

Spis treści

Wstęp	7
Rozdział I	
Współczesne środowisko walki o przewagę informacyjną	27
1. Infosfera a środowisko informacyjne – próba uporządkowania pojęć	27
1.1. Środowisko informacyjne z perspektywy informatologii	27
1.2. Środowisko informacyjne w domenie bezpieczeństwa	42
1.3. Środowisko informacyjne jako system informacyjno-decyzyjny	50
2. Proces informacyjny w środowisku walki o przewagę informacyjną	56
2.1. Proces informacyjny w systemach informacyjnych	56
2.2. Proces informacyjny w systemach decyzyjnych dla obronności	66
Rozdział II	
Integracja walki o przewagę informacją z procesem informacyjnym	73
1. Faza gromadzenia informacji	74
2. Faza opracowania informacji	78
3. Faza przechowywania informacji	82
4. Faza wyszukiwania informacji	85
5. Faza przetwarzania informacji	89
6. Faza udostępniania i wdrażania informacji	93
Rozdział III	
Szerokie i wąskie rozumienie pojęcia walki informacyjnej	101
1. Walka o informacje w kontekście kooperacji pozytywnej i kooperacji negatywnej	101
2. Walka informacyjna jako komponent wojny informacyjnej	118
Rozdział IV	
Informacyjne konteksty uzyskiwania przewagi	137
1. Nadmiar informacji w społeczeństwie światowego ryzyka	137
2. Konteksty uzyskiwania przewagi za pomocą informacji	152
2.1. Informacja jako fetysz w społeczeństwie (nie)wiedzy	158
2.2. Informacja jako patogen infosfery i broń masowej manipulacji	168
2.3. Informacja jako tworzywo inwigilacji	183
2.4. Informacja jako kapitał wywiadu konkurencyjnego	200

Rozdział V	
Służby wspomagające podmioty w procesach decyzyjnych	211
1. Analitycy, ich typologia i kompetencje	213
2. Źródła pozyskiwania informacji przez analityków	229
3. Zadania służb analityczno-informacyjnych i metody ich pracy	238
Rozdział VI	
Komponenty kultury bezpieczeństwa wpływające na bezpieczeństwo informacyjne	251
1. Charakterystyka informacyjnych komponentów kultury bezpieczeństwa	251
1.1. Kultura informacyjna	264
1.2. Ekologia informacji	273
1.3. Wychowanie do informacji	284
1.4. Kultura organizacyjna	293
1.5. Polityka informacyjna	308
1.6. Kultura bezpieczeństwa informacyjnego	317
2. Konwergencja informacyjnych komponentów kultury bezpieczeństwa	329
Rozdział VII	
Informatologiczny kontekst kultury bezpieczeństwa informacyjnego	341
1. Interdyscyplinarność i transdyscyplinarność nauk o bezpieczeństwie i nauki o informacji	347
2. Związek kultury bezpieczeństwa informacyjnego z nauką o informacji	356
3. Badanie kultury bezpieczeństwa informacyjnego	369
Rozdział VIII	
Znaczenie kultury bezpieczeństwa informacyjnego w środowisku walki o przewagę informacyjną	383
1. Potrzeba powszechnej świadomości informacyjnej społeczeństwa	383
2. Obszary edukacji dla kultury bezpieczeństwa informacyjnego	393
3. Kultura bezpieczeństwa informacyjnego buforem podmiotu bezpieczeństwa w walce o przewagę informacyjną	418
Zakończenie	429
Bibliografia	439
Wykaz tabel i rysunków	481
Indeks osobowy	483
Indeks przedmiotowy	491

Wstęp

Korzystaj z informacji albo giń!

Kultura bezpieczeństwa informacyjnego jako komponent kultury bezpieczeństwa kreującej środowisko bezpieczeństwa człowieka decyduje o odporności społeczeństwa na ataki informacyjne oraz o jego świadomości na temat współczesnej wojny informacyjnej¹. Jak zaznaczyłam w podsumowaniu jednego z rozdziałów monografii *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*², kultura bezpieczeństwa informacyjnego jest nie tylko nieodzowna w celu wykształcenia odporności członków danego społeczeństwa na wrogie działania w nie wymierzone, ale także niezbędna do budowy jego wrażliwości i „podwyższonej uważności” wobec sytuacji zagrożenia, jest również konieczna do przygotowania społeczeństwa do identyfikowania takich sytuacji w swoim otoczeniu i wykształcenia potrzeby (w tym wewnętrznego obowiązku) odpowiedniego reagowania na nie. Mowa o zagrożeniach wynikających z infekowania środowiska informacyjnego i o przeciwdziałaniu im, które wymaga zaangażowania państwa w budowanie społecznego ładu informacyjnego i zagwarantowanie odpowiedniego poziomu kultury informacyjnej obywateli. Realizacja tego zadania wiąże się z opracowaniem i wprowadzeniem w życie stosownych norm informacyjnych (szczegółowo pisał o nich Józef Oleński) jak również z wdrożeniem odpowiedniego systemu edukacji informacyjnej wspieranego upowszechnianiem wiedzy na temat wagi kompetencji informacyjnych

-
- ¹ We wstępie odwołano się do definicji terminów takich jak: *kultura bezpieczeństwa, kultura bezpieczeństwa informacyjnego, bezpieczeństwo informacyjne, ekologia informacji, przeciążenie informacyjne, walka informacyjna, służby analityczne, informacja, infosfera, patogeny informacyjne, cyberprzestrzeń, środowisko informacyjne, postprawda, procesy informacyjne*, opracowanych przez autorkę i zamieszczonych w *Vademecum bezpieczeństwa*, O. Wasiuta, R. Klepka, R. Kopeć (red.), Wydawnictwo Libron, Kraków 2018, oraz w *Vademecum bezpieczeństwa informacyjnego*, t. 1–2, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019.
 - ² H. Batorowska, *Przeciążenie informacyjne wyzwaniem dla kształtowania kultury bezpieczeństwa*, [w:] *Bezpieczeństwo informacyjne i medialne w czasach nadprodukcji informacji*, H. Batorowska, P. Motylińska (red.), Wydawnictwo Naukowe i Edukacyjne SBP, Warszawa 2020, s. 19–40.

i medialnych w przeciwdziałaniu zagrożeniom, na jakie narażony jest człowiek podejmujący rozmaite aktywności w infosferze i środowisku informacyjnym. Podmiot bezpieczeństwa mający świadomość zagrożenia istotnych dla niego aktywów musi być przygotowany do podjęcia działań zapobiegawczych i w razie potrzeby zainicjować walkę o ich ochronę oraz prawidłową stymulację. W tym celu musi być jednostką dojrzałą – także informacyjnie – i charakteryzować się wysokim poziomem kultury informacyjnej, aby:

prawidłowo dekodować komunikaty, interpretować je zgodnie z obiektywną wiedzą i aprobowanym przez naród systemem aksjologicznym, podejmować racjonalne decyzje i aktywnie uczestniczyć w działaniach na rzecz zachowania tożsamości kulturowej swojego narodu³.

Dlatego w książce tej za podmiot bezpieczeństwa uznano człowieka, który samodzielnie decyduje o wyborze określonych idei, przyjmując je za własne, jak również sam postanawia o uznaniu społecznie akceptowanego systemu aksjonormatywnego, ponadto jest zdecydowany, aby działać w zgodzie z tym wyborem, a będąc jednostką o podwyższonej wrażliwości i uważności na działania wymierzone w ten system, podejmuje, jak pisze Juliusz Piwowarski: „działania prewencyjne bądź walkę z użyciem środków i metod najbardziej adekwatnych do swych możliwości oraz skali i rodzaju powstałych zagrożeń”⁴.

