Mieszko Oziębłowski

"Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego", Tomasz R. Aleksandrowicz, Warszawa 2014 : [recenzja]

Ante Portas. Studia nad bezpieczeństwem nr 1 (3), 143-149

2014

mgr Mieszko Oziębłowski
Wyższa Szkoła Biznesu i Przedsiębiorczości
W Ostrowcu Świętokrzyskim

RECENZJA: TOMASZ R. ALEKSANDROWICZ, *ŚWIAT W SIECI. PAŃSTWA, SPOŁECZEŃSTWA, LUDZIE. W POSZUKIWANIU NOWEGO PARADYGMATU BEZPIECZEŃSTWA NARODOWEGO,* WARSZAWA 2014, SS. 257.

Problematyka nauk o bezpieczeństwie była i jest przedmiotem zainteresowania specjalistów, jednak w ostatnim czasie daje się zauważyć poszerzanie kwestionariusza badawczego nieustannie poddawanego empirycznej weryfikacji w oparciu o nowe fakty i zmiany w otaczającej nas rzeczywistości, zwłaszcza związanej z cyberprzestrzenią i szeroko pojętym dostępem do wiedzy i informacji.

Znaczące konsekwencje tych zmian w kontekście bezpieczeństwa tak jednostki, jak i całych systemów są tym bardziej istotne, że obecnie zagrożenia podlegają dynamicznym zmianom nieustannie przybierając różne formy i wektory, co niejako wywołuje sprzężenie zwrotne w postaci prób ich antycypacji, zwłaszcza że w przypadku bezpieczeństwa sieciowego jest to szczególnie trudne a jednocześnie rudymentarne.

Stąd też z uwagą odnotować należy pojawienie się na rynku wydawniczym książki, której dyskurs dotyka znaczenia rozpoznawania zagrożeń w nowoczesnym społeczeństwie ery informacyjnej.

W wielopłaszczyznowym dyskursie Tomasz Aleksandrowicz omawia znaczenie informacji w sieciowym uniwersum, szczególną uwagę przykładając do ich specyfiki oraz nowego paradygmatu rozumianego jako reakcja na fundamentalne zmiany podmiotu i przedmiotu bezpieczeństwa.

Cała książka zawiera osiem rozdziałów poświęconych różnym aspektom sieciowego społeczeństwa i władzy oraz konsekwencji zmian cywilizacyjnych, ze szczególnym naciskiem na nowe ujęcie problematyki bezpieczeństwa. Postulowane przez autora odejście od państwocentryczności, zakłada również nową perspektywę dla aktorów stosunków międzynarodowych, obsadzając ich w roli sieciowych podmiotów, w równie sieciowym środowisku.

Aleksandrowicz ukazuje konsekwencje końca świata dwubiegunowego, choć cytując niejako przy okazji Brzezińskiego, podkreśla atrakcyjność kulturową Ameryki i produktów szeroko rozumianej amerykańskiej kultury masowej[1], nie wskazuje przy tym w żadnym razie na procesy dyfuzji w tyglu multikulturowych synkretyzmów.

Omawiając powstanie społeczeństwa informacyjnego oraz rozwój środowisk sieciowych autor odwołuje się do Manuela Castellsa oraz innych protagonistów nauki o informacji, jednocześnie nie przeceniając wartości strategicznej samej

[1] T. A. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa, ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego,* Warszawa 2014, s. 31-32.

informacji w kontekście tzw. *attentioncrash*, czy *Devil of Information Overload*[2]. Z drugiej jednak strony dla Aleksandrowicza powstanie społeczeństwa informacyjnego wraz z przynależnymi mu atrybutami już samo w sobie stanowiło i nadal stanowi daleko idącą zmianę cywilizacyjną, której symptomy dotyczą zarówno funkcjonowania społeczeństw, państw oraz całego systemu międzynarodowego, ogarniając jego główne elementy siecią[3]. W tym kontekście można się zgodzić z autorem, dla którego kluczowym pojęciem opisującym funkcjonowanie społeczeństw i państw w wieku informacji jest zbiór wzajemnie powiązanych zależności w postaci węzłowej architektury – czyli sieć.

Autor zauważa przy tym, że konstytutywną cechą społeczeństwa informacyjnego jest takie podejście do informacji, które zakłada ich strategiczną rolę oraz kategoryzuje ich zbiór jako stricte strategiczny, równocześnie niejako przy okazji próbując upowszechnić do nich dostęp, co więcej ich przetwarzanie staje się podstawą tworzenia dochodu narodowego i źródłem utrzymania coraz bardziej znaczącej części społeczeństwa, a jednocześnie, co paradoksalne, dostęp do informacji, zdolność do jej przetwarzania, zabezpieczenia, przekazywania i przechowywania staje się również kluczowe dla bezpieczeństwa międzynarodowego[4].

