MAŁGORZATA KUDZIN-BORKOWSKA
ORCID: 0000-0002-5816-3676

DOI: 10.4467/20801335PBW.21.009.13566

Cyberbezpieczeństwo w Grupie Wyszehradzkiej – koncepcje i strategie

Impulsem do podjęcia rozważań dotyczących problematyki cyberbezpieczeństwa w Grupie Wyszehradzkiej (dalej: Grupa V4), która od początku swojego istnienia jest postrzegana jako najbardziej dynamiczne ugrupowanie w Europie Środkowej, jest okrągła, trzydziesta rocznica jej utworzenia, przypadająca w 2021 r. Bezpieczeństwo cybernetyczne we wszystkich czterech państwach członkowskich tej Grupy stanowi ważny element działań politycznych, militarnych, społecznych i gospodarczych. Upowszechnianie się cybertechnologii spowodowało konieczność wprowadzenia zmian w prawie oraz zarządzaniu bezpieczeństwem teleinformatycznym, zwłaszcza w pierwszej dekadzie XXI w. Praca ma charakter przyczynkarski i jest próbą uwypuklenia wybranych zagadnień dotyczących koncepcji cyberbezpieczeństwa i cyberstrategii w poszczególnych państwach członkowskich Grupy V4. Najważniejszym celem autorki było scharakteryzowanie definicji i podstawowych pojęć związanych z cyberbezpieczeństwem oraz przybliżenie różnic i podobieństw w postrzeganiu tego zagadnienia w wybranych dokumentach strategicznych.

W naukach o bezpieczeństwie można znaleźć wiele terminów dotyczących bezpieczeństwa informacyjnego, jednak w ostatnich latach w dokumentach strategicznych oraz w ustawach dominuje kategoria pojęciowa cyberbezpieczeństwo (*cybersecurity*[1]). Celem badań przeprowadzonych w ramach niniejszej pracy jest przeanalizowanie inicjatyw w zakresie cyberbezpieczeństwa podejmowanych w Grupie V4 oraz przedstawienie głównych działań realizowanych w tym zakresie przez Unię Europejską i Organizację Traktatu Północnoatlantyckiego (dalej: NATO). Z wykorzystaniem

[1] Prawie wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje za każdym razem tej informacji. Informacja pojawia się jedynie w przypadku wyrazów obcych pochodzących z języka innego niż angielski (przyp. red.).

metody *desk research*[2] oraz krytycznego przeglądu literatury autorka podjęła próbę refleksji teoretyczno-metodologicznej nad siatką pojęciową stosowaną w nauce oraz w dokumentach strategicznych, aby określić skończony zbiór pojęć synonimicznych oraz bliskoznacznych pojęciu „cyberbezpieczeństwo". Dokonała analizy treści i analizy porównawczej dokumentów strategicznych państw członkowskich Grupy V4. Kwestie dotyczące cyberbezpieczeństwa wymagają rozwiązań nie tylko wewnątrzkrajowych, lecz także międzynarodowych. Z tego względu celem autorki jest poszukanie odpowiedzi na następujące pytania: czy istnieje współpraca państw Grupy V4 w tym zakresie, czy występują zasadnicze różnice w dokumentach strategicznych dotyczących cyberbezpieczeństwa przygotowanych przez poszczególne państwa członkowskie oraz czy w tych dokumentach jest deklarowana współpraca w ramach Grupy V4? Autorka zakłada, że konceptualizacje cyberbezpieczeństwa w dokumentach strategicznych poszczególnych państw Grupy V4 istotnie różnią się od siebie, nie można zatem mówić o wspólnej i spójnej polityce cyberbezpieczeństwa tej Grupy.

Od drugiej połowy XX w. podstawowym czynnikiem rozwoju cywilizacji są procesy zarządzania informacją, a więc jej wytwarzania, przechowywania, wyszukiwania, przekształcania i przesyłania[3]. Gigantyczny przepływ informacji i ciągły rozwój technologii cyfrowych wydają się nie mieć żadnych ograniczeń i stanowią o istocie współczesnej techniki, gospodarki czy wojskowości. Tak jak w przypadku innych obszarów życia społecznego i gospodarczego oraz aktywności ludzkiej również w sferze zarządzania informacją pojawiają się rozmaite zagrożenia, którym trzeba przeciwdziałać, aby zapewnić bezpieczeństwo komunikowania i korzystania z informacji[4].