Dbalność o kulturę bezpieczeństwa decyduje zatem o poziomie bezpieczeństwa danego podmiotu, w tym o jego bezpieczeństwie informacyjnym, medialnym, cyfrowym, technologicznym, które wchodzi w skład szeroko rozumianej kultury bezpieczeństwa narodowego. Uznanie kultury bezpieczeństwa informacyjnego za ważny komponent ogólnej kultury bezpieczeństwa wynika ze stwierdzenia, że składa się na nią odpowiednio dobrany zespół elementów (mentalnych, społecznych i materialnych), które wpływają na bezpieczeństwo zarządzania informacją oraz odnoszą się do sposobu, w jaki informacja jest postrzegana, tworzona i wykorzystywana, a także sprzyjają dążeniu do pozytywnego oddziaływania na środowisko informacyjne, chroniąc je przed degradacją. Kultura bezpieczeństwa informacyjnego spleta się z innymi informacyjnymi komponentami kultury bezpieczeństwa – takimi jak kultura informacyjna, ekologia informacji, wychowanie do informacji, polityka informacyjna, kultura organizacyjna – na które w negatywny sposób oddziałuje zjawisko nadmiarowości informacji i przyspieszenia technologicznego, potęgujące ryzyko demontażu zastanych struktur. Stąd zainteresowanie badaczy kultury bezpieczeństwa informacyjnego rewolucją

³ Tamże, s. 31–32.

⁴ J. Piwowarski, *Nauki o bezpieczeństwie. Między kulturą bezpieczeństwa a studiami bezpieczeństwa*, Difin, Warszawa 2018, s. 30–31.

informacyjną i wynikającą z niej dominacją społeczeństw informacji i wiedzy. Widać to szczególnie wyraźnie w kontekście zagrożeń dla demokracji generowanych przez społeczeństwo informacyjne – postrzegane przez pryzmat społeczeństwa ryzyka – oraz w kontekście problemów globalnego rządzenia i społecznego ładu informacyjnego. Badacze nawiązują głównie do problemów niszczenia infosfery wynikających z przekształcania jej w poligon walki informacyjnej, lecz także do zjawisk takich jak: mediatyzacja, detronizacja prawdy, potop informacyjny i obniżenie jakości informacji, wykorzystywanie trudności z jej weryfikacją i obiektywną oceną.

Naturalną konsekwencją nadprodukcji informacji jest stres informacyjny utrudniający podmiotowi podejmowanie mądrych decyzji. Nadmiar informacji najczęściej uniemożliwia odróżnianie informacji prawdziwej od zniekształconej, zdeformowanej czy zmanipulowanej. Sztucznie fabrykowany – ułatwia sterowanie świadomością odbiorców redundantnych komunikatów, rozpowszechnianych zwłaszcza za pośrednictwem mass mediów. Ich dysponenci – kształtując opinię publiczną – zyskują dominującą pozycję w obiegu informacji. Media masowe stają się władzą, od której coraz bardziej uzależniona jest nie tylko polityka, ale także mądrość społeczeństwa. Modyfikując obraz rzeczywistości za pomocą coraz bardziej wyrafinowanych narzędzi technologicznych oraz odpowiednich stylów narracyjnych odwołujących się do emocji, uprzedzeń i osobistych przekonań, sprawiają, że społeczeństwo funkcjonuje w warunkach postprawdy, kłamstwa, fikcji; jest oszukiwane, ponieważ:

poddające się powszechnej weryfikowalności fakty są lekceważone i zastępowane przez tak zwane narracje, budowane na emocjach i uprzedzeniach, umiejętnie potęgowanych przez wspierające je media⁵.

Oznacza to, że interpretacja otaczającego podmiot świata dokonywana jest na podstawie nie faktów, ale odczuć, ponieważ w przestrzeni społecznej obiektywna prawda jest podporządkowana propagandzie. Dlatego Tomasz Goban-Klas, nazywając mass media pierwszą siłą społeczną, ukazuje ich moc niszczącą dla demokracji, stwierdzając, że „profesjonalnie wmawiają obywatelom, że informują, debatują, analizują, gdy [...] dają tylko pozór mądrości, a nie mądrość prawdziwą”⁶.

Badacz dostrzega w kryzysie wiarygodności mediów także uaktywnienie się nowej agory publicznej, tj. mediów społecznych, *public relations* i dziennikarstwa

⁵ T. Borkowski, *Brzytwa Ockhama przeciwko postprawdzie*, [w:] *Postprawda. Spojrzenie krytyczne*, T.W. Grabowski, M. Lakomy, K. Oświecimski, A. Pohl (red.), Wydawnictwo Naukowe Akademii Ignatianum, Kraków 2018, s. 29.

⁶ T. Goban-Klas, *Jak wolne mass media psują demokrację*, [w:] *Transformacje demokracji. Doświadczenia – Trendy – Turbulencje – Perspektywy*, L.W. Zacher (red.), Difin, Warszawa 2011, s. 296.

obywatelskiego wspomagających demokrację. Jedynie wolny obieg informacji może zagwarantować społeczny ład informacyjny, który Józef Oleński łączy z:

kompleksowym, spójnym systemem społecznych norm informacyjnych, społecznych procesów informacyjnych, społecznych systemów informacyjnych, społecznych zasobów informacyjnych w państwie, społeczeństwie, w gospodarce narodowej i w skali międzynarodowej, zaspokajającym potrzeby informacyjne ludzi, podmiotów gospodarki narodowej i instytucji sfery publicznej⁷.

Oznacza to, że zasady, które obowiązują w odniesieniu do gromadzenia, przechowywania i przekazywania informacji, muszą zagwarantować wszystkim podmiotom życia społecznego, ekonomicznego i politycznego zarówno dostęp do informacji, jak i jego ochronę, a także określać normy jakościowe niezbędne do profesjonalnego uczestnictwa tych podmiotów w procesie informacyjnym. Jasne reguły – określające, kto ma dostęp do jakich informacji, w jakiej formie może je otrzymać i jakie musi ponieść w związku z tym koszty, a także jakie warunki techniczne i organizacyjne są konieczne do realizacji procesów informacyjnych – są według Oleńskiego wymogiem utrzymania ładu informacyjnego w społeczeństwie⁸. Badacz rysuje także obraz państwa, w którym społeczny ład informacyjny jest zachwiany i prowadzi do coraz większego uzależnienia społeczeństwa od dysponentów informacji i mediów. Oskarża elity autokracji i kleptokracji o świadome pozbawianie mas zdolności do aktywności społecznej i obywatelskiej oraz kreowanie konsumpcyjnego stylu życia. W warunkach kleptokracji model społecznego ładu informacyjnego opiera się na:

posiadaniu przez państwo monopolu na środki masowego przekazu, edukację i badania naukowe oraz na wyłącznej dominacji sterującej funkcji informacji nad pozostałymi jej funkcjami⁹.

Oznacza to, że dozwolona i dostępna dla społeczeństwa będzie tylko taka informacja, która zapewni transfer środków z sektora publicznego lub prywatnego do podmiotów należących do wybranych grup interesów, zajmujących w kraju dominujące miejsce.

Także system autokratyczny, scentralizowany bądź rozproszony stanowi wyraźne zagrożenie dla społecznego ładu informacyjnego. W systemie tym nadrzędnym celem państwa jest bezpieczeństwo, trwałość i rozwój aparatu państwa, a środkami

⁷ J. Oleński, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Uniwersytet Warszawski, Warszawa 2006, s. 19.

⁸ Tenże, *Ekonomika informacji. Metody*, PWE, Warszawa 2003, s. 126.

⁹ Tenże, *Spoleczne bezpieczeństwo informacyjne podstawą demokratycznego państwa*, „Rocznik Kolegium Analiz Ekonomicznych” 2015, nr 36, s. 31, 34.

zapewnienia tego bezpieczeństwa są gospodarka i społeczeństwo¹⁰. Dlatego dopuszczana do obiegu jest tylko taka informacja, która jest korzystna dla elit autokracji i „służy bezpieczeństwu wybranych instytucji aparatu państwa oraz niektórych grup jego funkcjonariuszy”¹¹.

Trzeci model polityczno-ekonomiczny państwa, który Oleński określa jako ksenokrację, nie służy ani łaadowi informacyjnemu, ani powszechnemu bezpieczeństwu informacyjnemu, liczą się bowiem w nim interesy innych państw, organizacji czy podmiotów zagranicznych lub międzynarodowych. W tym modelu dobra informacja to taka:

za pomocą której skutecznie można kształtować zasoby informacyjne, środowisko informacyjne i sterować zachowaniami społecznymi zgodnie z interesami innych państw i zewnętrznych grup interesów¹².