Dla Aleksandrowicza konsekwencje przemian dla środowiska szeroko rozumianego bezpieczeństwa to szczególnie poszerzenie przedmiotowego katalogu zagrożeń, które już od pewnego czasu nie koncentrują się w znaczącej mierze wokół działań wojennych czy innych militarnych presji ze strony państw i agresywnych struktur zorganizowanych[5]. Zwłaszcza jeśli weźmiemy pod uwagę kluczowy wytwór społeczeństwa informacyjnego w dziedzinie komunikacji i usieciowienia, jakim jest Internet. To dla asymetrycznych pól walki idealne narzędzie wywiadowcze, dzięki któremu można typować cele zamachów, dokonywać co najmniej wstępnego rozpoznania, określać drogi dojścia i odskoku, wybierać najbardziej optymalny *modus operandi*, czy wreszcie w przypadku włamania do sieci wewnętrznej – również zniszczyć istniejące zabezpieczenia, czy wręcz uniemożliwić funkcjonowanie instytucji wybranej na cel[6].

Aleksandrowicz nie widzi przesady, zresztą nie sposób odmówić jego twierdzeniu słuszności, że największy wpływ na zmianę sposobów prowadzenia konfliktów zbrojnych mają takie rezultaty rewolucji informacyjnej, z których wynika zwiększenie możliwości pozyskiwania informacji, a w konsekwencji również skuteczna koordynacja działań poszczególnych części składowych konkretnego przedsięwzięcia[7]. Szczególnie jest to widoczne w przypadku konfliktów asymetrycznych, gdzie jedna ze stron na skutek dysproporcji potencjałów militarnych zechce zastosować taktyki niekonwencjonalne z punktu widzenia przeciwnika, wciągać go

[2] Ibidem, s. 65-66.
[3] Ibidem, s. 70.
[4] Ibidem, s. 79.
[5] Ibidem, s. 81.
[6] Ibidem, s. 95
[7] Ibidem, s. 97.

w obszary nieznane jemu samemu, innymi słowy uderzać nie w siły przeciwnika, lecz w jego sieciowe otoczenie[8].

Pisząc o sieciach, autor zwraca uwagę na ich stałą obecność w systemach społeczeństw oraz ewolucję tych sieci pod wpływem rozwoju technologii komunikacyjnych, co implikuje zmiany dotykające w zasadzie wszelkich przejawów aktywności człowieka na polu społeczno-politycznym[9]. Dla Aleksandrowicza bezdyskusyjne jest to, że w społeczeństwie informacyjnym o charakterze sieciowym, klasyczne opisy władzy oparte na hierarchii, podziale kompetencji, wyznaczaniu granic nie spełniają funkcji deskryptywnej ani eksplanacyjnej, bowiem dla państwa realizującego swoje zadania w warunkach usieciowienia, koniecznym się staje uwzględnienie roli czy interesu wielu węzłów i klastrów sieci, ponieważ ich znaczenie, możliwości i zasoby stoją w opozycji do narzucanej przez państwo całkowitej dominacji[10]. Tym samym możemy mieć do czynienia z dyfuzją władzy tak dobrze widoczną podczas kryzysu ukraińskiego[11].

Dla autora konsekwencje przemian dla środowiska bezpieczeństwa to nie tylko dyfuzja władzy, czy osłabienie roli państwa. To także, a może przede wszystkim, utrata prywatności w paradoksalnym uniwersum wolnego przepływu informacji. Aleksandrowicz jednocześnie konstatuje, że nasza podatność na manipulację jest w znacznej mierze konsekwencją złych wyborów, takich jak: beztroskie udostępnianie sensytywnych danych w serwisach społecznościowych czy też bezrefleksyjne używanie funkcji lokalizacyjnych[12].

Czy zatem państwo może być jeszcze bezpieczne?

Aleksandrowicz odpowiada na to pytanie z właściwą dychotomią wpisaną w kontekst przemian cywilizacyjnych. Bo z jednej strony mamy prawne regulacje użycia siły w stosunkach międzynarodowych, z kluczowym z punktu interesów bezpieczeństwa Rzeczpospolitej Polskiej art. 5 NATO[13], z drugiej strony sieciowy paradygmat bezpieczeństwa państwa *in statu nascendi*, którego próby opisu za pomocą tradycyjnych realistycznych i neoliberalnych paradygmatów nie tylko nie przynosiły zadowalających rezultatów, ale były niewystarczające do zrozumienia wykraczających poza ich ramy dynamicznych i fundamentalnych przemian podmiotu bezpieczeństwa, jego przedmiotu i wzajemnych relacji[14].