Wyróżnia się kilka kategorii pojęciowych odnoszących się do różnych obszarów i zagadnień z zakresu bezpieczeństwa, które są wykorzystywane w dziedzinie zarządzania informacją. Najbardziej ogólną jest bezpieczeństwo informacyjne (*information security, information safety*)[5], przez które najczęściej rozumie się ochronę informacji przed niepożądanym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania, a podejmowane środki bezpieczeństwa mają zapewnić poufność, integralność oraz dostępność informacji[6]. Pojęcie bezpieczeństwo

[2] Metoda badawcza polegająca na kompilacji, analizowaniu oraz przetwarzaniu danych i informacji pochodzących z istniejących źródeł, a następnie formułowaniu na ich podstawie wniosków dotyczących badanego problemu. Za: Encyklopedia Zarządzania, mfiles.pl/index.php/Desk_research [dostęp: 26 I 2021] – przyp. red.

[3] R. Borkowski, *Cywilizacja, technika, ekologia. Wybrane problemy rozwoju cywilizacyjnego u progu XXI wieku*, Kraków 2001, s. 64.

[4] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012.

[5] Oba terminy funkcjonują w języku angielskim i są zamiennie stosowane przez anglosaskich autorów i ekspertów.

[6] Zob. K. Liedel, *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, s. 45–62; tenże, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2014; J. Jańczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013; O. Strnád, *Riadenie rizík informačnej bezpečnosti*, Ostrava 2010.

informacji (*security of information*) wiąże się z kolei z zagadnieniami ochrony informacji niejawnych, tajemnicy państwowej, tajemnicy biznesowej oraz zagrożeniami wywiadu wojskowego,politycznego i przemysłowego[7]. Trzy kolejne kategorie pojęciowe stosowane w literaturze przedmiotu są ze sobą ściśle powiązane i w dużej mierze dotyczą zagadnień z zakresu technologii informatycznych, technicznych zabezpieczeń i ochrony przestrzeni przetwarzania informacji oraz interakcji zachodzących w sieciach teleinformatycznych. Rozumienie pojęcia bezpieczeństwo informatyczne najczęściej jest zawężane do oprogramowania służącego do zapewnienia bezpieczeństwa, w tym rozwiązań antywirusowych, zapór sieciowych (*firewalls*) oraz systemów wykrywania włamań (*intrusion detection system*, IDS), a także do przestrzegania przez użytkowników odpowiednich procedur bezpieczeństwa podczas korzystania z oprogramowania[8]. Z kolei o bezpieczeństwie systemów informatycznych (komputerowych) mówi się, mając na myśli m.in. eliminację błędów już na etapie projektowania i tworzenia oprogramowania oraz w fazie testowania urządzeń[9]. Przez bezpieczeństwo teleinformatyczne i teleinformacyjne, a także przez bezpieczeństwo Internetu rozumie się natomiast zbiór zagadnień z zakresu telekomunikacji i informatyki koncentrujących się na analizie ryzyka i kontrolowaniu zagrożeń związanych z korzystaniem z komputerów, sieci komputerowych oraz urządzeń przesyłowych[10]. Ogromnego znaczenia nabrała w ostatnim czasie inżynieria ochrony danych, którą Krzysztof Liderman definiuje jako metodykę i narzędzia stosowane podczas projektowania i wdrażania mechanizmów ochrony danych[11].

Wiele pojęć, pomimo ich używania w dokumentach państwowych oraz w wojskowości, ma, jak podkreśla Cezary Banasiński, charakter nieostry i zgoła nienaukowy, a ich definicje pojawiły się w literaturze pięknej[12]. Do takich pojęć należą: rzeczywistość wirtualna (*virtual reality*), cyberprzestrzeń (*cyberspace*) oraz wspomniane już „cyberbezpieczeństwo". To ostatnie pojęcie jest obecnie stosowane najczęściej, o czym już nadmieniono, i wypiera z dyskursu publicznego inne kategorie pojęciowe[13]. Przez „cyberprzestrzeń" rozumie się najczęściej globalną infrastrukturę

---

7 *Ochrona informacji niejawnych w XXI wieku*, S. Topolewski (red.), Siedlce 2016, s. 5.

8 Zob. K. Liderman, *Bezpieczeństwo informacyjne – nowe wyzwania*, Warszawa 2017, s. 152–153, 160–161; tenże, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2009; R. Pręgiel, P. Buchwald, *Internet w społeczeństwie informacyjnym – nowoczesne systemy informatyczne i ich bezpieczeństwo*, Dąbrowa Górnicza 2014.