Władze nie są zainteresowane tworzeniem własnych zasobów rzetelnej i użytecznej informacji, gdyż ich dostępność wiązałaby się z ryzykiem zdemaskowania prowadzonych przez decydentów działań dezinformacyjnych i manipulatorskich. Poprzez właściwą ocenę i interpretację tych zasobów można by ujawnić prawdziwe cele władzy.

Wszystkie wymienione systemy prowadzą do pogorszenia dostępu obywateli do informacji jako dobra publicznego, zdejmują z siebie odpowiedzialność za społeczny ład informacyjny gwarantujący obywatelom prawo do informacji. Tylko w modelu politykratycznym, którego podstawą jest społeczny ład informacyjny zapewniający wszystkim obywatelom, podmiotom gospodarczym i społecznym oraz władzy symetrię informacyjną, dostrzega wybitny ekonomista możliwość zapewnienia bezpieczeństwa informacyjnego. Państwo demokratyczne oparte na tym modelu musi mieć siłę, by przeciwstawić się destrukcyjnym działaniom elit kleptokracji, autokracji i ksenokracji, zdając sobie sprawę, że walka z nimi jest prowadzona głównie w sferze informacyjnej, dlatego:

przejęcie kontroli nad informacją i uzyskanie monopolu na dystrybucję informacji za pomocą środków masowego przekazu nie tylko jest warunkiem przejęcia i utrzymania władzy, lecz także daje możliwość kształtowania modelu społeczno-gospodarczego i świadomości społecznej¹³.

¹⁰ Tamże, s. 24.

¹¹ J. Oleński, *Instytucjonalne determinanty zarządzania jakością informacji*, [w:] *Zarządzanie informacją*, W. Babik (red.), Wydawnictwo Naukowe i Edukacyjne SBP, Warszawa 2019, s. 491.

¹² Tamże, s. 500.

¹³ J. Oleński, *Spoleczne bezpieczeństwo informacyjne...*, dz. cyt., s. 36.

Spółeczny ład informacyjny jest szczególnie narażony na demontaż w środowisku postprawdy. Piotr Pawełczyk i Jakub Jakubowski przypisują postprawdzie nową jakość, która związana jest nie tylko z incydentalnym występowaniem kłamstwa mającego wprowadzać adresata w błąd, lecz także z kreowaniem całkowicie nowej rzeczywistości, w której kłamstwa wynikają ze wzajemnego wzmacniania się informacji prawdziwych, półprawd i kłamstw medialnych. W świecie takim zanika umiejętność odróżniania komentarza od faktu, prawda przestaje istnieć jako synonim obiektywności, ponieważ następuje jej oderwanie od odbicia w umyśle ludzkim i w rzeczywistości, w której nastąpiło zubożenie na prawdę samą w sobie¹⁴. Z kolei dla Macieja Fladera postprawda jest:

odzwierciedleniem kryzysu rzeczywistości, w którym pojęcia stosowane w codziennym życiu w coraz mniejszym stopniu odpowiadają doświadczeniom pojedynczych osób i całych społeczności. W rezultacie ustaje możliwość racjonalnego porozumiewania się między ludźmi, ponieważ społeczną komunikację opanowują emocje, a przemoc zastępuje dialog i nie dba się o to, aby pozostać wiernym wydarzeniom lub myślom¹⁵.

W związku z tym budowanie ładu informacyjnego wymaga od społeczeństwa świadomości informacyjnej i postawy obywatelskiej. Jest to jednak za mało dla zachowania bezpieczeństwa informacyjnego. Piotr Sienkiewicz, podkreślając relację między innowacyjnością nowych technik informowania a potrzebą społecznego sterowania ich skutkami, wskazuje konieczność:

- demokratyzacji procesów masowego informowania,
- poszerzenia dostępu do źródeł informacji,
- doskonalenia mechanizmów selekcyjnych i specjalizacyjnych¹⁶.

Nowoczesna demokracja wymaga bowiem od obywateli umiejętności osądu, uczestniczenia w dyskursie dotyczącym życia publicznego, aktywności w życiu politycznym, świadomego korzystania z wolności wyboru¹⁷. Aby realizować te wymagania, społeczeństwo demokratyczne musi być społeczeństwem kompetentnym, dobrze

14 P. Pawełczyk, J. Jakubowski, *Postprawda i nowe media. Czy potrzebujemy postprawdy?*, „Środkowoeuropejskie Studia Polityczne” 2017, nr 1, s. 204; H. Batorowska, K. Batorowska, *Postprawda*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 2: *N-Z*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019, s. 133–138.

15 M. Flader, *Postprawda jako efekt błędnego poszukiwania prawdy*, „Teologia i Człowiek” 2018, t. 44, nr 4, s. 42–43.

16 P. Sienkiewicz, *Zagrożenia demokracji w społeczeństwie informacyjnym*, [w:] *Transformacje demokracji...*, dz. cyt., s. 223.

17 A. Wiktorska-Świećka, *Poprawianie demokracji. Założenia współczesnych koncepcji kształcenia obywatelskiego*, [w:] *Transformacje demokracji...*, dz. cyt., s. 194–214.

poinformowanym, wyedukowanym, nie tylko mającym szybki dostęp do aktualnej informacji, ale też ciągle konsultującym się i pozostającym w nieustannej interakcji, ponadto potrafiącym i chcącym realizować dobro wspólne (ang. *common good*). Kategorię dóbr wspólnych w szerszym rozumieniu Justyna Hofmokl łączy z domeną życia publicznego, sferą funkcjonowania demokracji, realizacją wolności obywatelskich, wolności słowa, ochroną dziedzictwa kulturowego, osobistą autonomią w relacji do zasobów materialnych i intelektualnych¹⁸.

Wypracowanie politycznych i społecznych form współżycia między autonomicznymi, wolnymi jednostkami o równych uprawnieniach wymaga nabywania przez nie określonych kompetencji obywatelskich w skali lokalnej i globalnej. Dlatego Lech W. Zacher dostrzega konieczność dążenia do utworzenia globalnego społeczeństwa obywatelskiego, czyli społeczeństwa partycypującego i współdecydującego, a najlepiej rządzącego na zasadzie permanentnego referendum, w którym władze byłyby wykonawcą obywatelskich decyzji¹⁹. Bez wykształcenia takich cech społeczeństwa trudno mówić o ukonstytuowaniu się globalnego społeczeństwa informacyjnego. Wspomniany badacz formułuje pytania, na które współcześnie odpowiedzi brzmią bardzo utopijnie. Jednak nie odrzuca idei społeczeństwa obywatelskiego, którą w przyszłości mogą urzeczywistnić „sieciowe kontakty i działania wielkich mas ludzi dobrej woli”, których połączy globalna współodpowiedzialność, globalne współdecydowanie i wspólny los²⁰. Zadanie to powinny wspierać tzw. demokracje informacyjne umożliwiające obywatelom uczestnictwo w podejmowaniu decyzji poprzez sieci informacyjno-komunikacyjne i bezpośrednią obecność w ich politycznym życiu. Antonina Szulak nazywa te demokracje partycypacyjnymi i deliberatywnymi (czyli demokracjami udziału i dyskusji). Dzięki wykorzystaniu najnowszych technologii informacyjnych

otwierają [one – przyp. aut.] możliwości realizacji praw człowieka, woli i interesów, które są podstawą demokracji bezpośredniej i stają się naturalnym środowiskiem wymiany poglądów grup reprezentujących swoje interesy, profesje, pasje, idee, potrzeby konsumenckie itp.²¹

18 J. Hofmokl, *Internet jako nowe dobro wspólne*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2009, s. 14–15.

19 L. W. Zacher, *Globalne rządzenie i globalne społeczeństwo obywatelskie*, [w:] *Transformacje demokracji...*, dz. cyt., s. 396.