Wydaje się, że autor tutaj funduje czytelnikowi niepotrzebną obfuskację, z jednej strony bowiem traktuje paradygmaty realistyczne i neoliberalne jako niewystarczające, z drugiej konkluduje,że w badaniach nad bezpieczeństwem za dominujące należy uznać poglądy mieszczące się w ramach szkoły realistycznej, wliczającej pozostałe paradygmaty (neoliberalny, konstruktywny, krytyczny) do wywodzących się z teorii bezpieczeństwa realistów, którzy z kolei rozwijają je w różnych kierunkach przyjmując je jako punkt wyjścia do tworzenia nowych krytycznych interpreta-

[8] Ibidem, s. 100-101.
[9] Ibidem, s. 114.
[10] Ibidem, s. 116-117.
[11] Ibidem, s. 122.
[12] Ibidem, s. 125.
[13] Ibidem, s. 136 – 140.
[14] Ibidem, s. 183.

cji wobec realizmu[15]. Jednocześnie Aleksandrowicz zauważa, że nowatorskie podejście do bezpieczeństwa prezentują koncepcje wypracowane w ramach konstruktywizmu, głoszone przez szkołę kopenhaską, z kluczowym pojęciem sekurytyzacji[16].

Odpowiadając na pytanie, czy państwo może być bezpieczne, autor widzi je zarówno jako podmiot jak i przedmiot bezpieczeństwa, a zacieranie się granicy pomiędzy bezpieczeństwem zewnętrznym a wewnętrznym państwa oraz poszerzanie katalogu zagrożeń i wartości chronionych wprost przekłada na konieczność redefiniowania pojęcia bezpieczeństwa narodowego, wpisując w jego zakres obydwa bezpieczeństwa[17].

Aleksandrowicz opisując środowisko bezpieczeństwa narodowego, dostrzega rosnącą rolę znacznej ilości podmiotów pozapaństwowych, posiadających podlegające ochronie własne cele i wartości, a które nie zawsze pokrywają się z wartościami chronionymi przez państwo oraz dodatkowo działania tych podmiotów mogą wpływać, i nierzadko to czynią, na bezpieczeństwo państwa, co oczywiste działają one jednak w potrzebie zabezpieczenia własnego bezpieczeństwa[18], posiadając przy tym globalne interesy. Przy okazji niejako ich działania mogą generować poważne zagrożenia dla bezpieczeństwa państwa, zarówno powodowane celowym zamysłem np. terroryzm, jak też zupełnym przypadkiem np. przestępczość, koncerny ponadnarodowe[19]. Zresztą konsekwencje procesów globalizacyjnych dla autora przekładają się na nadmiarową reprezentację problemów, także globalnych wyzwań i zagrożeń, charakteryzujących się transgranicznym, kosmopolitycznym charakterem, co w konsekwencji wymaga również specyficznego podejścia do ich analizy i zwalczania adekwatnie do ich ponadnarodowości, bowiem w opisywanym konstrukcie pojedyncze państwo, czy nawet grupa państw nie mogą samodzielnie się mierzyć z takimi wyzwaniami w zakresie bezpieczeństwa[20].

Procesy globalizacyjnestanowią swoistą sieć, a dla Aleksandrowicza korporacje transnarodowe, wpływające w coraz większym zakresie na funkcjonowanie państw narodowych, znakomicie odnajdują się w środowisku sieciowym, które je spaja, przy okazji demonstrując atrybut transnacjonalizacji rozumianej jako zmiana wektoru zaangażowania politycznego i pozbawienie państwa monopolu inicjowania procesów politycznych[21].

Autor zauważa przy tym, że sieciowy charakter przybierają także podmioty generujące asymetryczne zagrożenia dla bezpieczeństwa państwa (organizacje terrorystyczne, zorganizowane grupy przestępcze działające częstokroć na skalę międzynarodową)[22]. Aleksandrowicz opisując współczesne stosunki międzynarodowe przedstawia je jako wielocentrową siatkę powiązań, w której państwo narodowe jest tylko jednym z węzłów łączących pozostałe klastry[23].

[15] Ibidem, s. 184.
[16] Ibidem, s. 186.
[17] Ibidem, s. 187, 191 – 192.
[18] Ibidem, s. 194.
[19] Ibidem, s. 195.
[20] Ibidem, s. 196.
[21] Ibidem, s. 198.
[22] Ibidem.
[23] Ibidem, s. 199.

