Sabina Olszyk

"Sieciocentryczne bezpieczeństwo: wojna, pokój i terroryzm w epoce informacji", red. Krzysztof Liedel, Paulina Piasecka, Tomasz R. Aleksandrowicz, Warszawa 2014 : [recenzja]

Przegląd Naukowo-Metodyczny. Edukacja dla Bezpieczeństwa nr 2, 309-313

2014

Sabina OLSZYK
Uniwersytet Pedagogiczny im. KEN w Krakowie

RECENZJA

Krzysztof Liedel, Paulina Piasecka, Tomasz R. Aleksandrowicz (red. nauk.), *Sieciocentryczne bezpieczeństwo: wojna, pokój i terroryzm w epoce informacji, Wyd.*, Difin SA. Warszawa 2014, ss. 223, bibliogr. ISBN 978-83-7930-271-0

Recenzowana publikacja wydana została w formie pracy zbiorowej pod redakcją: Krzysztofa Liedla, Pauliny Piaseckiej oraz Tomasza R. Aleksandrowicza i stanowi wnikliwe oraz bardzo ciekawe studium nad bezpieczeństwem współczesnego świata w dobie cyfrowej informacji. Opiekę redakcyjną nad publikacją roztoczyło trzech znakomitych ekspertów w zakresie badań nad bezpieczeństwem i społeczeństwem informacyjnym oraz terroryzmem międzynarodowym.

Pierwszy z redaktorów to Krzysztof Liedel – polski prawnik, doktor nauk wojskowych, a przede wszystkim wybitny specjalista w zakresie terroryzmu międzynarodowego oraz bezpieczeństwa informacyjnego. Jego wielodziedzinowe wykształcenie oraz bogactwo doświadczeń zawodowych zdobytych w najwyższych instytucjach państwowych i naukowych,[1] sytuują go w gronie największych polskich znawców tej tematyki.

Drugim redaktorem jest Paulina Piasecka – absolwentka Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego oraz stypendystka rządu Stanów Zjednoczonych. Pełniła funkcję głównego specjalisty w Wydziale ds. Przeciwdziałania Zagrożeniom Terrorystycznym Departamentu Bezpieczeństwa Publicznego MSWiA oraz Zastępcy Kierownika Instytutu Analizy Informacji Collegium Civitas. Aktualnie pełni funkcję **Zastępcy Dyrektora Centrum Badań nad Terroryzmem ds. Programowych**, jak również obejmuje stanowisko Naczelnika Wydziału Bezpieczeństwa Publicznego w Biurze Bezpieczeństwa Narodowego.[2]

---

[1] Jest absolwentem Wyższej Szkoły Policji w Szczytnie oraz Wydziału Prawa i Administracji w Uniwersytecie Marii Curie-Skłodowskiej w Lublinie. Ukończył także studia podyplomowe w zakresie bezpieczeństwa informacyjnego (Akademia Obrony Narodowej w Warszawie), nauk o polityce (Collegium Civitas w Warszawie) oraz organizacji i zarządzania (Wojskowa Akademia Techniczna w Warszawie). W 2009 r. obronił rozprawę doktorską nt. *Zarządzanie zasobami informacyjnymi w warunkach zagrożeń terrorystycznych dla bezpieczeństwa państwa*, napisaną pod kierunkiem prof. Piotra Sienkiewicza na Wydziale Bezpieczeństwa Narodowego Akademii Obrony Narodowej. Posiada bardzo bogate doświadczenie zawodowe m.in. jako zastępca Dyrektora Departamentu Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego, dyrektor Centrum Badań nad Terroryzmem Collegium Civitas oraz kierownik Instytutu Analizy Informacji Collegium Civitas. Jest też wykładowcą Collegium Civitas w Warszawie, Akademii Obrony Narodowej, Uniwersytetu Warszawskiego oraz Wyższej Szkoły Policji w Szczytnie. Krzysztof Liedel jest ponadto redaktorem naczelnym kwartalnika *Terroryzm: zagrożenia – prewencja – przeciwdziałanie*, jak również autorem wielu cenionych książek, monografii i ponad pięćdziesięciu artykułów na temat terroryzmu i jego zwalczania oraz bezpieczeństwa informacyjnego. *Krzysztof Liedel: prywatna strona internetowa [Informacje o mnie]* [online]. Dostępny w Internecie: *http://www.liedel.pl/?page_id=2* (pobrano 28.04.2014 r.)