20 Tamże, s. 398.

21 A. Szulak, *Demokracja informacyjna*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: A–M, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019, s. 278; zob. też: A. Motyko, *Model technokratyczny demokracji informacyjnej. Osobliwości i problemy stosowania*, „Historia i Polityka” 2014, nr 11 (18), s. 107–116. Istnieje jednak obawa, że komunikacja sieciowa staje się niezbędną głównie dla władzy,

Lech W. Zacher dostrzega możliwość podjęcia takiej globalnej współpracy także w powstających na świecie grupach protestu, w aktywizmie technonaukowym obywateli, w „sądach nauki” i „sklepiach nauki”, w badaniach naukowych ukierunkowanych na rozwój społeczności itd.²² Na tej samej zasadzie Ulrich Beck pokłada nadzieję w światowych wspólnotach ryzyka (lub w światowych wspólnotach strachu, niebezpieczeństw), które mogą powstrzymać zagrożenia powstające jako skutki uboczne rozwoju cywilizacyjnego²³. Wspólnoty te łączy solidarność wynikająca z lęku i na tym lęku opiera się ich siła polityczna. Jednak, jak zaznacza Beck, strach nie jest podstawą racjonalnego działania, a więc trudno na nim budować stabilną politykę, tym bardziej że „wspólnota strachu może być [w każdej chwili – przyp. aut.] rozproszona przez lekki powiew antyinformacji”²⁴. Ponadto manipulowanie strachem pozwala na usprawiedliwienie dążenia państwa do wprowadzenia autorytarnych rządów, inwigilacji i unieważnienia podstawowych zasad demokracji w imię obrony społeczeństwa przed niebezpieczeństwem.

W takich warunkach „hakowanie ludzi” staje się normalnością. Julia Angwin łączy je z możliwością namierzenia podmiotu w każdej chwili, podglądania go w domu, niemożnością ukrycia przez podmiot czegokolwiek, możliwością podszycia się pod niego lub wykorzystania finansowego, a także wystąpienia nadużyć tzw. okazania policyjnego (gdy podmiot bez powodu jest kierowany przed funkcjonariuszy policji) czy wpadnięcia w pułapkę „korytarza luster” (zaspokajanie przez firmy potrzeb klientów, nawet jeżeli nabywcy jeszcze nie wiedzą, jakie one są, co oznacza szufladkowanie konsumentów ograniczające ich swobodę)²⁵. Żyjemy więc w czasach, w których bezpieczeństwo człowieka coraz bardziej zależy od bezpieczeństwa informacji o nim, od możliwości ochrony przed nieuprawnionym dostępem do informacji świadczących o jego tożsamości, a także od umiejętności zarządzania tym bezpieczeństwem. Patrząc z tej perspektywy, Wiesław Babik dostrzega konieczność obrony cyfrowego odbiorcy przed zmasowanym atakiem na jego percepcję,

a niekompetentne technologicznie masy w dyskursie tym będą zmuszone zdać się na wąską merytokratyczną elitę, która będzie reprezentować ich interesy.

²² L.W. Zacher, *Nauka i technika jako obszar eksperymentów i praktyk partycypacyjnych*, [w:] *Transformacje demokracji...*, dz. cyt., s. 116–118.

²³ U. Beck, *Społeczeństwo światowego ryzyka. W poszukiwaniu utraconego bezpieczeństwa*, tłum. B. Baran, Wydawnictwo Naukowe Scholar, Warszawa 2012, s. 319; tenże, *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, tłum. S. Cieśla, Wydawnictwo Naukowe Scholar, Warszawa 2002, s. 64–65, 348.

²⁴ Tamże, s. 65.

²⁵ J. Angwin, *Społeczeństwo nadzorowane. W poszukiwaniu prywatności, bezpieczeństwa i wolności w świecie permanentnej inwigilacji*, tłum. Kurhaus Publishing, Kurhaus Publishing, Warszawa 2017, s. 26.

a także potrzebę uchronienia go przed zachowaniami ryzykownymi wynikającymi z demontażu norm etycznych, konsumpcjonizmu, lansowania modelu presumpcji. Nieustanny ruch i przeciążenie informacyjne wywołują stany napięcia i ciągłego stresu informacyjnego, utrudniają adaptację i autorefleksję, co oznacza, że trudno budować środowisko bezpieczeństwa „bez bezpiecznej informacji, częstego komunikowania i spotykania się ludzi oraz budowania wzajemnego zaufania i zaufania do informacji”²⁶. Powyższe prowadzi do wniosku, że bezpieczeństwo informacyjne nie jest możliwe bez zagwarantowania bezpieczeństwa środowiska, w którym człowiek produkuje, upowszechnia i wykorzystuje informacje.

Uwrażliwienie na zagrożenia generowane przez cywilizację cyfrową staje się cechą nie tylko pożądaną w społeczeństwie, ale wręcz niezbędną do ograniczania jego podatności na niebezpieczne zachowania w infosferze i obrony przed działaniami dezinformacyjnymi wymierzonymi w społeczny ład informacyjny. Do walki tej należy się przygotować. W tym celu konieczna jest ciągła i powszechna edukacja społeczeństwa w zakresie zagrożeń stwarzanych przez cywilizację cyfrową i problemów dotyczących bezpieczeństwa informacyjnego. Rozwijanie świadomości społeczeństwa i wyczulanie go na zachowania zagrażające bezpieczeństwu informacyjnemu państwa należy do zadań priorytetowych. Kultura bezpieczeństwa informacyjnego w znaczącym stopniu przyczynia się do podnoszenia poziomu bezpieczeństwa informacyjnego kraju. Można uznać, że zgodnie z koncepcją Donalda Marchanda składają się na nią wszystkie elementy – świadomość podmiotu bezpieczeństwa, wartości i postawy umożliwiające budowanie środowiska bezpieczeństwa – zachowania będące gwarancją utrzymania stanu bezpieczeństwa, które wpływają na bezpieczeństwo zarządzania informacją oraz odnoszą się do sposobu, w jaki informacja jest postrzegana, tworzona i wykorzystywana²⁷.

Kulturę bezpieczeństwa informacyjnego, posiłkując się definicją Mariana Cieślarczyka oraz wyjaśnieniem terminu „kultura informacyjna”, które zaproponowałam w jednej z prac, można określić jako sferę aktywności człowieka kształtowaną przez świadomość informacyjną i sposób myślenia o bezpieczeństwie; wartości, normy i reguły wspierające potrzebę podwyższenia poziomu kultury bezpieczeństwa pozwalającej dostrzegać wyzwania, szanse i zagrożenia w lokalnej i globalnej przestrzeni informacyjnej; postawy wpływające na uwrażliwienie społeczeństwa

²⁶ W. Babik, *Bezpieczeństwo informacji wyzwaniem dla bezpieczeństwa lokalnego*, [w:] *Elementy teorii i praktyki transdyscyplinarnych badań problemów bezpieczeństwa*, t. 7: *Teoretyczne i formalne aspekty bezpieczeństwa w wymiarze lokalnym*, A. Filipek, D. Krzewniak (red.), Wydawnictwo UPH, Siedlce 2018, s. 118.

²⁷ M. Sumiński, *Kultura informacyjna: przegląd teorii oraz potencjalne problemy badawcze*, [w:] *Wyzwania i perspektywy współczesnego zarządzania. Innowacje, kryzys, przedsiębiorczość*, t. 1, K. Łukasik (red.), Politechnika Częstochowska, Częstochowa 2013, s. 68.

na znaczenie bezpieczeństwa i kształtowanie zachowań charakterystycznych dla dojrzałych informacyjnie użytkowników infosfery współodpowiedzialnych za to bezpieczeństwo²⁸. Zachowania te wynikają ze współdziałania wymienionych powyżej komponentów kultury bezpieczeństwa. Odnoszą się one do przedmiotów i innych wytworów związanych z bezpieczeństwem informacyjnym i uczestnictwem podmiotów w procesie informacyjnym.

