LECH WYSZCZELSKI ▶▶

Akademia Obrony Narodowej w Warszawie
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
ORCID ID: <https://orcid.org/0000-0003-2063-4281>

O bezpieczeństwie w cyberprzestrzeni

[recenzja książki *Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia*]

On security in cyberspace

[book review *Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia*]

О безопасности в киберпространстве

[рецензия книги *Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia*]

Problematyka bezpieczeństwa stała się popularna w świecie już co najmniej od lat 70. XX wieku, w Polsce od lat 90. tego samego stulecia, w szczególności po uznaniu „ nauk o bezpieczeństwie ” jako dyscypliny naukowej oraz ustanowieniu kierunku studiów „ bezpieczeństwo ” z jego różnymi specjalnościami. Z każdym rokiem w tej sytuacji pojawia się w historiografii w ogóle, w tym polskiej, wiele publikacji zajmujących się różnymi aspektami wiedzy z tej tematyki.

W 2020 r. Wydawnictwo Adam Marszałek w Toruniu wydało pracę zbiorową o przywoływanym tytule, przygotowaną w przeważającej części przez pracowników Uniwersytetu Jana Kochanowskiego w Kielcach. Jej treść została podzielona na trzy wyodrębnione części tematyczne, zaś autorami jest 17 osób. Stąd ważna była rola redaktorów naukowych jak i redakcji wydawnictwa w przyporządkowaniu autorów do poszczególnych części publikacji oraz nadaniem jej jednolitego charakteru redakcyjnego (forma poszczególnych

artykułów, jednolitość stosowania aparatu naukowego i inne). Stwierdzam, że wymienieni na ogół dobrze wywiązali się z tego zadania. Mam pewne uwagi do ich przyporządkowania w części drugiej i trzeciej. Natomiast brakuje, w tym wypadku wydaje się, że we wstępie, informacji o kryteriach wyboru autorów tej publikacji. Czy był wynikiem planu tematycznej konferencji lub sympozjum naukowego, a może indywidualnych zaproszeń? Nie ma to jednak większego wpływu na wartość tej publikacji, z pewnością potrzebnej głównie dla studentów kierunku bezpieczeństwo, ale nie tylko.

Przywoływana książka składa się ze wstępu i trzech części. Pytam, dlaczego nie umieszczono nawet syntetycznego zakończenia? Zastosowana została metoda podawania bibliografii po każdym artykule, a zabrakło nawet selektywnej ogólnej bibliografii na zakończeniu tej książki. Wstęp opracowała wymieniona dwójka redaktorów naukowych. Jest on zwięzły (wydaje się, że nawet za bardzo), ale poprawnie wprowadzający do tematyki tego opracowania.

Część pierwsza pt. „Przestrzeń międzynarodowa a cyberbezpieczeństwo” jest działem czwórki autorów. I tak Andrzej Żebrowski przygotował obszerny artykuł pt. „Aktywność informacyjna zagrożeniem dla środowiska bezpieczeństwa międzynarodowego”. Jego dość obszerna treść jest w miarę dobrym wprowadzeniem do bardziej szczegółowo prezentowanych wybranych składowych mieszczących się w pojemnym terminie „bezpieczeństwo”. Dotyczy to także ogólnego wprowadzenia do dalszej treści tej publikacji. Kolejny rozdział, autorstwa Niny Stępnickiej, Stanisława Wieteski i Artura Zimnego, został zatytułowany „Potencjalne zagrożenia bezzałogowych statków powietrznych w eksploatacji cywilnej”. Jest on specyficznym opracowaniem poświęconym „bezzałogowcom” jako środkom powietrznym i zagrożeniom, jakie mogą one stanowić dla społeczeństwa. Wydaje się, że jest to tematyka nieco odstająca od treści pozostałych publikacji poświęconych na ogół sprawom bezpieczeństwa ogólnego, a nie jednostkowego. Jest jednak ważnym zwróceniem uwagi na nowoczesne środki transportu powietrznego i zagrożenia, jakie mogą one stwarzać dla cywilnego społeczeństwa. Kolejna publikacja – autorstwa Adriana Mitręgi i nosząca tytuł „Aktywność Chińskiej Armii Ludowo-Wyzwoleńczej w cyberprzestrzeni” – z pozoru wydaje się opracowaniem odbiegającym od ogólnych rozważań nad bezpieczeństwem, jednak jej treść oceniam jako interesującą i zawierającą bardzo