W konsekwencji dla Aleksandrowicza bezpieczeństwo państwa jawi się jako kluczowy i niezwykle ważny element, przy czym jego sieciowy paradygmat znajduje *in statu nascendi*, dlatego w książce przedstawia tylko jego zarys, zauważając jednocześnie, że daleko mu do kompletności i kompleksowości tradycyjnych paradygmatów bezpieczeństwa[24]. Po raz kolejny autor podkreśla odmienne kwestie opisujące paradygmat sieciowy, zauważając, że separacja od państwocentryczności, osadza go z jednej strony w roli jednego z wielu istotnych węzłów, z drugiej jednocześnie paradoksalnie przypisując mu kluczową pozycję, zagrożoną co prawda przez niepaństwowe podmioty i to pomimo osadzenia całego paradygmatu w architekturze rozproszonej[25].

W tym kontekście Aleksandrowicz bezpieczeństwo Rzeczpospolitej Polskiej osadza również w ramach paradygmatu sieciowego, widocznego zarówno w postrzeganiu podmiotu bezpieczeństwa narodowego, jak i jego przedmiotu oraz relacjach między tymi elementami[26]. Co więcej, autor analizując sposób traktowania przedmiotu bezpieczeństwa narodowego wprost wskazuje na wyraźne tendencje, takie jak, po pierwsze odejście od państwocentryczności i wiązania zagrożeń dla bezpieczeństwa narodowego wyłącznie z wrogimi działaniami podejmowanymi przez podmioty państwowe, przede wszystkim na płaszczyźnie militarnej, po drugie amalgamat bezpieczeństwa wewnętrznego i zewnętrznego, oraz po trzecie włączenie do katalogu zagrożeń działań nieintencjonalnych, będących wynikiem różnych katastrof[27].

Aleksandrowicz doskonale dostrzega elementy paradygmatu sieciowego w opisach współczesnego otoczenia bezpieczeństwa, za podstawowy czynnik determinujący kształt otoczenia bezpieczeństwa uważając w tym kontekście globalizację, która również determinuje obszar bezpieczeństwa Rzeczpospolitej Polskiej[28]. Autor wskazuje przy tym, że sieciowy paradygmat bezpieczeństwa stanowi nie tylko teoretyczną konstrukcję lecz jest praktycznie wykorzystywany w strategii i polityce bezpieczeństwa Rzeczpospolitej Polskiej, a także innych państw[29].

Sieciowy paradygmat to nie tylko odejście od państwocentryczności, ale jak objaśnia Aleksandrowicz to także, a może przede wszystkim zwrot ku zagrożeniom związanym z cyberprzestrzenią, powiązanymi atakami na infrastrukturę krytyczną, i wypracowania przez poszczególne węzły sieci nie tylko zdolności defensywnych ale także ofensywnych – do dokonywania ataków w cyberprzestrzeni, wymierzonych w przeciwnika zarówno państwowego, jak i pozapaństwowego[30].

W kontekście cyberprzestrzeni, zagadnień wojen sieciowych, czyli również antycypacji zagrożeń, książka zawiera niezwykle cenne rozważania dotyczące przyszłości i jej alternatywnych obrazów. Tutaj autor ukazuje możliwe scenariusze, jednocześnie zaznacza, że tworząc prognozę nie należy przewidywać faktów, które

[24] Ibidem, s. 200.
[25] Ibidem, s. 201.
[26] Ibidem, s. 202 – 204.
[27] Ibidem, s. 205 – 206.
[28] Ibidem. s. 207, 211.
[29] Ibidem, s. 214.
[30] Ibidem, s. 214 – 215.

zaistnieją lub nie w przyszłości, lecz skupić się na tendencjach, megatrendach i zadać sobie pytanie, jakie warunki muszą być spełnione, aby trend podlegał kontynuacji, czy są czynniki, które go osłabiają, wzmacniają, zmieniają[31]? Jest to, według autora, podstawa do budowania scenariuszy, oczywiście z właściwą perspektywą horyzontu czasowego[32]. Aleksandrowicz niezwykle sprawnie kreśli przed nami scenariusze na przyszłość, najpierw jednak stawiając pytania o koniec kryzysu gospodarczego, powstanie luk zarządzania, rozwój potencjalnych konfliktów, łuk niestabilności czy wreszcie wpływ nowych technologii[33]. W odpowiedzi dostajemy od autora zestaw scenariuszy przygotowanych przez analityków wywiadu amerykańskiego o intrygujących nazwach: wstrzymane silniki, fuzja, dżinn wydostał się z butelki, świat bezpaństwowy[34], przy czym należy stwierdzić, że ich wyjaśnienie jest jak najbardziej wyczerpujące.