Komponenty kultury bezpieczeństwa informacyjnego o charakterze mentalnym (wartości, normy, zasady), materialnym (infrastruktura informacyjna) i organizacyjnym (działania, regulacje prawne, procedury, polityki bezpieczeństwa informacyjnego, struktury) przenikają się, a kultura informacyjna łączy je także w odniesieniu do poszczególnych sektorów bezpieczeństwa, takich jak bezpieczeństwo ekologiczne, zdrowotne, polityczne, społeczne, technologiczne, kulturowe itd. Kluczowym komponentem tej kultury jest kultura informacyjna i rozwijane przez nią kompetencje informacyjne. Nie ograniczają się one do umiejętności rozpoznawania potrzeb informacyjnych, lokalizowania i oceny, zastosowania i tworzenia informacji w kontekście edukacyjnym. Są to także kompetencje mające zasadnicze znaczenie dla uzyskiwania przewagi konkurencyjnej osób, przedsiębiorstw, regionów i narodów, wykraczające poza obecne technologie i obejmujące uczenie się, krytyczne myślenie i umiejętności interpretacyjne. Oznaczają posiadanie specyficznego rodzaju wiedzy wykorzystywanej we wszystkich sferach życia indywidualnego i społecznego do refleksyjnego podejmowania decyzji oraz stanowią podstawowy warsztat pracy dla specjalistów od zarządzania bezpieczeństwem informacyjnym. Transformując wniosek Wiesława Babika na temat relacji łączących kulturę informacyjną z *information literacy*, można uznać, że bez kultury informacyjnej trudno jest kształtować kulturę bezpieczeństwa informacyjnego współczesnego człowieka. Kultura informacyjna i kultura bezpieczeństwa informacyjnego przenikają się i wzajemnie uzupełniają, żadnej z nich nie można analizować oddzielnie, przedmiotem obu jest człowiek funkcjonujący w przestrzeni informacyjnej, który może być przyczyną zagrożenia dla bezpieczeństwa informacji i infosfery, ale też sam wymaga ochrony przed niekorzystnym oddziaływaniem informacji i dychotomicznego środowiska informacyjnego (rzeczywistego i wirtualnego)²⁹.

28 M. Cieślarczyk, *Kultura informacyjna jako element kultury bezpieczeństwa*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym – teoria i praktyka*, t. 1, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2015, s. 22; H. Batorowska, *Od alfabetyzacji informacyjnej do kultury informacyjnej. Rozważania o dojrzałości informacyjnej*, Wydawnictwo SBP, Warszawa 2013, s. 81–82.

29 W. Babik, *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014, s. 63; tenże, *Kultura informacyjna – spojrzenie z punktu widzenia ekologii informacji*, „Bibliotheca Nostra” 2012, nr 2 (28), s. 32.

Komponentami kultury bezpieczeństwa informacyjnego są również: kompetencje komunikacyjne, kompetencje międzykulturowe, umiejętność postępowania z ryzykiem i odpowiedzialność za nie, kompetencje technologiczne i cyfrowe, a także etyka informacyjna, prawo informacyjne, ekologia informacji, wychowanie do mass mediów i wychowanie do informacji, polityka informacyjna, profilaktyka informacyjna itd. Przenikają się one z wyznacznikami innych informacyjnych komponentów kultury bezpieczeństwa³⁰. Kształcenie kompetencji obchodzenia się z lękiem i niepewnością oraz funkcjonowania w społeczeństwie ryzyka pozwala na racjonalne wykorzystanie wiedzy o zagrożeniach generowanych przez cywilizację technologiczną, w tym o zagrożeniach związanych z atakami cyberterrorystycznymi i wojną informacyjną. Z kolei kształcenie kompetencji obywatelskich i współżycia społecznego przygotowuje jednostkę do przeciwstawiania się sterowanym działaniom popierającym i pielęgnującym niewiedzę tłumu. Uczenie kompetencji informacyjno-medialnych wykształca umiejętność samodzielnego doboru źródeł informacji i własnej refleksji nad treścią komunikatów, stając się podstawowym narzędziem zapewniania bezpieczeństwa informacyjnego i medialnego. Z kolei rozwijanie kompetencji międzykulturowych i wielokulturowych daje możliwość rozumienia innych ludzi i nieulegania wpływowi podmiotów szerzących szowinizm, a poprzez to wzmacnia odporność na manipulację. Rozwijanie kompetencji komunikacyjnych, umiejętności negocjacji, prowadzenia dialogu, rozwiązywania konfliktów, wzajemnego poznawania swoich racji wymaga umiejętności analizy i syntezy danych, uogólniania i interdyscyplinarnego podejścia do pozyskanych informacji.

Aby postulaty te zostały spełnione, konieczne jest dążenie do wychowania dojrzałych informacyjnie obywateli, bo tylko takie osoby są w stanie stworzyć kulturę bezpieczeństwa informacyjnego. Dojrzałość wymaga od nich refleksyjności, otwartości, racjonalności, odpowiedzialności, pracowitości, inteligencji, mądrości, generatywności, relatywizmu, transcendencji, mądrości, samokrytycyzmu i etyczności³¹. Dojrzałość informacyjna podmiotu jest warunkiem uzyskania nie tylko wysokiego poziomu kultury bezpieczeństwa informacyjnego, ale też kultury bezpieczeństwa w ogóle. Edukację w tym zakresie należy traktować jako narzędzie umożliwiające świadome uczestnictwo w życiu społecznym oraz przygotowujące do odgrywania w nim obranej roli, jest więc ona środkiem w dążeniu do osiągnięcia wysokiego stopnia przystosowania społecznego i odpowiedzialności za rozwój i bezpieczeństwo przestrzeni, w której podmiot funkcjonuje.

Uogólniając, można stwierdzić, że obszarem zainteresowań badaczy kultury bezpieczeństwa informacyjnego są głównie problemy:

³⁰ Zob. rysunki: 14, 16–18, 20–21.

³¹ H. Batorowska, *Od alfabetyzacji...*, dz. cyt., s. 36.

- dbania o rozwój świadomości bezpieczeństwa informacyjnego w społeczeństwie,
- pozyskiwania wiedzy o zagrożeniach generowanych przez cywilizację cyfrową,
- odpowiedzialności za utrzymywanie stanu bezpieczeństwa w infosferze,
- pielęgnowania wartości, na których można budować bezpieczeństwo jednostki i narodu oraz kształtować kulturę bezpieczeństwa i mocy,
- kształtowania postaw ludzi wobec problemów bezpieczeństwa informacyjnego, wpływania na ich emocje związane z dążeniem do przeciwdziałania zagrożeniom i wzmacniania więzi pozwalających na zwiększenie odporności na ataki informacyjne,
- kształtowania zachowań, które sprzyjają budowaniu poczucia bezpieczeństwa informacyjnego i niwelowaniu stanów zagrożenia,
- ochrony człowieka przed jego uprzedmiotowieniem w środowisku walki informacyjnej i postprawdy,
- zrównoważonego rozwoju człowieka w świecie cywilizacji cyfrowej i kultury,
- rozwijania kompetencji informacyjnych,
- dbania o bezpieczeństwo informacyjne i medialne,
- zarządzania bezpieczeństwem informacji w środowisku informacyjnym.

Przesłaniem tej książki jest stwierdzenie, że podmiot nie będzie mógł osiągnąć zadowalającego poziomu bezpieczeństwa, jeżeli nie będzie czuł się bezpiecznie w otaczającym go środowisku informacyjnym. Refleksję tę należy rozszerzyć o wniosek Józefa Oleńskiego, według którego „jakość środowiska informacyjnego determinuje bezpieczeństwo i suwerenność kraju we wszelkich innych dziedzinach życia politycznego, społecznego i ekonomicznego”³². Badacz, dostrzegając szczególne zagrożenie naszego kraju obserwowanymi w globalnej przestrzeni atakami informacyjnymi podejmowanymi przez podmioty dążące do dominacji politycznej, ekonomicznej i społecznej, szczególnie w narastającej atmosferze antypolonizmu, widzi konieczność przeciwstawienia się tym atakom, „by obronić suwerenność i jakość nie tylko środowiska informacyjnego, ale – w dłuższym okresie – suwerenność polityczną kraju”³³.

*

Przedstawione powyżej zagadnienia znalazły swoje rozwinięcie w książce. Podzielono ją na osiem rozdziałów traktujących o środowisku informacyjnym

³² J. Oleński, *Zarządzanie bezpieczeństwem infrastruktury informacyjnej w globalnej cyberprzestrzeni*, [w:] *Zarządzanie informacją*, dz. cyt., s. 552–553.