9 J. Jaźwiński, K. Ważyńska-Fiok, *Bezpieczeństwo systemów*, Warszawa 1993.

10 *Bezpieczeństwo teleinformatyczne państwa*, M. Madej, M. Terlikowski (red.), Warszawa 2009.

11 K. Liderman, *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Warszawa 2003, s. 9.

12 *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2018, s. 23–27.

13 Zob. M. Lakomy, *Dylematy polityki cyberbezpieczeństwa Polski*, w: *Dylematy polityki bezpieczeństwa Polski na początku drugiej dekady XXI wieku*, K. Czornik, M. Lakomy (red.), Katowice 2014, s. 425–454; J.L. Bayuk i in., *Cyber Security Policy Guidebook*, Hoboken 2012; K. Liedel, *Cyberbezpieczeństwo – wyzwania przyszłości. Działania społeczności międzynarodowej*, w: *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2011, s. 437–448.

informacyjną, a więc przestrzeń komunikacyjną tworzoną przez system powiązań internetowych albo też wszechogarniającą świat domenę informacyjną, w której nośnikiem danych jest spektrum elektromagnetyczne[14]. Posługując się kategorią pojęciową „rzeczywistość wirtualna", można zdefiniować „cyberprzestrzeń" jako wirtualne środowisko mniej lub bardziej otwartego komunikowania się za pośrednictwem połączonych systemów komputerowych oraz powiązań informacyjnych i informatycznych[15].

Badacze internetu oraz społeczeństwa informacyjnego, jak Sherry Turkle czy Clay Shirky, głoszą pogląd, że globalna sieć nie jest już tylko produktem rozwoju technologii i jednym z elementów cywilizacji naukowo-technicznej, lecz sama stała się istotą cywilizacji. Jest bowiem zbiorem narzędzi, zasobów i praktyk kulturowych organizujących życie współczesnego człowieka, zarówno w wymiarze rzeczywistości materialnej, jak i symbolicznej. Próba wyobrażenia sobie świata bez internetu jest *de facto* wyobrażeniem świata bez cywilizacji i stanowi często kanwę powieści oraz obrazów filmowych o charakterze postapokaliptycznym[16]. Zagrożenia w cyberprzestrzeni i ochrona przed nimi stały się istotnym problemem współczesnego świata, w którym wciąż postępują cyfryzacja różnych dziedzin życia oraz rozwój technologii ICT (*information and communication technologies*). Zdaniem wielu badaczy problematyki, podzielanym przez Cezarego Banasińskiego, cyberbezpieczeństwo jest zagadnieniem charakteryzującym się złożonością, interdyscyplinarnością oraz multidyscyplinarnością, łączącym obszary badawcze z zakresu informatyki, socjologii internetu, psychologii i zarządzania. Dlatego jego badanie mieści się w obszarze securitologii, będącej nauką transdycyplinarną[17].

Warto zwrócić uwagę, że przedrostek „cyber-" pochodzi od słowa „cybernetyczny", a cybernetyka to nauka o sterowaniu, organizacji i zarządzaniu, a w mniejszym stopniu – o przetwarzaniu informacji[18]. Stąd też kategoria pojęciowa „cyberbezpieczeństwo" odnosiłaby się raczej do bezpieczeństwa sterowania, co w przypadku bezpieczeństwa informacji oznaczałoby sterowanie procesami przepływu informacji. Pojęcie informacja pochodzi od łacińskiego słowa *informatio* oznaczającego 'wizerunek', 'obraz', 'pojęcie oraz od czasownika *informo* oznaczającego 'wyobrażać', 'tworzyć' lub 'kształtować'. Pomimo wątpliwości semantycznych przedrostek „cyber-" upowszechnił się w mass mediach w odniesieniu do zagadnień związanych z technologiami informatycznymi i, jak podkreśla Tomasz Pączkowski, obecnie pod pojęciem cyberzagrożenia

[14] *Cyberbezpieczeństwo*…, s. 24–25.

[15] Tamże.

[16] Zob. E. Bendyk, P. Rutkowski, *Poranek bez sieci*, „Polityka" 2019, nr 16, s. 44–46; S. Turkle, *Life on the Screen: Identity in the Age of Internet*, New York 2011; C. Shirky, *Here Comes Everybody: The Power of Organizing without Organizations*, New York–London 2009; B. Snow, *What Would a World Without Internet Look Like? A thought experiment*, „The Atlantic", 5 IV 2016 r., www.theatlantic.com/technology/archive/2016/04/a-world-without-internet/476907/ [dostęp: 18 II 2021].

