ACTA UNIVERSITATIS LODZIENSIS
FOLIA LIBRORUM 2 (25), 2017
ISSN 0860-7435

Małgorzata Bańkowska
Państwowa Wyższa Szkoła Zawodowa
im. Prezydenta Stanisława Wojciechowskiego w Kaliszu
e-mail: m.bankowska@bu.pwsz.kalisz.pl

Tomasz R. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa: Editions Spotkania, 2016, 223 ss.

DOI: http://dx.doi.org/10.18778/0860-7435.25.07

W 2016 r. nakładem oficyny wydawniczej Editions Spotkania ukazała się praca Tomasza R. Aleksandrowicza pt. *Podstawy walki informacyjnej*, która stanowi kolejną część nienumerowanej serii „Bezpieczeństwo Dziś i Jutro". Opracowanie prezentuje wyniki wieloletnich badań nad problematyką informacji we współczesnym świecie i uwzględnia interdyscyplinarny charakter procesów informacyjnych osadzonych w zróżnicowanych kontekstach społecznych i politycznych. Na publikację o objętości 223 stron składają się trzy odrębne części tematyczne, z których każda poprzedzona została wprowadzeniem prezentującym podstawowe tezy. Każda z części zawiera trzy rozdziały numerowane w sposób ciągły. Taki układ pracy uzasadniony został „chęcią usystematyzowania obszernej problematyki będącej przedmiotem analizy" (s. 13).

Jak czytamy we *Wstępie* „praca stanowi rozwinięcie wcześniejszych badań" (s. 13) ze szczególnym uwzględnieniem kwestii bezpieczeństwa narodowego i międzynarodowego oraz walki i wojny informacyjnej. W swojej analizie T. Aleksandrowicz wychodzi od rewolucji informacyjnej określonej przez cyfrową postać informacji (powstanie cyberprzestrzeni) i wskazuje na zasadnicze zagrożenia związane z szumem informacyjnym oraz dezinformacją i masowością informacji. Rozważania oscylują wokół zasadniczych konsekwencji rozwoju informacji. Autor zalicza do nich: „powstanie i rozwój spo-

łeczeństwa informacyjnego" (s. 11) o charakterze sieciowym, nadanie informacji strategicznego wymiaru, prowadzenie działań dezinformacyjnych oraz walki i wojny informacyjne w cyberprzestrzeni, które zagrażają bezpieczeństwu narodowemu i międzynarodowemu.

W części I (*Zmiany środowiska bezpieczeństwa w pierwszej połowie XXI wieku*) omówiono początki społeczeństwa informacyjnego. Autor wskazuje na konstytutywne cechy społeczeństwa informacyjnego, do których zalicza m.in. intensywny rozwój środków masowego przekazu oraz IT, cyberkulturę, integrację i globalizację informacji. Stawia także tezę, że społeczeństwo informacyjne i „społeczeństwo oparte na wiedzy" cechują podobne postawy i warunki dostępu do informacji, tj.: rozwój technologii informacyjnych, „dominacja kontaktów pośrednich nad bezpośrednimi" (s. 25), nieograniczony czasowo dostęp do informacji i funkcjonowanie w cyberprzestrzeni. Jako główne konsekwencje rozwoju społeczeństwa informacyjnego T. Aleksandrowicz wymienia nadmiar informacji, utratę prywatności, „możliwość inwigilacji", manipulowanie informacją oraz dyfuzję władzy (udział w rządzeniu przez podmioty pozapaństwowe) (s. 39). Zdaniem Autora powstają nowe rodzaje władzy – „władza usieciowiona", realizowana „przez jedne węzły nad innym węzłami", „władza sieciowa" tworzona przez sieci komunikacyjne, „władza sieci", której przejawem jest kontrola komunikatów i dostępu oraz „władza sieciotwórcza", aktywna na płaszczyźnie tworzenia i programowania sieci (s. 39).

Część II (*Informacja jako zasób strategiczny*) poświęcona została zagadnieniom natury terminologicznej. W dokonanym przeglądzie definicji informacji T. Aleksandrowicz odwołuje się głównie do koncepcji polskich informatologów (m.in. Krzysztofa Liedla, Mariana Mazura, Piotra Sobolewskiego). Przeprowadzoną analizę różnorodnych atrybutów informacji konstatuje on stwierdzeniem, że informacja „jako zasób strategiczny – posiada […] swoją wartość", a „jej zdobycie i wykorzystanie pociąga za sobą określone koszty, zaś jej brak oznacza brak skuteczności w działaniu" (s. 57). W kontekście społecznego zapotrzebowania na informację i jej znaczenia dla jednostek oraz grup społecznych Autor wskazuje na zagrożenia wynikające z dezinformacji, podkreślając przy tym jej ścisłe związki z propagandą i manipulacją (np. wydarzenia II wojny światowej oraz wojny w Wietnamie). Jako zabezpieczenie przed dezinformacją w każdej sferze ludzkiej działalności T. Aleksandrowicz uznaje właściwy dobór źródeł informacji, ocenę ich wiarygodności oraz rzetelnie przeprowadzane analizy. Wśród analiz eksperckich omawia analizy akademickie i decyzyjne (s. 63).