³³ Tamże, s. 553.

współczesnego człowieka, kontekstach pozyskiwania przewagi informacyjnej i służbach zajmujących się pozyskiwaniem informacji i pośredniczeniem w jej przekazywaniu, a także o komponentach kultury bezpieczeństwa informacyjnego i jej znaczeniu dla zachowania zrównoważonego rozwoju podmiotu w środowisku informacyjnym. W rozdziale I ukazano współczesne środowisko walki o przewagę informacyjną, dokonując próby uporządkowania terminologii naukowej odnoszącej się do środowiska informacyjnego i infosfery, opisując pojęcia zarówno z perspektywy informatologii (nauki o informacji), jak i nauk o bezpieczeństwie. W obu domenach wyeksponowano podejście procesowo-systemowe, starając się zróżnicować procesy informacyjne charakterystyczne dla systemów informacyjno-wyszukiwawczych i systemów decyzyjnych. Elementem łączącym oba podejścia jest proces zarządzania informacją, którego integralną częścią jest zarządzanie bezpieczeństwem informacyjnym. Kompetencje w tym zakresie są nieodzowne w kształtowaniu kultury bezpieczeństwa informacyjnego, stanowiąc równocześnie komponent kultury bezpieczeństwa nierozdzielnie związanej z kulturą informacyjną i ekologią informacji.

Dlatego w rozważaniach nad kulturą bezpieczeństwa informacyjnego uwzględniono dwie perspektywy i uznano je za konieczne z uwagi na interdyscyplinarny charakter badań nad bezpieczeństwem informacyjnym³⁴. Równocześnie prowadzona w środowisku naukowym dyskusja nad szerokim rozumieniem bezpieczeństwa informacyjnego – nieograniczającym się tylko do ochrony danych oraz urządzeń i systemów odpowiedzialnych za ich gromadzenie i przechowywanie – sprzyja rozszerzeniu obszaru badań nad kulturą bezpieczeństwa informacyjnego. Informatologia jako dyscyplina nauk społecznych zajmuje się zjawiskami informacyjnymi zachodzącymi w świecie społecznym, głównie transferem wiedzy w kontekście kulturowym i społecznym³⁵. Przeprowadzona przez Barbarę Sosińską-Kalatę analiza bibliometryczna problematyki badań omawianych na łamach trzech światowych czasopism z zakresu nauki o informacji dowodzi, że głównymi obszarami badawczymi tej domeny są:

- architektura informacji,
- badania użytkowników informacji,
- ekonomia informacji i e-gospodarka,
- komunikacja naukowa,
- polityka informacyjna,

34 H. Batorowska, *The Informatological Context of Safety Culture*, „Przegląd Biblioteczny” 2019 (Special Issue), s. 35.

35 B. Sosińska-Kalata, *Obszary badań współczesnej informatologii (nauki o informacji)*, „Zagadnienia Informatologii – Studia Informacyjne” 2013, t. 51, nr 2 (102), s. 35–36.

- zarządzanie informacją i wiedzą,
- nauka o informacji,
- organizacja wiedzy,
- usługi informacyjne,
- technologia informacyjna,
- społeczny Web,
- źródła informacji i ich jakość.

Ponieważ rozwój nauk o bezpieczeństwie jest – jak zaznacza Leszek F. Korzeniowski – ściśle związany z absorbowaniem dorobku poszczególnych dyscyplin i dziedzin, których przedmiotem są różne aspekty bezpieczeństwa człowieka, włączenie do tego obszaru informatologii wydaje się w pełni uzasadnione. Szczególnie dotyczy to jej problematyki odnoszącej się do: kultury informacyjnej, ekologii informacji, zagrożeń generowanych przez cywilizację cyfrową (takich jak stres informacyjny, choroby informacyjne, uzależnienia medialne, potop informacyjny, przeciążenie informacyjne itp.), a także zniekształcenia informacyjnego, zachowań informacyjnych, ewaluacji źródeł informacji, audytu informacji, kultury organizacyjnej i polityki informacyjnej. Włączenie do nauk o bezpieczeństwie zagadnień bezpieczeństwa informacyjnego oraz konieczność uwzględnienia ich jako odrębnej specjalności naukowej w tym obszarze postuluje wielu badaczy i ekspertów zajmujących się tą dziedziną³⁶. Przychylam się do stanowiska Korzeniowskiego, według którego:

bezpieczeństwo jako przedmiot badań, podejście holistyczne i dialektyczne, przekraczanie granic, wieloaspektowość i wykorzystywanie metodologii różnych nauk (podobnie jak w naukach o zarządzaniu) staje się wyznacznikiem tożsamości nauki o bezpieczeństwie [...], oznacza dostrzeżenie i respektowanie nierozzerwalnych związków między psychospołecznymi, ekonomicznymi, techniczno-wytwórczymi i innymi aspektami rozwoju człowieka i funkcjonowania organizacji stanowiących przedmiot badań nauk o bezpieczeństwie i prowadzi do nowej syntezy i oryginalnych wniosków³⁷.

Nauka o informacji, na co zwrócił uwagę Ryszard Szpyra, jest dyscypliną analizującą problemy przepływu informacji w społeczeństwie, a więc zajmującą się systemami informacyjnymi i zarządzaniem informacją³⁸. W tym kontekście

³⁶ K. Liderman, *Bezpieczeństwo informacyjne. Nowe wyzwania*, PWN, Warszawa 2017, s. 12.

³⁷ L.F. Korzeniowski, *Podstawy nauk o bezpieczeństwie. Zarządzanie bezpieczeństwem*, Difin, Warszawa 2012, s. 71–72.

³⁸ R. Szpyra, *Operacje informacyjne państwa w działaniach sił powietrznych. Rozprawa habilitacyjna*, AON, Warszawa 2002, s. 38.

można za Katarzyną Materską odnieść pole badawcze informatologii do informacji w określonym środowisku (gospodarczym, politycznym, naukowym, edukacyjnym, kulturalnym, organizacyjnym, bezpieczeństwa, sieciowym, indywidualnym) oraz do procesów z nią związanych. Efektywne zarządzanie informacją oraz wiedzą nie jest według badaczki możliwe:

bez znajomości ich cech, własności i funkcji, które bada nauka o informacji [informatologia – przyp. aut.], bez obserwacji potrzeb i zachowań informacyjnych danej organizacji oraz indywidualnych użytkowników informacji, bez świadomości faktycznego i pożądanego stanu wiedzy indywiduum czy społeczności, wreszcie bez badań nad tworzeniem i wykorzystywaniem wiedzy³⁹.

W rozdziale II zwrócono uwagę na integrację problemów walki o przewagę informacyjną z procesem informacyjnym. Ukazano, że na każdym z jego etapów może dochodzić do ataków informacyjnych, ponieważ wszystkie elementy procesu społecznej komunikacji (gromadzenie, przechowywanie, opracowywanie, wyszukiwanie, przetwarzanie, generowanie, udostępnianie, prezentowanie informacji itd.) podatne są na jakieś formy wpływania na integralność informacji wprowadzonej do systemu informacyjnego. Walka o przewagę informacyjną nad jednostką czy grupą niedoinformowaną – pozbawioną dostępu do informacji lub zmanipulowaną – to tylko jedna strona analizowanego zagadnienia, odnosząca się do istnienia tzw. kooperacji negatywnej. Walka o cenne informacje prowadzona jest bowiem także w celu niesienia pomocy innym, wspierania ich, samorozwoju, dla dobra publicznego – stanowi wówczas cel działań kooperacji pozytywnej, nastawionej na współpracę, doskonalenie, rozwój, ochronę, profilaktykę. Walka o informacje w kontekście kooperacji pozytywnej lub kooperacji negatywnej pozwala na postrzeganie pojęcia walki informacyjnej w jego szerokim lub wąskim rozumieniu (rozdział III). Nie oznacza to, że walkę informacyjną w jej wąskim rozumieniu należy utożsamiać jedynie z wojną informacyjną. Niemniej stanowi ona podstawowy komponent wojny informacyjnej prowadzącej do destrukcji, chaosu i zniszczenia.