[17] Zob. *Cyberbezpieczeństwo*…, s. 37; L.F. Korzeniowski, *Securitologia: nauka o bezpieczeństwie człowieka i organizacji społecznych*, Chorzów 2009.

[18] Zob. *Słownik pojęć współczesnych*, A. Bullock i in. (red.), Katowice 1999; J. Kossecki, *Cybernetyka społeczna*, Warszawa 1981, s. 10.

rozumie się wszelkie niebezpieczeństwa związane z korzystaniem z internetu[19]. Można zatem uznać, że używanie określenia *cybersecurity* jest przejawem mody językowej i wynika z powszechnej dominacji terminologii anglojęzycznej. W wojskowości stosuje się pojęcia: cyberaktywność militarna, cyberoperacja militarna, cyberatak, cyberwojna i cyberobrona. Wprowadzono również pojęcie cyberterroryzm na określenie nowego rodzaju terroryzmu. Z kolei w medioznawstwie mówi się o cyberkomunikowaniu. Notabene pojęcia cyberprzestrzeń oraz rzeczywistość wirtualna pojawiły się w literaturze *science fiction* w 1984 r., a ich twórcą był William Gibson[20]. Kategoria „cyberbezpieczeństwo" nie jest więc synonimem pojęć „bezpieczeństwo informacyjne" i bezpieczeństwo cyfrowe (*digital security*), można natomiast przyjąć, że jest tożsama z pojęciem bezpieczeństwo komunikowania w cyberprzestrzeni. W literaturze pojawia się także pojęcie e-bezpieczeństwo (*e-safety*), tj. bezpieczeństwo elektroniczne[21].

W dokumencie *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, opublikowanym 7 lutego 2013 r., stwierdza się, że bezpieczeństwo cybernetyczne odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci oraz tę infrastrukturę uszkodzić. Z kolei przez pojęcie polityka bezpieczeństwa informacji (*information security policy*) należy rozumieć zbiór reguł i procedur, zgodnie z którymi państwo, siły zbrojne, służby lub korporacje tworzą i udostępniają zasoby informacyjne i zarządzają nimi oraz określają, które zasoby i w jaki sposób mają być chronione.

Z kolei w dokumentach strategicznych NATO używa się pojęć cyberobrona i zapewnianie bezpieczeństwa w cyberprzestrzeni, nie definiuje się natomiast samej kategorii „cyberbezpieczeństwo". W amerykańskich koncepcjach dotyczących bezpieczeństwa narodowego przyjęto zwięzłą definicję cyberbezpieczeństwa jako możliwość ochrony lub obrony cyberprzestrzeni przed cyberatakami[22]. W koncepcji strategicznej NATO obowiązującej na lata 2010–2020, uzgodnionej w Lizbonie 17 listopada 2010 r., cyberataki zostały sklasyfikowane na drugiej pozycji (po terroryzmie międzynarodowym) jako globalne zagrożenie światowego bezpieczeństwa. W natowskim dokumencie podkreślono, że do ataków w przestrzeni cyfrowej dochodzi coraz częściej, są one coraz lepiej zorganizowane i coraz bardziej kosztowne. Cyberbezpieczeństwo stało się bardzo ważne dla NATO zwłaszcza po cyberataku serbskich

[19] T. Pączkowski, *Słownik cyberbezpieczeństwa*, Katowice 2017, s. 10.

[20] Por. W. Gibson, *Neuromancer*, przeł. P. Cholewa, Opole 1992.

[21] Por. np. *E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni*, M. Zwierżdżyński i in. (red.), Kraków 2015.

[22] *Glossary of Key Information Security Terms*, R. Kissel (red.), NIST Interagency or Internal Report (NISTIR) 7298, 2013 r., revision 2, s. 58, https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [dostęp: 14 VIII 2020].

hakerów na strony natowskie w 1999 r., a także po ataku, jakiego w 2007 r. doświadczyła Estonia, a w 2008 r. – Gruzja. Również atak hakerski (najprawdopodobniej izraelski lub izraelsko-amerykański) przeprowadzony w 2010 r. na irańskie wirówki jądrowe pokazał, jak niewielkim kosztem można zadać poważne ciosy, wykorzystując narzędzia cyberwojny w postaci oprogramowania typu *malware* – w tym przypadku robaka komputerowego Stuxnet[23]. Tego rodzaju incydenty skłoniły NATO do podjęcia prac nad przygotowaniem odpowiednich strategii przeciwdziałania nowym zagrożeniom, czego pierwszym efektem było opracowanie w 2010 r. dokumentu *Polityka NATO w dziedzinie cyberobrony* (*The NATO Policy on Cyber Defence*).

