DOCTRINA
Studia Społeczno-Polityczne 19/2022
PL ISSN 1730-0274

Recenzje / Reviews

Piotr Bączek
ORCID: 0000-0002-5432-1657
piotr13571@gmail.com
Akademia im. A. Gieysztora w Pułtusku
Filia Akademii Finansów i Biznesu Vistula

Po pierwsze, informacja...!

Włodzimierz Fehler, *Podstawy bezpieczeństwa informacyjnego*, Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce 2021, ss. 257

DOI: 10.34739/doc.2022.19.17

Od zarania dziejów informacja odgrywała istotną rolę w cywilizacji. W ostatnich dekadach jej znaczenie wzrosło jednak jeszcze bardziej. Jest to konsekwencja zmian technologicznych, komputeryzacji pracy, rozwoju mediów. Sieć teleinformatyczna, łącząc pojedyncze komputery, stała się podstawą stworzenia cyberprzestrzeni. Kolejna rewolucja technologiczna z przełomu XX/XXI wieku doprowadziła do powstania mediów nowego typu oraz jeszcze większego upowszechnienia procesów komunikacyjnych. Dzięki temu informacja oddziałuje na wiele sfer ludzkiej aktywności, m.in. na gospodarkę, kulturę, rozrywkę, politykę, naukę i bezpieczeństwo. Powstanie mediów społecznościowych umożliwia, pomimo barier lokalizacyjnych, kontakt w czasie rzeczywistym. Społeczeństwo informacyjne osiągnęło wymiar globalny. Właściwe obchodzenie się z informacją, zarządzanie nią i ochrona tej sfery są niezbędnymi warunkami osiągnięcia sukcesu. Informacja oraz wiedza stały się zasobami strategicznymi, które umożliwiają uzyskanie przewagi gospodarczej, naukowej, politycznej oraz poprawę bezpieczeństwa.

Z jednej strony informacja stała się dobrem, które wpływa na rozwój cywilizacyjny danego państwa, ale z drugiej jest również instrumentem walki. Współczesne środowisko informacyjne człowieka stało się globalne. Oprócz pozytywnych konsekwencji tego procesu (np. sposoby przechowywania informacji, metody jej prezentacji, dostęp do niej) są także negatywne. Infosfera została zainfekowana informacjami o niskiej jakości, nieużytecznymi, a także pod wieloma względami niebezpiecznymi. Jedną z przyczyn tej sytuacji jest tzw. „otwarty" internet[1]. Stwarza to nowe możliwości agresywnych i przestępczych działań. Informacja umiejętnie wykorzystywana może stać się groźną bronią skutecznie obezwładniającą przeciwnika. Metody wykorzystujące działania informacyjne (np. szpiegostwo, wprowadzanie w błąd, wywieranie wpływu psychologicznego) były stosowane od starożytności[2]. Już starochiński mędrzec Sun Tsu nauczał, że należy uzyskać o przeciwniku „uprzedzającą wiedzę" i powinna to być „konkretna informacja pochodząca od człowieka, który dobrze zna sytuację wroga"[3].

Aktualnie do źródeł takich informacji należą również m.in. media społecznościowe. Dzięki nim praca służb wywiadowczych przeniosła się na zupełnie inny poziom. Media nowego typu zawierają cenne zasoby informacyjne umożliwiające charakteryzowanie i profilowanie obiektów będących celem działań operacyjnych. Za pomocą tych mediów służby specjalne mogą również prowadzić operacje informacyjne o charakterze politycznym, militarnym i gospodarczym[4]. Od kilku lat eksperci wskazują, że upowszechnienie mediów społecznościowych jest wykorzystywane przez Federację Rosyjską. Państwo to dzięki grupom blogerów, trolli, hakerów oraz botów rozpowszechnia antyzachodnie treści, prowadzi intensywną ofensywę informacyjną w cyberprzestrzeni. Nabrała ona już cech kompleksowej polityki państwowej. Celem Rosji jest podsycanie strachu, niepewności, niezadowolenia społecznego oraz podważanie