Zasadnicza analiza bezpieczeństwa informacyjnego i zagrożeń informacyjnych przedstawiona została w części III (*Bezpieczeństwo informacyjne. Walka i wojna informacyjna*). W przyjętym porządku terminologicznym Autor

wychodzi od wyjaśnienia pojęcia walki informacyjnej rozumianej jako działania mające na celu „wykorzystanie, uszkodzenie, zniszczenie informacji […] albo też zaprzeczenie informacjom po to, aby osiągnąć znaczne korzyści" (s. 105). W tym kontekście pojęcie bezpieczeństwa informacyjnego (s. 107) rozumiane jest jako jeden z elementów bezpieczeństwa państwa (podmiotu) obok bezpieczeństwa militarnego, politycznego, ekonomicznego, ekologicznego, humanitarnego, ideologicznego i kulturowego (s. 111–112). Katalog zagrożeń jest jednak o wiele większy i składa się nań szereg różnorodnych elementów, dotyczących procesów informacyjno-decyzyjnych (zawiera je m.in. Projekt Doktryny Bezpieczeństwa Informacyjnego RP). Główny teren walki informacyjnej stanowi cyberprzestrzeń oraz środki masowego przekazu. Medialność uznawana jest także za „jedną z konstytutywnych cech terroryzmu": „Terroryzm jest formą walki informacyjnej, sam bowiem akt terrorystyczny to jedynie środek wyrazu, a istotny jest przekaz, jaki ze sobą niesie użycie przemocy" (s. 138). Walka/wojna informacyjna to jeden z przejawów konfliktów międzynarodowych współczesnego świata. Cyberkonflikty i cyberwojna stanowią zasadniczy element, wspierający konwencjonalne działania militarne (s. 148) jako „piąte środowisko walki (po lądzie, morzu, przestrzeni powietrznej i kosmosie)" (s. 158). Na konkretnych przykładach Autor wskazuje, w jaki sposób współczesne mocarstwa wykorzystują narzędzia informacyjne (koncepcja rosyjskiej wojny informacyjnej, amerykańska koncepcja *information warfare*).

Ostatni rozdział (*Cyberprzestrzeń jako sfera walki i wojny informacyjnej*) poświęcony został zagrożeniom informacyjnym w świecie cyfrowym. Pod pojęciem cyberprzestrzeni rozumie się tu za Danielem T. Kuehlem „globalną domenę w ramach środowiska informacyjnego", która korzysta z technologii i infrastruktury teleinformatycznej (s. 175). W takim ujęciu cyberprzestrzeń traktowana jest jako przestrzeń operacyjna, w której mają miejsce różnorodne działania, nastawione na uzyskanie określonego celu. Działania te mogą mieć wymiar pozytywny (dostęp do informacji, wzbogacanie zasobów wiedzy, komunikowanie) i negatywny (dezinformacja, przestępczość komputerowa, szpiegostwo). Wśród różnorodnych zagrożeń związanych z informatyzacją życia społecznego i politycznego T. Aleksandrowicz wymienia aktywizm i haktywizm, prowadzony zarówno w sposób indywidualny, jaki i zorganizowany (ruchy polityczne i społeczne, organizacje terrorystyczne) (s. 183). Uzupełnienie analizy stanowi przegląd działań środowisk międzynarodowych na rzecz ochrony przestrzeni informacyjnej (rekomendacje Rady Europy, dyrektywy Unii Europejskiej) oraz polskich regulacji prawnych w zakresie bezpieczeństwa informacji.

W *Zakończeniu* T. Aleksandrowicz podkreśla, iż rewolucja cyfrowa stworzyła nowe zagrożenia i wykreowała nowy rodzaj wojny, w której brak reguł i stosownych, adekwatnych do potrzeb narzędzi obrony.

W założeniu autorskim publikacja adresowana jest do różnych grup odbiorców, zarówno teoretyków, jak i praktyków, zainteresowanych problematyką szeroko rozumianego bezpieczeństwa. Jednak dobór materiału i charakter opracowania wskazują, iż jej odbiorcami będą głównie osoby, które po raz pierwszy stykają się z zagadnieniami zarządzania informacją i problematyką bezpieczeństwa. Przedstawiona we *Wstępie* prezentacja metod i narzędzi badawczych zapowiada systematyczną, całościową analizę skomplikowanych zjawisk informacyjnych. Autor deklaruje racjonalizm metodologiczny, podejście holistyczno-systemowe oraz zastosowanie szeregu metod analitycznych z zakresu nauk społecznych i wojskowych (s. 13). Wśród wykorzystanych narzędzi badawczych wymienia obserwację, analizę i krytykę źródłową, dogmatykę prawniczą oraz krytyczną ocenę piśmiennictwa. Zaprezentowana metodologia ma jednak wyłącznie charakter deklaratywny. Poszczególne części tematyczne stanowią zbiór wielowątkowych refleksji. Autor, czerpiąc z bogatej literatury przedmiotu, w tym zwłaszcza prac Tomasza Gobana-Klasa i Piotra Sienkiewicza, do których odwołuje się wielokrotnie, nie syntetyzuje zebranego materiału. Stanowi to poważny mankament opracowania, określanego przez Autora mianem monografii naukowej (s. 14). Badacz zrezygnował też z zasady „od ogółu do szczegółu" i umieścił podstawowe rozważania terminologiczne w drugiej części analizy, po omówieniu kwestii dotyczących zasobów informacyjnych i zasad zarządzania nimi.

W ogólnej ocenie książka stanowi zbiór podstawowych informacji dotyczących sieci informacyjnych, społeczeństwa informacyjnego oraz zasad bezpieczeństwa narodowego i międzynarodowego. Z uwagi na obszerną bibliografię przedmiotu (s. 207–220) oraz indeks przedmiotowy może być wykorzystywana jako lektura uzupełniająca dla studentów pierwszych lat kierunków związanych z bezpieczeństwem i informacją.