[2] *Eksperci CBnT: Paulina Piasecka* [online]. Dostępny w Internecie: *http://www.cbnt.collegium.edu.pl/index.php?option=com_content&view=article&id=125&Itemid=101* (pobrano 28.04.2014 r.)

Trzeci z redaktorów – Tomasz Aleksandrowicz – jest doktorem nauk prawnych, specjalistą w zakresie prawa międzynarodowego publicznego. Przez wiele lat był analitykiem politycznym łączącym działalność naukową z praktyką. Pracował w Urzędzie Ochrony Państwa i Zespole Doradców Prezydenta RP. Jego zainteresowania naukowe koncentrują się wokół zagadnień związanych z terroryzmem międzynarodowym, analizą informacji, rolą służb specjalnych w stosunkach międzynarodowych, zagadnieniami obowiązywania prawa Unii Europejskiej w krajowych porządkach prawnych oraz przemianami suwerenności państwa narodowego. **Aktualnie pełni funkcję Przewodniczącego Rady Naukowej Centrum Badań nad Terroryzmem** oraz Przewodniczącego Rady Programowej Instytutu Analizy Informacji.[3]

W obliczu złożoności i przenikania się różnych sfer otaczającej nas rzeczywistości istotne jest poznawanie owej rzeczywistości w różnych ujęciach. Niniejsza publikacja jest oryginalnym opracowaniem uwzględniającym złożoność zjawiska bezpieczeństwa w wymiarze sieciocentrycznym. Podejmuje rozważania na temat istoty społeczeństwa informacyjnego, tego jak ono funkcjonuje w środowisku sieci i przed jakimi zagrożeniami staje. Stanowi także próbę odpowiedzi na pytania o to, jak należy kształtować strategie bezpieczeństwa, by mogły one stanowić realną, efektywną odpowiedź na owe zagrożenia oraz by pozwoliły skutecznie im przeciwdziałać; jak aktorzy sceny międzynarodowej będą dbać o swoje bezpieczeństwo w dobie informacji cyfrowej; jak w przyszłości będzie wyglądał czas wojny i czas pokoju; jak państwo zabezpiecza się w cyberprzestrzeni; czy wojna przyszłości będzie się toczyć właśnie w wirtualnej, cyfrowej rzeczywistości.

W recenzowanej publikacji podjęto także próbę spojrzenia na środki i narzędzia zapewnienia bezpieczeństwa pod kątem zdolności ofensywnych państwa, niezbędnych w epoce sieciocentrycznych wojen i konfliktów cyfrowych (mających miejsce wyłącznie w cyberprzestrzeni). Zamierzeniem autorów poszczególnych rozdziałów nie była całościowa analiza tego szerokiego zjawiska, bo i jest to zapewne niemożliwe, celem było natomiast nakreślenie obszarów możliwych aktualnych i przyszłych zagrożeń związanych z sieciocentrycznością w wymiarze społecznym, technologicznym oraz politycznym. Zamierzeniem autorów było ponadto wywołanie debaty o tworzeniu się na naszych oczach dwoistego środowiska bezpieczeństwa, które przybiera zarówno charakter materialny, jak i cyfrowy, a które to płaszczyzny w dzisiejszym świecie nawzajem się przenikają (s. 7-8). W przekonaniu autorów książki można analizować bezpieczeństwa poszczególnych państw, bezpieczeństwa międzynarodowego oraz budować skutecznych strategii przeciwdziałania zagrożeniom bez uwzględnienia sieciocentrycznego charakteru współczesnego świata. Wpływa on nie tylko na codzienne życie poszczególnych obywateli, ale także zmusza władze państwa oraz podmioty międzynarodowe do dbania o swoje bezpieczeństwo w dobie cyfrowej informacji.

Praca, będąca przedmiotem analizy, składa się z czternastu fragmentów (rozdziałów), z których każdy stanowi odrębną refleksję autora/ów na wybrany

[3] *Eksperci CBnT: dr Tomasz Aleksandrowicz* [online]. Dostępny w Internecie: http://www.cbnt.collegium.edu.pl/index.php?option=com_content&view=article&id=125&Itemid=101 (pobrano 28.04.2014 r.)

temat. Klamrą spinającą poszczególne teksty jest Wprowadzenie i Zakończenie autorstwa K. Liedla.