[1] W. Babik, *Ekologia informacji*, Kraków 2014, s. 68.
[2] T.A. Kisielewski, *Uwaga szpieg! Dzieje wywiadu od Noego do Bonda*, Poznań 2018, s. 13-22; J. Piekałkiewicz, *Dzieje szpiegostwa*, Warszawa 1999, ss. 50-54; N. Polmar, T.B Allen, *Księga szpiegów. Encyklopedia*, Warszawa 2000, ss. IX-X, XIII.
[3] Sun Tzu, *Sztuka wojny*, Warszawa 1994, s. 140.
[4] B. Gałek, *Nowe instrumenty współczesnych operacji pozainformacyjnych*, „Doctrina. Studia Społeczno-Polityczne" 2018, nr 15, s. 72.

zaufania do NATO[5]. Logiczną konsekwencją tych zmian w środowisku bezpieczeństwa jest wzrost znaczenia informacyjnego wymiaru bezpieczeństwa.

Zagadnienia te są przedmiotem teoretycznych rozważań opublikowanej właśnie monografii Włodzimierza Fehlera *Podstawy bezpieczeństwa informacyjnego*[6]. Autor jest doktorem habilitowanym i nauczycielem akademickim na Wydziale Nauk Społecznych Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Specjalizuje się w problematyce bezpieczeństwa wewnętrznego, teorii bezpieczeństwa, polityki bezpieczeństwa. Jest autorem wielu prac z tego zakresu, m.in. monografii *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i praktyczne*[7]. Był również współredaktorem *Leksykonu Bezpieczeństwa Wewnętrznego*[8] oraz współautorem opinii dotyczącej konsekwencji rozwoju systemów sztucznej inteligencji dla sfery bezpieczeństwa i obronności w Polsce, sporządzonej 7 kwietnia 2021 r. dla Komisji Obrony Narodowej Sejmu RP (BAS-457/21A)[9].

W jego dorobku naukowym znajdują się również publikacje dotyczące bezpieczeństwa informacyjnego[10]. W najnowszej pracy W. Fehler kontynuuje ten wątek swoich zainteresowań badawczych. Monografia została podzielona na wstęp, cztery rozdziały merytoryczne i zakończenie. Dodatkowo zamieszczona została obszerna bibliografia[11], spis jedenastu tabel i pięciu rysunków[12] oraz streszczenie w językach polskim i angielskim[13]. Głównym problemem badawczym recenzowanej książki jest poszukiwanie odpowie-

[5] Eadem, *NATO jako cel rosyjskiej aktywności w środowisku informacyjnym państw bałtyckich*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2019, nr 2(5), s. 106-107.
[6] W. Fehler, *Podstawy bezpieczeństwa informacyjnego*, Siedlce 2021, s. 257.
[7] Idem, *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i praktyczne*, Warszawa 2012.
[8] *Leksykon Bezpieczeństwa Wewnętrznego*, red. W. Fehler, J.J. Piątek, R. Podgórzańska, Szczecin 2017.
[9] W. Fehler, A. Araucz-Boruc, A. Dana, A. Lasota-Kapczuk, *Systemy sztucznej inteligencji jako wyzwanie dla sfery bezpieczeństwa i obronności RP*, „Zeszyty Prawnicze" 2021, nr 2(70), s. 273-298.
[10] W. Fehler, *Informacyjny wymiar zagrożeń dla bezpieczeństwa współczesnej Polski*, „Przegląd Strategiczny" 2015, nr 8, s. 81-100; Idem, *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce 2016, s. 24-43.
[11] W. Fehler, *Podstawy bezpieczeństwa…*, s. 237-253.
[12] Ibidem, s. 255.
[13] Ibidem, s. 256-257.

dzi na następujące pytanie: „jak współcześnie powinniśmy rozumieć istotę bezpieczeństwa informacyjnego i jakie zasadnicze składniki wpływają na jego kształtowanie”[14]. Autor sformułował cztery dodatkowe problemy badawcze[15]. Przedstawił również cztery hipotezy szczegółowe[16]. W procesie badawczym zastosował takie metody badawcze, jak analiza, synteza, analogia i wnioskowanie[17].