Cyberprzestrzeń może być wykorzystana w wojnie psychologicznej, przede wszystkim do zakłócania przebiegu procesów wyborczych i wpływania na opinię publiczną w okresie wyborów. Jest to najczęściej wskazywana możliwość oddziaływania za pośrednictwem internetu na nastroje społeczne. Oprócz wywierania wpływu na bieg życia politycznego jako najbardziej prawdopodobne przyszłe zagrożenie wskazuje się wywoływanie zakłóceń w prawidłowym funkcjonowaniu Internetu rzeczy (*Internet of Things*, IoT). Coraz bardziej powszechne są połączenia przedmiotów, instalacji, obiektów i infrastruktury. Budzi to obawy ekspertów dotyczące możliwości przeprowadzenia ataków hakerskich na Internet rzeczy i dokonywania zniszczeń fizycznych przez wywoływanie awarii oraz katastrof technicznych. Jako jedno z głównych zagrożeń często wskazuje się również cyberterroryzm[24], chociaż jest to niewłaściwy i mylący termin, z którego, zdaniem coraz większej grupy ekspertów, należałoby zrezygnować na rzecz określeń „aktywność terrorystów w Internecie" oraz „cyberataki". Taki pogląd został zaprezentowany m.in. podczas konferencji CyberSec (European Cybersecurity Forum – Europejskie Forum Cyberbezpieczeństwa) w 2017 r., jak również w raporcie Europolu w 2018 r.[25]

Wykorzystanie narzędzi cybernetycznych do celów przestępczych jest określane jako „cyberprzestępczość" i najczęściej jest związane z działaniem transnarodowych grup przestępczości zorganizowanej (TPZ)[26]. Polega ono na dokonywaniu różnych

---

[23] Szerzej na temat cyberwojny zob. m.in.: P. Łuczuk, *Cyberwojna. Wojna bez amunicji*, Kraków 2017; M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015; P.W. Singer, A. Friedman, *Cybersecurity and Cyberwar. What Everyone Needs to Know*, Oxford 2014.

[24] *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, A. Podraza, P. Potakowski, K. Wiak (red.), Warszawa 2013; E. Lichocki, *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, s. 63–80; A. Bógdał-Brzezińska, F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.

[25] *Internet Organised Crime Threat Assessment (IOCTA) 2018*, Europol, Bruksela 2018, s. 52, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 [dostęp: 18 II 2021].

[26] Zob. D. Farbaniec, *Cyberwojna. Metody działania hakerów*, Gliwice 2018, s. 163, 199, 219–228; R. Borkowski, M. Kudzin-Borkowska, *Transnarodowa przestępczość zorganizowana*, w: *Zagrożenia i instytucje bezpieczeństwa międzynarodowego*, E. Cziomer (red.), Kraków 2016, s. 85–100; *Przestępczość w XXI wieku: zapobieganie i zwalczanie: problemy technologiczno-informatyczne*,

rodzajów oszustw, kradzieży informacji (*stealing*) i wyłudzeń (*phishing*), szantażowaniu (*ransomware*), dokonywaniu włamań do systemów komputerowych (*cracking*), stosowaniu botnetów, bomb logicznych, fałszywych alarmów (*hoax*), niszczeniu zasobów informacji przez wirusy komputerowe (*malware*), przekształcaniu oraz wprowadzaniu fałszywej informacji. Również rozwój Darknetu niesie niebezpieczeństwo wzrostu przestępczości zorganizowanej, zarówno o charakterze cyfrowym, jak i klasycznym.

W Polsce koncepcje strategiczne w zakresie cyberbezpieczeństwa są zawarte w pięciu dokumentach strategicznych. Są to: *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020* (opracowana przez Ministerstwo Cyfryzacji w 2016 r.), *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* (opracowana przez Ministerstwo Cyfryzacji w 2017 r.), *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej* (wydana przez Biuro Bezpieczeństwa Narodowego w 2015 r.), *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* (opracowana w Ministerstwie Administracji i Cyfryzacji oraz Agencji Bezpieczeństwa Wewnętrznego w 2013 r.) oraz *Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* (opracowany przez Ministerstwo Spraw Wewnętrznych i Administracji w 2010 r.).