W pierwszym rozdziale przeczytamy na temat zagrożeń rodzących się w związku z rozwojem nowoczesnych technologii informacyjnych, które powodują, że nowym środowiskiem walki staje się cyberprzestrzeń, będąca areną działań wojskowych i wywiadowczych, sabotażowych, przestępczych, chuligańskich, a także działań o charakterze politycznym i propagandowym. Jest to z związane ze zmieniającym się charakterem społeczeństwa informacyjnego, sieci oraz cyberprzestrzeni (T. R. Aleksandrowicz, K. Liedel). Kolejne rozdziały traktują na temat strategii bezpieczeństwa w cyberprzestrzeni (T. R. Aleksandrowicz) jak również podejmują tematykę cyberbezpieczeństwa w świetle *Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń JOIN(2013)1 final* (P. Rutkowski). W dalszej części recenzowanej publikacji analizowano, czy współczesna edukacja może stanowić tarczę przeciw BMM (Broni Masowej Manipulacji)? (W. Sokała), przedstawiono również aktualne wyzwania w zarządzaniu bezpieczeństwem informacji (P. Szeptyński) oraz ukazano sposoby kształtowania zdolności ofensywnych w cyberprzestrzeni (K. Liedel). Kolejne rozważania dotyczyły metod prowadzenia walki w cyberprzestrzeni w postaci: cyberwojny (K. Boruc), wojny sieciocentrycznej (P. Piasecka; D. Mąka). W opracowaniu poruszono ponadto kwestię bezpieczeństwa sił zbrojnych RP w dobie zagrożeń cybernetycznych (E. Lichocki, T. Mirosław) oraz wskazano sposoby wywołania konfliktu w cyberprzestrzeni tj. cyberatak (P. Marczak), szpiegostwo, inwigilacja (M. Grzelak) oraz tzw. „biały wywiad" (B. Saramak). Ostatni rozdział pracy dotyczy zabezpieczania dowodu elektronicznego (A. Mroczek, A. Sułowska).

Choć zamierzeniem autorów publikacji nie było całkowite wyczerpanie kwestii bezpieczeństwa w dobie sieciocentryczności ani ostateczne nakreślenie kierunku, w którym zmierzać będzie współcześnie globalne środowisko bezpieczeństwa, to udało im się zwrócić uwagę na ważniejsze zjawiska zagrażające bezpieczeństwu w cyberprzestrzeni oraz pokazać różnorodność i złożoność owego środowiska. Obiektywnym okiem specjalistów i znawców tematu autorzy nakreślili charakter i obszar aktualnych i przyszłych wyzwań jakie stoją przed organizacjami państwowymi w dobie społeczeństwa informacyjnego. Rozpoczęli również debatę na temat roli sieci, cyberprzestrzeni zarówno w wymiarze społecznym, technologicznym oraz informacyjnym w zapewnieniu bezpieczeństwa narodowego i międzynarodowego.

Warto podkreślić, że publikację cechuje jasna, klarowna konstrukcja, różnorodność poruszanych kwestii, co zasługuje na szczere uznanie. Zauważyć należy fakt, że w opracowaniu wykorzystano bogatą literaturę fachową zarówno w języku polskim, jak i angielskim. Ponadto logicznie zbudowana narracja, trafne uwagi i prognozy, uczyniły z omawianej książki pozycję o dużej wartości naukowej, otwierającą nowe obszary badawcze dla zainteresowanych tą tematyką naukowców.

Należy jednakże zwrócić uwagę na pewne drobne uchybienia zarówno w sferze formalnej, jak i merytorycznej pracy. Struktura formalna nie jest do końca zborna, gdyż artykuł pierwszy (T. R. Aleksandrowicz, K. Liedel) zajmuje 30 stron, podczas gdy część rozdziałów obejmuje ok. 10-14 stron, część nawet do 20 stron, natomiast artykuł autorstwa E. Cichockiego i T. Mirosława usytuowany jest tylko na 9 stronach. Należałoby zatem zachować większą równowagę w objętości poszczególnych artykułów.