Pierwszy rozdział recenzowanej monografii, zatytułowany *Informacja i jej znaczenie*, poświęcony jest rozważaniom dotyczącym pojęcia informacja. Autor analizuje szereg definicji tego terminu, choć jednocześnie zwraca uwagę, że w literaturze przedmiotu nie ma konsensusu w tym zakresie. Przytacza opinię włoskiego badacza filozofii informacji Luciano Floridi, że informacja wciąż jest złudnym pojęciem[18]. Rozdział ten kończy konstatacja, że zasoby informacyjne mogą być wykorzystywane do osiągania różnorodnych celów. Badacz podkreśla, że każdy zasób informacyjny danego podmiotu powinien być chroniony. Strategiczne zasoby informacyjne muszą być zabezpieczone szczególnie[19].

Głównymi problemami podejmowanego w ramach drugiego rozdziału, zatytułowanego *Społeczeństwo informacyjne*, są geneza oraz kolejne etapy rozwoju społeczeństwa informacyjnego. Autor zajmuje się istotą, cechami, funkcjami współczesnej cywilizacji opartej o przetwarzanie informacji. Przedstawia poglądy teoretyków, którzy wprowadzili do dyskursu naukowego termin „społeczeństwo informacyjne” oraz amerykańskich i europejskich przedstawicieli środowisk politycznych, zwracających uwagę na zachodzące zmiany cywilizacyjne[20]. Analizuje pozytywne konsekwencje powstania społeczeństwa informacyjnego dla wielu sfer ludzkiej aktywności, m.in. ekonomicznej, kulturowej, ekologicznej, politycznej, administracyjnej państwa, społecznej, ochrony zdrowia[21]. Zwraca również uwagę na wyzwania i zagrożenia związane z tymi przemianami. Podkreśla on jednak przy tym, że „rozwój społeczeń-

[14] Ibidem, s. 8.
[15] Ibidem, s. 9.
[16] Ibidem, s. 9-10.
[17] Ibidem, s. 10-11.
[18] Ibidem, s. 21-22.
[19] Ibidem, s. 64.
[20] Ibidem, s. 66-72.
[21] Ibidem, s. 81-84.

stwa informacyjnego wywołał i nadal generuje szereg zasadniczo korzystnych zmian w każdej dziedzinie życia społecznego i jednostkowego”[22]. Rozdział ten kończą rozważania dotyczące rozwoju sztucznej inteligencji i konsekwencji tego procesu dla infosfery.

W trzecim rozdziale, zatytułowanym *Zagrożenia i bariery informacyjne* W. Fehler podejmuje najważniejszą problematykę z punktu widzenia zapewnienia bezpieczeństwa informacyjnego jednostki i państwa. Rozdział ten jest zresztą najobszerniejszy, składa się z sześciu podrozdziałów i liczy aż 81 stron, czyli prawie 25 proc. objętości monografii[23]. Stanowi więc jej główną część. W pierwszym podrozdziale autor dokonuje scharakteryzowania zagrożeń informacyjnych oraz ich klasyfikacji. Konkludując tę część rozważań, badacz stwierdza m.in., że wielu ekspertów przedstawia właściwe projekty przeciwdziałania tym zdarzeniom, ale zbytnio pokłada nadzieje w działaniach jednostek, przy pomniejszeniu inicjatyw organów i instytucji państwa. W ocenie autora monografii nie jest możliwe ograniczenie współczesnych zagrożeń informacyjnych bez zaangażowania administracji państwowej[24].