W *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* cyberbezpieczeństwo jest zdefiniowane jako bezpieczeństwo sieci i systemów informatycznych oraz bezpieczeństwo teleinformatyczne i (…) *oznacza odporność systemów teleinformatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych, lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne*[27]. Strategia zakłada intensywną współpracę międzynarodową nie tylko w sferze politycznej, lecz także na poziomie operacyjno-technicznym, co będzie realizowane m.in. z pomocą sieci CSIRT (Computer Security Incident Response Team) w ramach Unii Europejskiej i NATO oraz Grupy V4.

Z kolei w *Doktrynie Cyberbezpieczeństwa Rzeczypospolitej Polskiej* cyberprzestrzeń jest traktowana jako piąte pole walki, gdyż według jej autorów jest polem konfliktu, na którym przychodzi zmierzyć się nie tylko z innymi państwami, lecz także z wrogimi organizacjami, m.in. z grupami ekstremistycznymi, terrorystycznymi czy zorganizowanymi grupami przestępczymi. Doktryna definiuje cyberprzestrzeń bardzo obszernie jako:

> (…) przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne (zespoły współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniające przetwarzanie, przechowywanie, a także

E. Pływaczewski, W. Filipkowski, Z. Rau (red.), Warszawa 2015; J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015.

[27] Ministerstwo Cyfryzacji, Warszawa 2017, www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351a-a025be09 [dostęp: 11 VI 2019].

> wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego przeznaczonego do podłączenia bezpośrednio lub pośrednio do zakończeń sieci) wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

Cyberbezpieczeństwo jest tu zdefiniowane jako (…) *proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni*[28]. Autorzy dokumentu stwierdzają:

> Szansą dla wzmocnienia cyberbezpieczeństwa RP jest wykorzystanie potencjału wynikającego z członkostwa Polski w sojuszniczych strukturach obrony i ochrony cybernetycznej (NATO, UE), ukierunkowane na potrzeby państwa zaangażowanie w prace organizacji międzynarodowych, aktywność na forum gremiów zajmujących się bezpieczeństwem w cyberprzestrzeni, a także bilateralna współpraca z państwami bardziej zaawansowanymi w sprawach cyberbezpieczeństwa.

W omawianym dokumencie nie ma natomiast żadnej wzmianki o współpracy w ramach Grupy Wyszehradzkiej.

W *Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej* cyberprzestrzeń jest definiowana jako (…) *przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne*. W tym dokumencie jest mowa również o bezpieczeństwie cyberprzestrzeni rozumianym jako (…) *zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni*[29]. Wprawdzie autorzy dokumentu stwierdzili, że istotnym elementem jest utrzymanie i rozwijanie współpracy międzynarodowej w tym zakresie, ale nie wspomnieli o partnerach tej współpracy.

W *Rządowym Programie Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* cyberprzestrzeń określono jako (…) *cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*. Autorzy operują pojęciem bezpieczeństwo w cyberprzestrzeni, ale go nie definiują, podają natomiast definicję pojęcia ochrona cyberprzestrzeni, która jest rozumiana jako (…) *zespółprzedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mający na celu niezakłócone funkcjonowanie i bezpieczeństwo*

---

[28] Biuro Bezpieczeństwa Narodowego, Warszawa 2015, http://en.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 14 VIII 2020].

[29] https://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf [dostęp: 29 IX 2018].

cyberprzestrzeni[30]. W zadeklarowanej współpracy międzynarodowej wskazuje się Unię Europejską i NATO, ale nie wspomina się o Grupie V4.

Jak widać, w różnych dokumentach strategicznych cyberbezpieczeństwo jest ujmowane i definiowane w sposób odmienny. W *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022* jest opisywane jako stan bezpieczeństwa sieci i systemów informatycznych oraz stanowi synonim bezpieczeństwa teleinformatycznego, rozumianego również jako odporność systemów. W *Doktrynie Cyberbezpieczeństwa RP* z 2015 r. jest pojmowane z kolei jako proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa i jego instytucji. Widoczne jest zatem, że w RP nie wypracowano dotychczas spójnej, długofalowej koncepcji polityki cyberbezpieczeństwa, a poszczególne instytucje państwa tworzą własne koncepcje. Różnią się one od siebie, zależnie od organu administracji publicznej tworzącego dokument oraz od zachodzących zmian politycznych.