ciekawe przemyślenia. Przede wszystkim autor wskazuje na wielkie zaangażowanie tak kierownictwa politycznego ChRL, jak i władz wojskowych, w nadaniu nowemu obszarowi ewentualnej konfrontacji militarnej, czyli „cyberprzestrzeni”, znamion bardzo ważnego perspektywicznego teatru wojny, nawet o znamionach globalnej konfrontacji militarnej. Wiele miejsca w tym opracowaniu poświęcone zostało chińskim formacjom wojskowym przygotowanym do walki w cyberprzestrzeni i uznanym za szczególnie współcześnie ważny teatr wojny. Ze swojej strony pragnę dodać, że od 2015 r. kierownictwo chińskiej dyplomacji, także wojskowi, zaczęli otwarcie sugerować przygotowywanie ich państwa do walki (politycznej, gospodarczej, ale i militarnej) o pozycję supermocarstwa, także w myślą o prowadzeniu jej w „cyberprzestrzeni”. Korzystając z tej okazji pragnę zwrócić uwagę na to, że analizując mocne i słabe strony dokonań w wykorzystywaniu środków określanych jako cyber..., chińska myśl wojskowa wykazuje zdecydowanie więcej tych pierwszych i stara się oddzielić pojęcie „wojny informacyjnej” od „wojny komputerowej”. Za podstawowe zagrożenie w tym obszarze teoretycy uznają: cyberprzestępstwa, haking, propagandę internetową oraz luki w systemach wojskowych (Borkowski, 2015, s. 51). Nacisk kładą też na uczestnictwo w walce elektronicznej, rozpatrywanej jako szpiegostwo. Występuje również refleksja nad prowadzeniem operacji wojskowych wykorzystujących elementy walki elektronicznej. Za takim rozwiązaniem opowiada się przykładowo Li Degin, zastępca dziekana Wydziału Teorii Działań Wojennych i Strategii Wojskowej Akademii Nauk (Borkowski, 2015, s. 52). Teoretycy tego państwa dowodzą, że cyberataki w połączeniu z możliwością unieszkodliwiania amerykańskich satelitów oraz ich centrów dowodzenia stanowią specjalną broń, która może zahamować amerykańskie działania wojenne w rejonie Zachodniego Pacyfiku. Wskazać należy i to, że USA i ChRL jako pierwsze stworzyły programy szpiegowskie wykorzystywane szeroko w sieciach teleinformatycznych. Obecna uwaga teoretyków tych państw skupia się na szpiegostwie gospodarczym, ale nie tylko. Możliwe, nawet wielce prawdopodobne, jest zastosowanie tego i dla celów militarnych, w czym prym wiedzie Izrael, ale też i niektóre państwa arabskie.

Ostatnia publikacja w tej części jest autorstwa Pawła Chabielskiego i nosi tytuł „CIMIC w cyberprzestrzeni”. Rozszyfrowując ten skrót, jest to ocena współpracy cywilno-wojskowej właśnie w obszarze cyberprzestrzeni.

Polecam zapoznanie się z tym interesującym przyczynkiem. Część pierwszą oceniam najwyżej wśród pozostałych.

Uznać trzeba, że kolejne dwie części tego opracowania dotyczą wężej ujmowanej tematyki. Ich autorzy to w większości młodzi pracownicy dydaktyczno-naukowi, doktoranci, w tym osoby wywodzące się spoza środowisk akademickich. Ich opracowania są jednak niekiedy dobrze podbudowane wiedzą specjalistyczną i to nawet traktowaną jako wąskotematyczną. Wobec tego uważam je za godne zaprezentowania. Uczynię to ze względów na wymogi wydawnicze tylko przez zaprezentowanie autorów i tytułów opracowań zawartych w tym wydawnictwie.

Najobszerniejsza objętościowo jest część druga – „Bezpieczeństwo państwa w cyberprzestrzeni”. Zamieszczone zostały w niej publikacje aż ośmiu autorów. Są to: Jan Zych („Bezpieczeństwo w środowisku sieciowym”), Paweł Górski („Bezpieczeństwo w cyberprzestrzeni XXI wieku – zarys problemu”), Joanna Grubicka („Świat w sieci – nowa jakość zagrożeń dla bezpieczeństwa państwa”), Piotr Zalewski („Od Netykiety do CSIR-tów. Geneza i rozwój regulacji prawnych i organizacyjnych powszechnego i krajowego systemu cyberbezpieczeństwa”), Rafał Kołodziejczyk („Bezpieczeństwo Rzeczypospolitej Polskiej w cyberprzestrzeni”), Martyna Ostrowska („Inteligentne systemy transportowe (ITS) a poprawa bezpieczeństwa uczestników ruchu drogowego”), Renata Gruszczyńska („Infrastruktura krytyczna – technologie i systemy jakimi posługuje się Straż Miejska w Kielcach) oraz Marcin Walczak („Cyberprzestępczość – definicja, formy i ich społeczno-ekonomiczne skutki dla gospodarki”). Już sama prezentacja tytułów sugeruje, że autorzy z reguły podejmują tematykę wąskoprzedmiotową i stąd te publikacje zaliczyć należy do kategorii przyczynków. Nie oznacza to, że należy postponować podejmowaną tematykę, tyle że kierowana jest ona bardziej do wąskich specjalności i osób tym się zajmujących. Polecam Czytelnikom lekturę wymienionych publikacji.