Fenomen wojny informacyjnej nie jest jednak przedmiotem rozważań prowadzonych w niniejszej książce. Stanowi go informacja będąca instrumentem poszukiwania przewagi, której specyficzne cechy ujawniły się w obliczu nadmiarowości komunikatów adresowanych do społeczeństwa żyjącego w środowisku permanentnego ryzyka i niepewności, co opisano w rozdziale IV. Ludzkość uzależniła się od technologii, a przyspieszenie technologiczne spotęgowało zjawisko nadmiarowości

³⁹ K. Materska, *Zarządzanie informacją i wiedzą*, [w:] *Nauka o informacji*, W. Babik (red.), Wydawnictwo SBP, Warszawa 2016, s. 360.

bodźców informacyjnych, wzmogło presję czasu, potrzebę natychmiastowego wyboru wiążącego się z większym ryzykiem, ciągłej rywalizacji, presję sukcesu, potrzebę aprobaty postępowania głoszonego przez środowisko i media. W monografii przedstawiono konteksty pozyskiwania przewagi za pomocą informacji, związane z przypisaniem jej określonej roli, jaką może odgrywać w społeczeństwie, opisanej metaforycznie jako: fetysz społeczeństwa (nie)wiedzy, patogen infosfery, broń masowej manipulacji, tworzywo inwigilacji i kapitał wywiadu konkurencyjnego.

Podmiotom nieradzącym sobie z nadmiarem informacji i mającym problemy z wyborem komunikatów pochodzących z nieuwiarygodnionych źródeł, o różnej wartości i aktualności, przychodzą z pomocą służby wspomagające procesy decyzyjne, np. służby infobrokerskie, służby pracowników informacji i dokumentacji, służby analityczne, służby wywiadowcze (rozdział V). Ekspersi od analizy informacji doskonałą narzędzia i metody przetwarzania informacji i danych, wykorzystując w tym celu najnowsze technologie informatyczno-komunikacyjne oparte na sztucznej inteligencji. Pozyskują informacje zarówno z jawnych, jak i niejawnych źródeł, uprawiając tzw. biały, szary i czarny wywiad. Przygotowują dla decydentów i kadry zarządczej wysokiej jakości spersonalizowane produkty analityczne (wywiadowcze). W zglobalizowanej i usieciowionej gospodarce, w społeczeństwie ryzyka, konfliktów i katastrof, w środowisku zdominowanym przez informacje decydenci będą zmuszeni w coraz większym stopniu korzystać z zaplecza analitycznego i doradczego. Zespoły specjalistów w tej dziedzinie muszą mieć świadomość współodpowiedzialności za podejmowane na podstawie efektów swojej pracy decyzje, które coraz częściej będą miały charakter strategiczny dla firmy, organizacji, narodu, ludzkości. Należy wziąć pod uwagę, że w rękach analityków, ekspertów od zarządzania informacją i wiedzą, netokratów zatrudnionych w służbach analitycznych leży bezpieczeństwo poszczególnych państw oraz bezpieczeństwo międzynarodowe⁴⁰.

W rozdziale VI przedstawiono informacyjne komponenty kultury bezpieczeństwa, wskazując na jej ważną rolę w społeczeństwie światowego ryzyka. Scharakteryzowano wybrane elementy kultury bezpieczeństwa, eksponując jej związek z kulturą informacji pojmowaną przez Małgorzatę Kisilowską jako „sposób świadomego i aktywnego funkcjonowania człowieka w przestrzeni informacyjnej oraz jego konsekwencje”⁴¹, kulturą informacji skoncentrowaną na analizie działań, jakie podejmuje podmiot w stosunku do informacji, a także z kulturą informacyjną, w której równie ważne jest ustalenie wpływu informacji na działania człowieka

⁴⁰ H. Batorowska, *Analityk w środowisku walki o dominację i przetrwanie*, [w:] *Walka informacyjna. Uwarunkowania – Incydenty – Wyzwania*, H. Batorowska (red.), Uniwersytet Pedagogiczny im. KEN w Krakowie, Kraków 2017, s. 193.

⁴¹ M. Kisilowska, *Kultura informacji*, Wydawnictwo SBP, Warszawa 2016, s. 42, 79.

i analiza konsekwencji jego zachowań wynikających z funkcjonowania w środowisku nadmiaru informacji i przyspieszenia technologicznego. Do informacyjnych komponentów kultury bezpieczeństwa zaliczono:

- kulturę informacyjną odpowiedzialną za profilaktykę zagrożeń cywilizacji cyfrowej,
- ekologię informacji, której przedstawiciele działają na rzecz obrony infosfery,
- kulturę bezpieczeństwa informacyjnego mającą wpływ na zwalczanie podatności podmiotu na ataki informacyjne i łączącą się z nią kulturę bezpieczeństwa medialnego kształtowaną w ramach edukacji medialnej, dzięki której możliwe jest budowanie środowiska bezpieczeństwa medialnego,
- kulturę organizacyjną wpływającą w zasadniczy sposób na bezpieczeństwo informacji w organizacji i biznesie dzięki kształtowaniu i promowaniu zachowań zgodnych z przyjętą przez organizację polityką bezpieczeństwa informacyjnego,
- politykę informacyjną uprawianą przez decydentów, której odzwierciedleniem jest społeczny ład informacyjny.

Analiza wybranych informacyjnych komponentów kultury bezpieczeństwa pozwala dostrzec relacje, jakie łączą nauki o bezpieczeństwie z nauką o informacji, oraz wskazuje możliwość opisania jej z perspektywy informatologicznej (rozdział VII). Interdyscyplinarność domeny kultury bezpieczeństwa informacyjnego, ujętej z perspektywy nauk o bezpieczeństwie i informatologii, pozwala na podkreślenie znaczenia informacyjnych komponentów kultury bezpieczeństwa w kształtowaniu środowiska walki informacyjnej i równoważeniu działań kooperacji negatywnej działaniami podejmowanymi w ramach kooperacji pozytywnej. Książkę kończą rozważania na temat znaczenia kultury bezpieczeństwa informacyjnego w zwalczaniu podatności społeczeństwa na różne wpływy infoagresorów (rozdział VIII). Uodpornienie społeczeństwa na te ataki łączy się z odpieraniem szkodliwych działań skierowanych przeciw narodowi, jego świadomości, jedności, kulturze, tożsamości, wolności. Kultura bezpieczeństwa informacyjnego jest środkiem obrony przed walką informacyjną prowadzoną przeciw podmiotom o niskim poziomie kultury informacyjnej. Łączy się ściśle z potrzebą kształtowania powszechnej świadomości informacyjnej społeczeństwa. Poczucie bezpieczeństwa informacyjnego jednostki w warunkach permanentnej walki informacyjnej jest podstawą budowania ładu społecznego. Poczucie to nie jest jednak cechą przypisaną całemu społeczeństwu.

Kultura bezpieczeństwa informacyjnego może stać się barierą wstrzymującą agresję informacyjną dzięki wyposażeniu każdego obywatela w odpowiednie kompetencje informacyjne, technologiczne i medialne oraz dzięki wykształceniu odpowiedniego systemu aksjologicznego pozwalającego przewyciężyć zagrożenia

generowane przez współczesną cywilizację technologiczną (m.in. nadmiarowość informacji, presję czasu, nowości, przymus wyboru, brak pewności podjętych decyzji, presję sukcesu). Działają one destrukcyjnie na wartości uniwersalne, na które zwraca uwagę Andrzej Pieczywok, wymieniając: podmiotowość i tożsamość człowieka, swobody obywatelskie, demokrację, tolerancję, możliwość samorealizacji, godność, odpowiedzialność itp.⁴² Oznacza to, że zestaw przyjętych i uznawanych przez podmiot bezpieczeństwa wartości ukierunkowuje jego działania, reguluje sposób postępowania i wpływa na kształtowanie postaw. Dlatego wychowanie do informacji musi być oparte nie tylko na wiedzy o informacji, lecz przede wszystkim na aksjologii zachowań związanych z uczestnictwem podmiotu w procesie informacyjnym.