Na Węgrzech jedynym obowiązującym dokumentem państwowym dotyczącym *cybersecurity* jest *Magyarország Nemzeti Kiberbiztonsági Stratégiájáról* (*Strategia Cyberbezpieczeństwa Węgier*) z 2013 r. Cyberprzestrzeń jest w nim określona jako globalnie połączone, zdecentralizowane, zwiększające się zasoby informacji, elektroniczne systemy i dane. Cyberbezpieczeństwo zostało natomiast dość szeroko zdefiniowane jako polityczne, prawne i techniczne narzędzia umożliwiające skuteczne utrzymanie akceptowalnego poziomu ryzyka w cyberprzestrzeni. Strategia zawiera odniesienia do koncepcji strategicznych NATO oraz Unii Europejskiej w zakresie polityki bezpieczeństwa cyberprzestrzeni, nie ma w niej natomiast żadnego nawiązania do Grupy V4. Znajduje się jedynie zapis mówiący o tym, że Węgry poświęcają szczególną uwagę regionowi Europy Środkowej i Wschodniej.

W Republice Czeskiej inicjatywy dotyczące opracowania cyberstrategii podjęto dwukrotnie, przyjmując *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012–2015* (*Strategię w zakresie cyberbezpieczeństwa Republiki Czeskiej na lata 2012–2015*), a następnie *Národní strategie kybernetické bezpečnosti naźobdobí let 2015 až 2020* (*Narodową strategię bezpieczeństwa cybernetycznego na lata od 2015 do 2020*). Ani w pierwszym, ani w drugim dokumencie nie zdefiniowano pojęć „cyberbezpieczeństwo" oraz „cyberprzestrzeń" [31]. Jeśli chodzi o współpracę międzynarodową, to w pierwszym z nich zadeklarowano współdziałanie w ramach Unii Europejskiej, NATO, Organizacji Narodów Zjednoczonych, Organizacji Współpracy Gospodarczej i Rozwoju (dalej: OECD), Międzynarodowej Unii Telekomunikacyjnej oraz innych organizacji międzynarodowych, a w strategii aktualnie obowiązującej podkreśla się znaczenie współpracy międzynarodowej, ale w sposób wyjątkowo ogólny, i w ogóle nie

[30] Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010, www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [dostęp: 17 X 2020].

[31] Národní úřad pro kybernetickou a informační bezpečnost, https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf [dostęp: 9 III 2020].

wspomina się o Grupie V4[32]. Deklaruje się aktywne wspieranie partnerów międzynarodowych w zapobieganiu cyberatakom i promowanie cyberbezpieczeństwa oraz współpracy w dziedzinie obronności, jak również budowanie dialogu dotyczącego tych kwestii między krajami środkowoeuropejskimi. W towarzyszących planach działania (czes. *Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období 2012–2015* oraz *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020*) problematyka współpracy Republiki Czeskiej z Grupą V4 została nakreślona jako współdziałanie w ramach Środkowoeuropejskiej Platformy Cyberbezpieczeństwa (Central European Cyber Security Platform, CECSP) utworzonej przez Austrię i Czechy.

Na Słowacji jako pierwszą przyjęto strategię o nazwie *Národná stratégia pre informačnú bezpečnosť v Slovenskej republike 2008* (*Narodowa strategia na rzecz bezpieczeństwa informacyjnego Republiki Słowacji 2008*). Siedem lat później został ogłoszony obowiązujący do dziś dokument zatytułowany *Koncepcia kybernetickej bezpecnosti Slovenskej republiky na roky 2015–2020* (*Koncepcja bezpieczeństwa cybernetycznego Republiki Słowacji na lata 2015–2020*)[33]. W pierwszej strategii pojęcie „cyberbezpieczeństwo" w ogóle nie występuje, mówi się natomiast o aspekcie cybernetycznym, elektronicznym oraz infrastruktury krytycznej w odniesieniu do bezpieczeństwa informacyjnego, ale nie definiuje się żadnego z tych pojęć. Wskazuje się na znaczenie współpracy międzynarodowej w ramach UE, OECD, ISO (Międzynarodowa Organizacja Normalizacyjna) oraz z Republiką Czeską, nie wymienia się natomiast Grupy V4. W koncepcji obowiązującej aktualnie pojęcie „cyberbezpieczeństwo" jest zdefiniowane obszernie i zawile jako system ciągłego podnoszenia świadomości politycznej, prawnej i ekonomicznej, a także system podnoszenia poziomu bezpieczeństwa i obrony oraz zwiększania skuteczności przyjętych i stosowanych techniczno-organizacyjnych środków zarządzania ryzykiem w cyberprzestrzeni. W ten sposów zmierza sie do jej przekształcenia w środowisko godne zaufania, które pozwoli na bezpieczne funkcjonowanie społeczne i gospodarcze.