W kolejnych pięciu podrozdziałach W. Fehler scharakteryzował zagrożenia informacyjne, które pogrupował w pięciu kategoriach: przestępstwa i przestępczość informacyjna, dezinformacja, walka informacyjna, wojna informacyjna oraz bariery informacyjne. W przypadku przestępstw i przestępczości informacyjnej badacz zwraca uwagę, że należy wprowadzić do obiegu naukowego terminy „przestępstwo informacyjne” oraz przestępczość informacyjna”. Katalog przestępstw dotyczących sfery informacyjnej jest bardzo rozległy. Są one uwzględnione w rozmaitych aktach prawnych, w związku z tym powinna zostać wyodrębniona nowa dziedzina nauk prawnych – „prawo informacyjne”[25]. W Europie Zachodniej taki proces autonomizacji prawa informacyjnego rozpoczął się już w latach 90. XX wieku[26]. W. Fehler twierdzi, że niezbędne jest przyjęcie terminu „przestępczość informacyjna” i określenie jego znaczenia. W ocenie badacza konieczne jest wypracowanie „zbiorczej

[22] Ibidem, s. 91.
[23] Ibidem, s. 109-190.
[24] Ibidem, s. 120-121.
[25] Ibidem, s. 122.
[26] Ibidem, s. 124.

formuły, obejmującej ogół czynów karalnych wymierzonych w prawo do informacji, obowiązki informacyjnej i ochronę informacji w różnych formach”[27].

Wysoce aktualne znaczenie posiadają rozważania dotyczące dezinformacji. Przeprowadzona charakterystyka tego zagrożenia może mieć praktyczny wymiar, zwłaszcza w kontekście np. rozpowszechniania fałszywych informacji po wybuchu epidemii COVID-19[28] oraz kampanii propagandowych podczas działań hybrydowych Białorusi na granicy z Polską[29]. Badacz na podstawie analizy krajowej i zagranicznej literatury przedmiotu formułuje własną definicję dezinformacji. Ocenia, że dezinformacja jest jednym „z najbardziej destrukcyjnych zagrożeń dla informacyjnego wymiaru bezpieczeństwa”[30]. Wskazując przy tym, że współcześnie dezinformacja może dotykać „praktycznie każdej sfery funkcjonowania podmiotów będących celem oddziaływań dezinformujących”[31]. Podkreśla m.in., że „zagrożenia generowane przez dezinformacje są w stanie wywierać negatywny wpływ na: funkcjonowanie i kształt systemów politycznych, nastroje, relacje i preferencje społeczne, podejście do problemów ekologicznych, sferę militarną i kulturową”[32].

Autor dokonuje rozróżnienia pojęć „walka informacyjna” i „wojna informacyjna”. Zwraca uwagę, że wiąże się to z wyodrębnieniem teoretycznych i praktycznych rozstrzygnięć m.in. w sztuce wojennej lub prawa wojennego[33]. Ostatnią grupą negatywnych zdarzeń informacyjnych analizowaną w tym rozdziale są bariery informacyjne, które związane są z ludzkimi zachowaniami informacyjnymi, które dotyczą m.in. wykształcenia, doświadczenia zawodowego, światopoglądu, pozycji zawodowej, środowiska zewnętrznego[34]. Bariery informacyjne powodują zakłócenia systemu komunikowania i obieg informacji. Stanowią one niezmienny element procesu

[27] Ibidem, s. 138.
[28] P. Bączek, *Kampanie dezinformacyjno-propagandowe jako rodzaj zagrożeń informacyjnych w sytuacjach kryzysowych na przykładzie pandemii choroby COVID-19*, „Security Review” 2020, nr 3(16), s. 3-14.
[29] W. Repetowicz, *Działania psychologiczno-dezinformacyjne kluczowe w ataku na Polskę [OPINIA]*, https://www.infosecurity24.pl/dzialania-psychologiczno-dezinformacyjne-kluczowe-w-ataku-na-polske-opinia (data dostępu: 14.11.2021).
[30] W. Fehler, *Podstawy bezpieczeństwa…*, s. 154.
[31] Ibidem, s. 155.
[32] Ibidem, s. 154.
[33] Ibidem, s. 177.
[34] Ibidem, s. 178-179.

kształtowania infosfery[35]. Jest to kolejny interesujący wkład autora w rozwój analizy problematyki bezpieczeństwa informacyjnego, gdyż dotychczas rozważania dotyczące barier informacyjnego były głównie ujmowane w takich gałęziach nauk, jak np. pedagogika, ekologia informacji, bibliotekoznawstwo, lingwistyka, socjologia, psychologia. Badacze tych zagadnień coraz częściej wskazują na związek barier informacyjnych z zagrożeniami powstałymi w wyniku przemian cywilizacyjnych[36].