Istotnym uchybieniem, w moim przekonaniu, jest brak jasnego zdefiniowania pojęcia *sieciocentryczności* w kontekście bezpieczeństwa tym bardziej, że termin ten występuje w tytule publikacji. O ile pojęcie *cyberprzestrzeni* czy *cyberwojny* wyjaśnione zostało w pracy w kilku nawet artykułach, o tyle terminowi *sieciocentryczność,* zdaniem recenzentki, nie poświęcono należytej uwagi. W artykule pierwszym, co prawda, przeprowadzono krótką analizę pojęcia *sieć*, *struktury sieciowe*, jednak nie wskazano jasnej i klarownej definicji zjawiska sieciocentryczności, nie przedstawiono stanu badań nad tym procesem, co może budzić pewien niedostatek szczególnie u słabo wprawionego w tej tematyce czytelnika.

W poszczególnych rozdziałach zaobserwowano ponadto pewne nieścisłości terminologiczne. Wydaje się, że niektórzy autorzy nie rozróżniają pojęć tj. *wojna sieciocentryczna, wojna informacyjna, cyberwojna, cyberprzestępczość, cyberatak,* ale traktują owe terminy jako tożsame (synonimy). Słusznie jednak w jednym z rozdziałów (s. 27) zwrócono uwagę, że są to pojęcia odrębne o odmiennym znaczeniu.

Pomimo znacznej różnorodności poruszanych w książce kwestii, autorka recenzji odczuwa jednak pewien niedosyt. Nie uwzględniono bowiem kilku istotnych problemów jakie, w przekonaniu recenzentki, powinny się znaleźć m.in. szersze potraktowanie kwestii przestępstw komputerowych, zwrócenie większej uwagi na aspekty prawne regulujące kwestie bezpieczeństwa w sieci, narzędzia zapobiegania cyberprzestępczości etc. Niektóre tematy dotyczące np. konkretnych rodzajów cyberataków zostały potraktowane dość skrótowo (s. 149-154), inne kwestie pojawiały się natomiast stosunkowo często w kilku nawet artykułach różnych autorów. Za przykład niech posłuży chociażby częste definiowanie tych samych pojęć w różnych rozdziałach np. *cyberprzestrzeń* (s. 23-27; s. 182-183), c*yberwojna* (s. 31-37; s. 98-102), *cyberterroryzm* (s. 139-143; s. 153; s. 182-183). Kilkukrotnie także w różnych artykułach, analizowano te same przykłady cyberataków np. Tallin w 2007 r. (s. 102; s. 157-158) czy Gruzja w 2008 r. (s. 102-106; 158-161). Te drobne nieścisłości i powtórzenia wydają się trudne do uniknięcia w przypadku pracy zbiorowej, kiedy publikacja jest dziełem kilku autorów. W przekonaniu recenzentki należałoby jednak w przyszłości zwrócić uwagę również na te aspekty.

Powyższe uwagi nie zmierzają jednak do podważenia dużej wartości naukowej pracy jako całości. Książka, w moim przekonaniu, może liczyć na sporą grupę odbiorców, wykraczającą poza krąg badaczy zajmujących się tematyką społeczeństwa informacyjnego oraz cyberterroryzmu. Decyduje o tym przede wszystkim nowatorska tematyka, odważne prognozy wobec kierunków przyszłych konfliktów i zagrożeń państw oraz związanej z tym konieczności zapewnienia bezpieczeństwa, różnorodne i ciekawe przykłady zjawisk funkcjonujących w cyberprzestrzeni oraz przystępność języka, jakim książka została napisana.

W sumie otrzymaliśmy pracę, która w znacznym stopniu pogłębia i poszerza stan naszej wiedzy na temat skomplikowany, cały czas żywy i tym samym coraz bardziej zróżnicowany. Opracowanie posiada niewątpliwe walory eksplanacyjne, stanowi ważne uzupełnienie literatury przedmiotu, będąc jednocześnie źródłem wiedzy o społeczeństwie informacyjnym, mechanizmach i narzędziach walki w cyberprzestrzeni oraz o kierunku wyzwań, przed jakimi stoją instytucje państwowe i społeczne w celu zapewnienia bezpieczeństwa narodowego. Skłania do wielu refleksji i otwiera nowe pola badawcze zarówno dla specjalistów z dziedziny bezpieczeństwa, jak również dla politologów, socjologów, informatyków i innych uczonych, podejmujących zainteresowanych problematyką bezpieczeństwa w świecie cyfrowym.