Ostatnia część recenzowanej książki, zatytułowana „Bezpieczeństwo personalne w cyberprzestrzeni”, reprezentowana jest przez pięciu autorów. Są to: Magdalena Molendowska, autorka artykułu pt. „Bezpieczeństwo w sieci – wybrane problemy”, Rafał Miernik („Dezinformacja i fake newsy w Internecie jako zagrożenia bezpieczeństwa w Unii Europejskiej”), Katarzyna Rządowska („Deepfake jako jeden z elementów zagrożenia cybernetycznego”),

Marcin Banaszek („Bezpieczeństwo bankowości internetowej i mobilnej”) i Anna Ptaszek, zamykająca książkę publikacją pt. „Wpływ fonoholizmu na bezpieczeństwo społeczne”. Podobnie jak pisałem w odniesieniu do części drugiej i ta część złożona jest z wąskotematycznych przyczynków. Ich autorzy to z reguły początkujący dopiero autorzy lub też specjalizujący się w wąskich specjalnościach. Czy jest to zarzut recenzenta? Raczej nie, bowiem szanuję prawo młodych naukowców do wykazywania się swoją wiedzą i to nawet bardzo wyprofilowaną, co z czasem będzie owocowało znaczącymi pozycjami monograficznymi. Do tego nawet tematyka stosunkowo wąska jest potrzebna dla szerszej refleksji teoretycznej. W tym wypadku z pewnością zainteresowane osoby mogą skorzystać z wyników badawczych autorów przywoływanych w tej części opracowania.

Wszystkie z prezentowanych opracowań zostały przygotowane zgodnie ze współczesnymi wymogami edytorskimi, ale i wymaganiami stawianymi przez resort nauki dla zaliczenia ich do odpowiedniej punktacji. Mają one wprowadzenia, podsumowania i inne stosowne wymogi resortowe. Nie mam uwag do formy zamieszczanych przypisów. Każde z opracowań zawiera bibliografię. W odniesieniu do niej proponowałbym jednak jej podział na opracowania zwarte i przyczynkarskie, w niektórych wypadkach wydzielenie także aktów normatywnych. W tym wypadku pochwalić należy redaktorów naukowych i redaktora prowadzącego za formę przygotowania tej książki. Została ona zrecenzowana przez dr. hab. Henryka Wyrobka.

Uznaję wobec tego powyższe opracowanie jako pożyteczne dla pewnego uporządkowania wiedzy z obszaru bezpieczeństwa, także za podawanie nowych szczegółowych ustaleń badawczych.

Podkreślenia wymaga też forma edytorska tej publikacji. Wydawca – Wydawnictwo Adam Marszałek z Torunia – ma udział w przygotowaniu i wydaniu oraz wprowadzeniu do obiegu księgarskiego tej książki. Niniejsza recenzja ma natomiast zachęcić potencjalnych Czytelników do zapoznania się z tą publikacją. Może to służyć poszerzeniu wiedzy z tak modnego współcześnie obszaru jak cyberprzestrzeń, a w nim także niemniej modnej problematyki cyberbezpieczeństwa.

PROF. DR HAB. LECH WYSZCZELSKI

Profesor emerytowany
Akademia Obrony Narodowej w Warszawie
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
lech.wyszczelski1942@gmail.com

Bibliografia

- Borkowski, K. (2015). Koncepcje cyberbezpieczeństwa w ujęciu Chińskiej Republiki Ludowej – wybrane aspekty. *Przegląd Bezpieczeństwa Wewnętrznego*, 15(7), ss. 49–59.
- Molendowska, M., Miernik, R. (2020). *Bezpieczeństwo w cyberprzestrzeni. Wybrane zagadnienia*. Toruń: Wydawnictwo Adam Marszałek.