Ostatni rozdział monografii nosi tytuł *Bezpieczeństwo informacyjne i bezpieczeństwo informacji*. Autor dokonuje w nim analizy pojęć „bezpieczeństwo informacyjne" oraz „bezpieczeństwo informacji". Słusznie podkreśla, że w aparacie pojęciowym związanym z tą kategorią bezpieczeństwa istnieje duże zamieszanie. Wskazują na to np. liczne definicje bezpieczeństwa informacyjnego, które ograniczają to zagadnienie do problemów ochrony informacji niejawnych lub bezpieczeństwa systemów teleinformatycznych[37]. W ocenie badacza płaszczyzną do rozwiązywania problemów związanych z zagrożeniami informacyjnymi, uwarunkowaniami bezpieczeństwa, racji stanu, strategicznych interesów danego państwa oraz efektywnymi koncepcjami postępowania jest polityka bezpieczeństwa informacyjnego tego państwa[38]. Taka polityka powinna zapewnić solidne podstawy dla bezpieczeństwa państwa oraz społeczeństwa[39]. Jej głównym kreatorem musi być państwo, ale powinny być w niej również uwzględnione działania podmiotów pozapaństwowych[40].

Na koniec monografii W. Fehler przedstawił wnioski wynikające z przeprowadzonych badań. Przeprowadzona analiza wskazuje, że temat istoty bezpieczeństwa informacyjnego jest coraz częściej podejmowany w literaturze przedmiotu, choć raczej w ujęciu hasłowym. Przeważają rozważania dotyczące problemów szczegółowych. Badacz stwierdził również, że istota bezpieczeństwa informa-

[35] Ibidem, s. 189.
[36] H. Batorowska, *Wybrane problemy kultury bezpieczeństwa, kultury informacyjnej i bezpieczeństwa informacyjnego w refleksji nad funkcjonowaniem człowieka w świecie informacji*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka. Tom II*, red. H. Batorowska, Z. Kwiasowski, Kraków 2016, s. 36.
[37] W. Fehler, *Podstawy bezpieczeństwa*..., s. 191.
[38] Ibidem, s. 211.
[39] Ibidem, s. 213.
[40] Ibidem, s. 214.

cyjnego jest zniekształcana przez uznanie za odrębną kategorię cyberbezpieczeństwa. Kolejnym wnioskiem wynikającym z badań jest uznanie, że brakuje teoretycznych prac z zakresu istoty bezpieczeństwa informacyjnego oraz systemów bezpieczeństwa informacyjnego. Autor skonstatował także, że istnieje „swoista inercja definicyjna" dotycząca pojęć ze sfery bezpieczeństwa informacyjnego (np. takich jak walka informacyjna, wojna informacyjna, polityka bezpieczeństwa informacyjnego, polityka bezpieczeństwa informacji). W ostatnim wniosku W. Fehler stwierdza, że istnieje deficyt konkretnych propozycji praktycznych zmian organizacyjnych, prawnych, instytucjonalnych. Na podstawie powyższych wniosków formułuje on kierunki dalszych badań obszaru bezpieczeństwa informacyjnego[41].