Omawiając scenariusze Aleksandrowicz dodatkowo wprowadza pojęcie „czarnego łabędzia" jako zjawiska mogącego zakłócić ciąg przyczynowo-skutkowy leżący u podstaw jakiegokolwiek realizowanego scenariusza. W ten sposób autor wprowadza słynną zmienną – *coś o czym nie wiemy, że nie wiemy*. Jednocześnie zauważa pewny paradoks: jak można prognozować występowanie czegoś co z definicji jest nieprognozowalne[35]? Okazuje się, że jednak można. Aleksandrowicz, nawiązując do „czarnego łabędzia", przywołuje niezwykle interesującą prognozę Global Trends 2030, która wymienia osiem czarnych łabędzi – pandemię, zmiany klimatyczne, upadek euro i rozpad Unii Europejskiej, zmiany demokratyczne/autorytarne w Chinach, demokratyczne reformy w Iranie, wojnę z użyciem broni masowego rażenia i/lub pełnego arsenału cyberbroni, słoneczny impuls elektromagnetyczny, wycofanie się USA z pełnienia funkcji supermocarstwa na arenie międzynarodowej[36].

Następnie autor pyta, co będzie determinować nasze bezpieczeństwo w przyszłości, przed jakimi wyzwaniami, czy szansami przyjdzie nam stanąć, z jakim ryzykiem się zetkniemy, by następnie trafnie skonstatować, że niewykorzystane szanse przynoszą z reguły porażkę, niepodjęte wyzwania, którym nie udało się sprostać, lubią przekształcać się w zagrożenia, brak wiedzy, choćby nieznaczny oznacza ryzyko popełnienia błędów oraz niedostrzeżenie szans, wyzwań i zagrożeń, a bierne oczekiwanie na to, co ma się zdarzyć jest rozwiązaniem fatalnym, które sprawia, że zagrożenia skwapliwie uznajemy za „nagłe", „nieodwracalne", „nieuniknione" – choćby wcale takie nie były[37].

Zdaniem Aleksandrowicza zasadniczy wpływ na kierunki rozwoju, a tym samym środowisko bezpieczeństwa będą miały wydarzania, zaliczane przez autora do prawdopodobnych – nowe źródła energii, opracowanie opłacalnej ekonomicznie metody odsalania wody morskiej, pojawienie się skutecznych metod manipulacji

[31] Ibidem, s. 216 – 217.
[32] Ibidem, s. 217.
[33] Ibidem, s. 219 – 221.
[34] Ibidem, s. 222.
[35] Ibidem, s. 226.
[36] Ibidem, s. 226 – 227.
[37] Ibidem, s. 227.

genetycznych i powrót do eugeniki, powstanie zaawansowanej AI[38]. Jednocześnie autor prognozuje niekorzystne zjawiska typu „czarny łabędź", takie jak: kwestia użycia broni masowego rażenia, legalne zdobycie władzy przez imigrantów w jednym bądź kilku krajach europejskich, zmiany klimatyczne, katastrofy naturalne i burze solarne[39].

Ostatecznie dla Aleksandrowicza kluczowym czynnikiem przemian pozostaje technologia informacyjna, a bezpieczeństwo państwa stanowi rozległy obszar poznania naukowego[40].

Reasumując, wartość poznawcza książki pozostaje poza dyskusją, czytelnik dostaje kompletny wykład na temat paradygmatu bezpieczeństwa, może nie tylko narodowego co bezpieczeństwa w ogóle. Szczególnie cenną poznawczo jawi się kwestia zestawienia owego paradygmatu z atrybutami społeczeństwa sieciowego, jednostek i organizmów państwowych. Choćby dlatego, że obecne tempo zmian w technologiach komunikacyjnych oraz ich wykorzystanie przez społeczeństwo sieci nie stanowi precedensu w dotychczasowej historii ludzkości, a zmiany te mają również wpływ na bezpieczeństwo tak jednostek, jak i całych systemów. Świat zanurzony w sieci potrzebuje bezpieczeństwa, a Aleksandrowicz, poszukując paradygmatu bezpieczeństwa, wydaje się go nie tylko odnajdywać, ale całkiem zgrabnie objaśniać.

[38] Ibidem, s. 229.
[39] Ibidem, s. 229 – 230.
[40] Ibidem, s. 233 – 234.