną odpowiedź na coraz trudniejsze pytanie: jak jest? Zestaw informacji koniecznych dla odpowiedzi na to pytanie jest dostępny, państwo polskie posiada wielu ludzi, ekspertów w wąskich dziedzinach, osoby doświadczone, od lat pracujące na poszczególnych kierunkach. Ich wiedza i doświadczenie wielokrotnie nie są wykorzystywane, nie ma możliwości przebicia się na wyższe szczeble i bycia elementem szerszej analizy strategicznej. Wiele z informacji, które produkują państwo i ludzie na rzecz jego pracujący, trafia w próżnię. Nigdy nie są analizowane całościowo, tylko w najlepszym razie sektorowo. To sprawia, że nie ma jednego miejsca, które agregowałoby wiedzę, tworzyło świadomość sytuacyjną infosfery i miało na względzie bardzo różne procesy. W sposób oczywisty nie jest możliwe samodzielne

obsłużenie merytoryczne takiej głębi i wielości obszarów przez jedną instytucję, zresztą państwo już posiada wiele takich zdolności, tylko nie są one koordynowane. Nie chodzi zatem o tworzenie rozdętych struktur, a raczej o usprawnienie obecnego systemu, który już w wielu obszarach funkcjonuje.

Drugim zadaniem pełnomocnika do spraw przeciwdziałania dezinformacji powinno być przygotowywanie analiz, prognoz, rekomendacji oraz strategii w zakresie polityki informacyjnej państwa. Niemniej jednak w przeciwieństwie do punktu pierwszego, czyli centralizacji i agregacji wiedzy, oddziaływanie informacyjne powinno być rozproszone. Oznacza, to że pełnomocnik ma za zadanie gromadzić, analizować i udostępniać wiedzę, którą następnie odpowiednie organy mogą wykorzystywać zgodnie z właściwościami swoich kompetencji. Nie chodzi zatem o centralizację prowadzenia polityki informacyjnej i odpowiedzi na zagrożenia w domenie bezpieczeństwa informacyjnego. Takie działanie nie będzie skuteczne, frontów jest zbyt wiele, zbyt różne są specyfiki i okoliczności. Zadanie to sprowadza się raczej to funkcji rekomendacyjnej. Tak więc pełnomocnik powinien opracowywać wytyczne i strategie, które następnie implementowane będą w poszczególnych działach administracji i nie tylko. Wiele tego typu instytucji, także tych finansowanych przez rząd, pracuje w oparciu o plany roczne. W strategie działania poszczególnych instytucji powinny być wpisane elementy będące operacjonalizacją wytycznych pełnomocnika. Tak aby zarówno jednostki rządowe, jak i inne mogły realizować szerszą politykę informacyjną rządu w swoich działaniach. Trzeba podkreślić, że nie chodzi tutaj o bieżące działania polityczne, a raczej o długofalowe oparte o identyfikację trendów korzystnych dla interesów narodowych i mitygowanie zidentyfikowanych zagrożeń. Aspekt analizy nie tylko polskiego, ale międzynarodowego środowiska informacyjnego wydaje się tutaj absolutnie kluczowy.

W celu realizacji tych zadań istnieć powinien niewielki interdyscyplinarny zespół analityczny, który zajmowałby się opracowywaniem i tzw. analizą kroczącą środowiska informacyjnego Polski zarówno w ujęciu wewnętrznym, jak i zagranicznym. Dzięki temu Polska mogłaby przewidywać, wyprzedzać, a kiedy trzeba sprawnie

reagować nie tylko punktowo jako poszczególne instytucje, ale szerzej jako jeden organizm. W toku pracy analitycznej można bowiem identyfikować trendy narracyjne atakujące polskie interesy, odnotowywać operacje informacyjne wymierzone w Polskę jeszcze na etapie przygotowania i przeciwdziałać im systemowo, długofalowo utrudniając przeciwnikowi wejście w naszą infosferę. Oczywistym jest, co pokazały w szczególności ostatnie lata, że międzynarodowa przestrzeń informacyjna bywa dla Polski niekorzystna za sprawą tych samych aktorów. Propagują oni linie narracyjne godzące w polskie interesy, ale linie te są stosunkowo łatwe do identyfikacji i mogą być ograniczane za pomocą działań strategicznych. Problem jest taki, że państwo polskie zasadniczo nie ma wyraźnej strategii informacyjnej, nie jest jasne, co chce osiągnąć, jakimi środkami i w jaki sposób. Należy przy tym oddać, że wielokrotnie okazywało się sprawcze w kryzysowych sytuacjach komunikacyjnych w obszarze międzynarodowym, ale i tu długofalowość i analiza wiele by pomogły. Przygotowanie takiego ogólnego dokumentu w postaci wytycznych pozwoliłoby na synchronizację polskiej polityki informacyjnej, przy zachowaniu zasady pomocniczości, gdzie implementacja polskiej perspektywy będzie dokonywana na różnych polach przez osoby i instytucje specjalizujące się w danej tematyce. To właśnie różnorodność metod oddziaływania i pól analizy jest tutaj kluczowa. Błędem byłoby bowiem sprowadzenie dbania o bezpieczeństwo informacyjne do prasówki, monitoringu mediów i reaktywnego działania na procesy widoczne w telewizorze. Przeciwnie, to musi być stała i dojrzała analiza, nieco oderwana od bieżących wydarzeń, które często przysłaniają istotę sprawy. To ona pozwoli na prowadzenie działań osłonowych wobec planowanych działań. Kluczowe jest całościowe spojrzenie na tego typu funkcje, nie chodzi bowiem tylko o czysto polityczną warstwę bezpieczeństwa informacyjnego, ale także o inne obszary pokrewne jak polityka historyczna, kultura czy gospodarka. Wszystko to stanowi mozaikę informacyjną, musi więc być całościowo analizowane zarówno pod kątem tego, jak Polska jest atakowana, jak i tego, jak powinna się bronić, wyprzedzać, narzucać swoje siatki pojęciowe, ramy myślenia. Ważny byłby tu także wspomniany już aspekt interdyscyplinarny, co oznacza