W związku z przeobrażeniami cywilizacyjnymi oraz coraz powszechniejszym wykorzystaniem broni informacyjnej w konfliktach hybrydowych zwiększyło się znaczenie bezpieczeństwa informacyjnego. Należy prognozować, że ta tendencja będzie ciągle wzrastała. Trawestując znane hasło wyborcze „Po pierwsze gospodarka, głupcze!" z kampanii prezydenckiej Billa Clintona[42], już niedługo będzie trzeba (a może nawet obecnie) zmienić to hasło na inne: „Po pierwsze informacja…". Recenzowana monografia pomaga zrozumieć te trendy cywilizacyjne i ich oddziaływanie na bezpieczeństwo jednostki, społeczeństwa i państwa.

W. Fehler zarysowuje merytoryczną i dobrze udokumentowaną płaszczyznę do analizy zmieniających się uwarunkowań i wymiany poglądów. Wskazuje i ocenia pojawiające się nowe wyzwania, bariery oraz zagrożenia informacyjne. Autor nie powiela standardowych opinii, konfrontuje opinie różnych badaczy, niejednokrotnie w sposób polemiczny. Na podstawie bogatego zestawu źródeł przedstawia własne wnioski. Istotną zaletą monografii są autorskie definicje pojęć z obszaru bezpieczeństwa informacyjnego. W. Fehler analizuje różnorodne aspekty bezpieczeństwa informacyjnego, charakteryzuje wyzwania, bariery i zagrożenia informacyjne, wskazuje przy tym obszary kolejnych rozważań. Pewien niedo-

[41] Ibidem, s. 233-234.
[42] R. Korzycki, *Gospodarka w USA kwitnie. Trump będzie walczył o drugą kadencję*, https://www.gazetaprawna.pl/wiadomosci/artykuly/1406269,usa-trump-bedzie-walczyl-o-druga-kadencje.html (data dostępu: 14.11.2021).

syt budzi brak szczegółowej analizy polskiego systemu bezpieczeństwa informacyjnego oraz pojawiających się w Polsce zagrożeń informacyjnych. Oczywiście jest to konsekwencja przyjętego przez autora założenia ogólnego charakteru rozważań. Daje to jednak asumpt do podjęcia w przyszłości badań również i w tym zakresie. Monografia, pomimo pominięcia tej problematyki, jest ważna właśnie ze względu na bieżące wydarzenia polityczne w regionie środkowoeuropejskim. Została ona opublikowana w okresie zaistnienia wydarzeń bezpośrednio wpływających na bezpieczeństwo informacyjne Polski, czyli operacji informacyjnych dotyczących m.in. epidemii COVID-19, kryzysu migracyjnego na granicy polsko-białoruskiej oraz tzw. afery mailowej. W związku z tym praca *Podstawy bezpieczeństwa informacyjnego* jest publikacją niezwykle aktualną, której walory teoretyczne powinny zostać zoperacjonalizowane w praktycznej działalności.

Tak jak zaznaczono, analizowana monografia ma charakter teoretyczny, ale może być również przydatna w praktyce organów państwa w zakresie zwalczania obecnych i przyszłych zagrożeń informacyjnych. Przedstawione w monografii treści stanowią wartościowe i dobrze udokumentowane źródło wiedzy, które z powodzeniem może być wykorzystane w procesie dydaktycznym, kolejnych badaniach naukowych oraz w przedsięwzięciach administracji odpowiedzialnej za sferę informacyjną. Dlatego książka powinna wzbudzić zainteresowanie środowisk naukowych, studentów kierunków związanych z bezpieczeństwem oraz praktyków zajmujących się zawodowo problematyką bezpieczeństwa państwa.