Aby kulturę bezpieczeństwa informacyjnego wykorzystać do przeciwdziałania negatywnym skutkom walki o przewagę informacyjną, potrzebna jest powszechna edukacja społeczeństwa w obszarze bezpieczeństwa informacyjnego. Edukacja ta jest ściśle związana z edukacją informacyjno-medialną, edukacją w zakresie komunikacji społecznej, z kompetencjami wielokulturowymi w globalnym społeczeństwie informacyjnym, edukacją obywatelską wspartą wychowaniem do informacji⁴³.

*

Książkę wyposażono w dwa indeksy – osobowy i przedmiotowy⁴⁴ – ułatwiające poruszanie się po treści publikacji i odnalezienie tematów przedstawianych w różnych miejscach z różnych perspektyw. Do publikacji dołączono także obszerną bibliografię wskazującą związek pomiędzy dwoma dyscyplinami naukowymi zajmującymi się kulturą bezpieczeństwa informacyjnego – naukami o bezpieczeństwie i nauką o informacji – w różny, ale i konwergentny sposób. Odwołano się do ponad 600 pozycji autorstwa zarówno polskich, jak i zagranicznych badaczy. Wykaz ten można potraktować jako przewodnik dla osób pragnących spojrzeć na zagadnienie

⁴² A. Pieczywok, *Degradacja aksjologicznej kultury bezpieczeństwa człowieka*, „Zeszyty Naukowe WSOWL” 2011, nr 2 (160), s. 188, 192.

⁴³ H. Batorowska, *Kultura bezpieczeństwa w kontekście modelu edukacji medialnej, informacyjnej i cyfrowej (MEMIC)*, [w:] *Człowiek – Media – Edukacja*, J. Morbitzer (red.), Wyższa Szkoła Biznesu, Dąbrowa Górnicza 2021 [w druku]; P. Motylińska, *Profilaktyka i kształtowanie świadomości w zakresie bezpieczeństwa informacyjnego w środowisku nadmiarowości informacji*, [w:] *Bezpieczeństwo informacyjne i medialne...*, dz. cyt., s. 205.

⁴⁴ W opracowaniu indeksu przedmiotowego wykorzystano hasła przedmiotowe zawarte w publikacji: *Słownik języka haseł przedmiotowych nauk o bezpieczeństwie i obronności polsko-angielski*, G. Kolek i in. (oprac.), Centralna Biblioteka Wojskowa, AON, Warszawa 2012.

kultury bezpieczeństwa informacyjnego w środowisku walki o przewagę informacyjną z perspektywy nauki o informacji i nauk o bezpieczeństwie.

Podsumowując: celem podjętych przeze mnie badań było zwrócenie uwagi na potrzebę uwzględnienia nauki o informacji w refleksji badawczej poświęconej kulturze bezpieczeństwa informacyjnego. Ta ostatnia wymaga włączenia do badań takich komponentów, jak: kultura informacyjna, ekologia informacji, wychowanie do informacji, polityka informacyjna i kultura organizacyjna. Przyczyniają się one w dużym stopniu do osiągnięcia przez podmiot bezpieczeństwa dojrzałości informacyjnej. Bez dojrzałości tej nie można budować środowiska bezpieczeństwa informacyjnego w dłuższym okresie. Tych pięć komponentów stanowi dla badaczy eksplorujących zjawisko pośredniczenia w przepływie informacji od jej źródła do końcowego odbiorcy sedno procesu badawczego (stąd częste odwoływanie się do ich dorobku). W przestrzeni tej dochodzi do zakłóceń transferu informacji i wiedzy. Powstają one nie tylko ze względu na niedoskonałości infrastruktury informacyjno-komunikacyjnej, ale też w wyniku świadomych lub nieświadomych działań podejmowanych przez nadawców, odbiorców i dysponentów informacji. Te pierwsze związane są z celową aktywnością podmiotów, a drugie z ich naiwną ignorancją generującą zagrożenia dla całego środowiska informacyjnego.

Starałam się wskazać, że prowadzone przez informatologów badania nad kulturą informacyjną silnie łączą się z analizą środowiska informacyjnego człowieka i jego ekosystemu informacyjnego, z wypracowaniem odpowiednich modeli i standardów kompetencji informacyjnych, cyfrowych i medialnych oraz z wdrażaniem ich do polityki oświatowej, gwarantującej możliwość sprawnego korzystania przez społeczeństwo z technologii informacyjno-komunikacyjnych i usług dostępnych za ich pośrednictwem. Poprzez edukację informacyjną i pośredniczenie w dostępie do informacji przeciwdziałają wykluczeniu informacyjnemu, technologicznemu i społecznemu obywateli, podnosząc ich poziom aktywności zawodowej, politycznej, kulturalnej i społecznej. Natomiast zainteresowanie badaczy nauk o bezpieczeństwie kwestią kultury informacyjnej koncentruje się na przygotowaniu odpowiedzialnych podmiotów bezpieczeństwa do życia w społeczeństwie informacyjnym, w którym technologie informacyjne oddziałują na ich sposób postrzegania rzeczywistości, formułowania opinii, a w konsekwencji na podejmowanie decyzji wpływających na poziom bezpieczeństwa. Zatem badania nad kulturą informacyjną obywateli włączają się w dyskurs kultury bezpieczeństwa, a szczególnie bezpieczeństwa informacyjnego i kultury bezpieczeństwa informacyjnego. Nie ulega wątpliwości, że wiedza na temat informacji, zarządzania nią, mechanizmów pozyskiwania przewagi informacyjnej, istoty walki informacyjnej wzmacnia świadomość informacyjną podmiotów, a odpowiednia edukacja i wychowanie informacyjne rozwijają kompetencje etyczne i odpowiedzialność społeczną. Starałam się ukazać celowość

wydzielenia w kulturze bezpieczeństwa zagadnień kultury bezpieczeństwa informacyjnego analizowanych w kontekście wyżej wymienionych pięciu komponentów. Dążenie do przewagi coraz częściej związane jest z chęcią zapanowania i dominacji nad stroną konkurencyjną, pragnieniem ograniczenia jej wpływów, a w konsekwencji jej wyeliminowania i zniszczenia. Dokonuje się to za sprawą informacji, dostępu do niej, możliwości wykorzystania jej w odpowiednim momencie i w odpowiednim miejscu, umiejętności zafałszowania i zmylenia przeciwnika. Walka informacyjna toczy się na słowa, a słowa mają siłę rażenia nieograniczoną – dzięki sieciowym połączeniom ludzi uczestniczących w tej walce.

Istotnym celem badań było ukazanie, że w codziennej walce o informację – walce o pozyskiwanie przewagi, a nawet dominacji informacyjnej – kultura bezpieczeństwa informacyjnego ma do odegrania ważną rolę polegającą na powstrzymywaniu, eliminowaniu, ograniczaniu negatywnych skutków tej walki oraz wspieraniu zadań związanych z działaniami kooperacji pozytywnej na rzecz ochrony środowiska informacyjnego człowieka. W związku z tym edukacja dla bezpieczeństwa nie może być prowadzona bez włączenia do niej elementów edukacji informacyjnej i wychowania do informacji wpływających na jakość kultury bezpieczeństwa informacyjnego. Oznacza to, że cele informatologów i badaczy nauk o bezpieczeństwie są w tym obszarze wspólne. W związku z tym starano się przedstawić model transdyscyplinarnego podejścia do problemu badawczego, jakim jest kultura bezpieczeństwa informacyjnego, wykorzystujący dokonania naukowców reprezentujących obie dyscypliny, dotąd ze sobą niepowiązane. Zastosowana metoda badawcza związana z analizą krytyczną publikacji czołowych ekspertów reprezentujących oba obszary badawcze pozwoliła dostrzec, że kultura bezpieczeństwa informacyjnego może być tą siłą, która zapewni współczesnemu człowiekowi większe poczucie bezpieczeństwa w jego środowisku informacyjnym. Aby powstrzymać przemoc nierozzerwalnie związaną z dążeniem do osiągnięcia przewagi informacyjnej, konieczne są działania prewencyjne oparte na budowaniu kultury bezpieczeństwa informacyjnego.