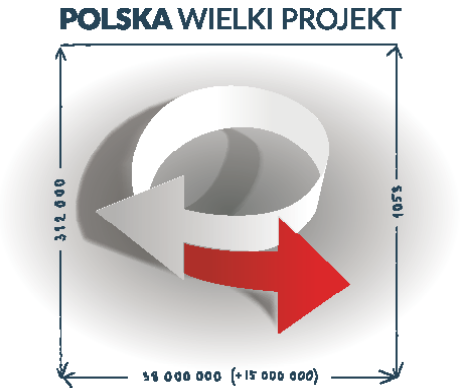
nie tylko różnorodność wykształcenia i doświadczenia osób pracujących w zespole, ale także stosowanie nowoczesnych technologii pozwalających na wgląd we współczesną sferę informacyjną.

Oczywistym jest, że zarówno pełnomocnik, jak i zespół analityczny pracujący na jego rzecz, w celu koordynacji muszą blisko współpracować i korzystać z danych zbieranych przez inne instytucje. Można zaryzykować tezę, że to jeden z najważniejszych czynników determinujących sukces przeciwdziałania dezinformacji. Dlatego też w każdym ministerstwie i w wybranych spółkach Skarbu Państwa oraz podmiotach finansowanych z budżetu powinien być ktoś na wzór „oficera łącznikowego". Ktoś, kto jest w stałym kontakcie z pełnomocnikiem, zna metody i tryb pracy, potrafi szybko i na odpowiednim poziomie politycznym zareagować, gdy czas jest kluczowym czynnikiem. Jest oczywiste, że w najbliższym gronie współpracy powinny być kluczowe elementy władzy wykonawczej. Ministerstwa, służby specjalne to najbliższy krąg współpracy, których praca powinna odbywać się w trybie niejawnym. Jest to ważne, bowiem zagrożenie dezinformacją (a więc świadomym i celowym działaniem) jest największe ze strony podmiotów państwowych, które używają do tego celu właśnie służb specjalnych. Natomiast tego typu praca nie może być dominująca. Konieczne jest także lepsze usieciowienie innych jednostek, w tym jednostek badawczych, i wyjście poza obszar *stricte* rządowy. Dobre usieciowienie będzie w tym przypadku kluczowe i musi z pewnością dotyczyć także relacji z mediami czy organizacjami pozarządowymi. Celem jest zatem wydobycie potencjału z zasobów, które już istnieją, nie zaś tworzenie dużych i kosztowych struktur. Wyjątkiem od tego jest kwestia informacyjnych technologii obronnych, czyli wykorzystania rozwoju technologii do kontroli i obrony infosfery, wolności słowa, spoistości społecznej. Nie wchodząc w szczegóły, można jedynie zasygnalizować, że Polska powinna rozwijać takie technologie. Są bowiem mechanizmy, które mogą pozwolić na skuteczne zwalczenie szeregu zagrożeń, choć i one wiążą się z pewnymi dylematami wkraczającymi wręcz w obszar filozofii polityki. Czymże bowiem innym jest dziś wykorzystywana metoda faktycznej cezury za pomocą algorytmów sieci społecznościowych

jak nie oddaniem pozornie obiektywnemu algorytmowi częściowej władzy nad jedną z największych zdobyczy cywilizacji zachodniej, jaką jest wolność słowa?

Należy podkreślić, że obowiązki i zadania powyżej opisane nie mogą być realizowane „przy okazji". Nie powinny być elementem bieżącego politycznego działania, a raczej współpracować ściślej z nieistniejącą jeszcze w Polsce strukturą odpowiedzialną za komunikację strategiczną. Powołanie takiego systemu odpowiedzialnego za komunikację strategiczną także jest konieczne i wymaga oddzielnej refleksji na ten temat. Jasne jest natomiast, że funkcje Centrum Informacyjnego Rządu, przeciwdziałania dezinformacji oraz komunikacji strategicznej są odrębne względem siebie, ale muszą ściśle ze sobą współpracować.

Na koniec należy podkreślić, że opisywane wyzwania są zupełnie niezależne od naszej percepcji. To walec, który jedzie, który zmienia sposób funkcjonowania ludzi, wspólnot, państw. Nie jest to rzecz, wobec której można nie zajmować stanowiska. Zespół kompleksowych zjawisk, o którym mowa, będzie miał znaczący wpływ na suwerenność państwa, zdolność realizacji interesów i obrony wspólnoty narodowej. Polska nie może pozwolić sobie na bycie biernym przedmiotem tych procesów, bo – jak wiele razy nasza historia pokazywała – jest to śmiertelnie niebezpieczne.



Fundacja Polska Wielki Projekt
www.polskawielkiprojekt.pl
Warszawa 2021

Redakcja:
Małgorzata Terlikowska

Opracowanie graficzne:
Magda Pyrgies / Wschód Studio