Wnioski wypracowane przez W. Fehlera mogą przyczynić się do wzbudzenia ożywionej dyskusji, a być może nawet do głosów polemicznych. Wydaje się, że obszarem takiego dyskursu może stać się krytyczne podejście autora do poglądów uznających cyberbezpieczeństwo za odrębny byt i sytuujących go poza tradycyjną sferą bezpieczeństwa informacyjnego. W ocenie badacza wydzielenie cyberbezpieczeństwa deformuje istotę informacyjnego wymiaru bezpieczeństwa i ogranicza go[43]. Konsekwencją tego rozumowania jest jednak uznanie, że zagrożenia informacyjne pojawiające się współcześnie w cyberprzestrzeni (np. cyberterroryzm, trolling, hakerstwo

[43] W. Fehler, *Podstawy bezpieczeństwa*..., s. 231, 233.

i inne przestępstwa komputerowe) również nie wymagają osobnej kategorii i powinny być stypizowane według dotychczasowych zasad. Takie podejście może jednak utrudnić oszacowanie nowych wyzwań oraz zagrożeń informacyjnych ze sfery wirtualnej, a w konsekwencji również przeciwdziałanie im. Niepodważalnym faktem jest jednak, że państwo nie wykreuje odpowiedniej i skutecznej polityki bezpieczeństwa bez właściwego określenia istoty bezpieczeństwa informacyjnego i potencjalnych zagrożeń. Rozważania W. Fehlera stanowią niezbędną pomoc w tych praktycznych pracach.

Bibliografia / References

Babik W., *Ekologia informacji*, Kraków 2014.

Batorowska H., *Wybrane problemy kultury bezpieczeństwa, kultury informacyjnej i bezpieczeństwa informacyjnego w refleksji nad funkcjonowaniem człowieka w świecie informacji*, [w:] *Kultura informacyjna w ujęciu interdyscyplinarnym. Teoria i praktyka. Tom II*, red. H. Batorowska, Z. Kwiasowski, Kraków 2016.

Bączek P., *Kampanie dezinformacyjno-propagandowe jako rodzaj zagrożeń informacyjnych w sytuacjach kryzysowych na przykładzie pandemii choroby COVID-19*, „Security Review" 2020, nr 3(16).

Gałek B., *NATO jako cel rosyjskiej aktywności w środowisku informacyjnym państw bałtyckich*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2019, nr 2(5).

Gałek B., *Nowe instrumenty współczesnych operacji pozainformacyjnych*, „Doctrina. Studia Społeczno-Polityczne" 2018, nr 15.

Fehler W., *Bezpieczeństwo wewnętrzne współczesnej Polski. Aspekty teoretyczne i praktyczne*, Warszawa 2012.

Fehler W., *Informacyjny wymiar zagrożeń dla bezpieczeństwa współczesnej Polski*, „Przegląd Strategiczny" 2015, nr 8.

Fehler W., *O pojęciu bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne w XXI wieku*, red. M. Kubiak, S. Topolewski, Siedlce 2016.

Fehler W., Araucz-Boruc A., Dana A., Lasota-Kapczuk A., *Systemy sztucznej inteligencji jako wyzwanie dla sfery bezpieczeństwa i obronności RP*, „Zeszyty Prawnicze" 2021, nr 2(70).

Fehler W., *Podstawy bezpieczeństwa informacyjnego*, Siedlce 2021.

Kisielewski T.A., *Uwaga szpieg! Dzieje wywiadu od Noego do Bonda*, Poznań 2018.

Korzycki R., *Gospodarka w USA kwitnie. Trump będzie walczył o drugą kadencję*, https://www.gazetaprawna.pl/wiadomosci/artykuly/1406269,usa-trump-bedzie-walczyl-o-druga-kadencje.html (data dostępu: 14.11.2021).

Leksykon Bezpieczeństwa Wewnętrznego, red. W. Fehler, J.J. Piątek, R. Podgórzańska, Szczecin 2017.

Piekałkiewicz J., *Dzieje szpiegostwa*, Warszawa 1999.

Polmar N., Allen T.B, *Księga szpiegów. Encyklopedia*, Warszawa 2000.

Repetowicz W., *Działania psychologiczno-dezinformacyjne kluczowe w ataku na Polskę [OPINIA]*, https://www.infosecurity24.pl/dzialania-psychologiczno-dezinformacyjne-kluczowe-w-ataku-na-polske-opinia (data dostępu: 14.11.2021).

Sun Tzu, *Sztuka wojny,* Warszawa 1994.