Jeżeli chodzi o wspólne działania czterech państw regionu na rzecz cyberbezpieczeństwa i bezpieczeństwa teleinformatycznego, to już w Deklaracji Wyszehradzkiej z 15 lutego 1991 r. znajduje się zapowiedź, że państwa członkowskie skoordynują rozwój swoich systemów energetycznych i sieci telekomunikacyjnych. Z biegiem czasu, wraz z ewolucją zagrożeń w sferze bezpieczeństwa wynikającą m.in. z członkostwa w NATO, komponent cyberprzestrzenny zyskała również współpraca wojskowa i policyjna[34]. Państwa Grupy V4 wypracowały swoje własne strategie cyberbezpieczeństwa na podstawie światowych wzorców w tej dziedzinie. W tych dokumentach zgłaszają

[32] Národní bezpečnosti úřad, https://www.cybersecurity.cz/data/navratil2014.pdf [dostęp: 5 IX 2020].

[33] Národný bezpečnostný úrad, https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf [dostęp: 22 XII 2019].

[34] *Współpraca państw Grupy Wyszehradzkiej w zapewnianiu cyberbezpieczeństwa – analiza i rekomendacje*, J. Świątkowska (red.), Kraków 2012.

wprawdzie gotowość szerokiej współpracy międzynarodowej, w tym środkowoeuropejskiej, jednak można zauważyć, że każdy z krajów członkowskich ma ambicje odgrywania roli lidera w regionie.

W czasie poszczególnych prezydencji w Radzie UE kraje członkowskie Grupy V4 deklarowały rozmaite wspólne inicjatywy. Postulat współpracy w dziedzinie cyberbezpieczeństwa został po raz pierwszy wyeksponowany w 2007 r., podczas prezydencji Republiki Czeskiej. W 2012 r. Polska, podczas swojej prezydencji, zapowiedziała konsultacje w sprawie bezpieczeństwa z udziałem również państw bałtyckich oraz Bułgarii i Rumunii, co stanowiło wyraźny przejaw dążenia do tworzenia tzw. Międzymorza. Z kolei Węgry w 2014 r. zaproponowały powołanie grupy roboczej poświęconej cyberobronie (Cyber Defence Working Group).

Wśród form działania na rzecz intensyfikacji polityki bezpieczeństwa cybernetycznego Grupy V4 trzeba wskazać wspólne ćwiczenia i warsztaty w rodzaju Cyber Visegrad Workshop, a także inicjatywy podejmowane w szerszym wymiarze, jak Europejskie Forum Cyberbezpieczeństwa. Strona polska aspiruje do roli regionalnego lidera i dąży do tego, aby rekomendacje wypracowywane w trakcie CyberSec pozwalały na wzmocnienie współpracy między państwami Grupy V4, Morza Bałtyckiego oraz innymi państwami Europy Centralnej na rzecz ochrony cyberprzestrzeni. Efektem konferencji, która odbyła się w 2016 r., było powołanie w Krakowie Cybersec Hub w celu stworzenia efektywnego sektora produktów i usług w obszarze cyberbezpieczeństwa oraz szkolenia światowej klasy cyberspecjalistów.

Bilans dotychczasowej współpracy na rzecz wypracowania wspólnej polityki bezpieczeństwa Grupy V4 w cyberprzestrzeni okazuje się jednak skromny. Największe osiągnięcia można dostrzec w zwalczaniu cyberprzestępczości, co wynika przede wszystkim z dobrze rozwiniętej regionalnej współpracy policyjnej w zwalczaniu przestępczości zorganizowanej. Znacznie mniej skuteczne są jest walka ze szpiegostwem w sieci oraz przeciwdziałanie zagrożeniom militarnym w cyberprzestrzeni. Na przeszkodzie do osiągnięcia spójności działań stoi wzajemna rywalizacja polityczna każdego z czterech państw oraz partykularne interesy elit rządzących. Zarówno Polska, jak i Węgry, Czechy czy Słowacja starają się rozwijać bezpośrednią współpracę z wiodącymi ośrodkami na Zachodzie, pomijając w tych staraniach wspólnotę wyszehradzką. Polska skupia swoje wysiłki na współpracy z państwami bałtyckimi, w tym przede wszystkim z wiodącym natowskim ośrodkiem CCDCOE (The NATO Cooperative Cyber Defence Centre of Excellence) w Tallinie. Konkurencja, której skutkiem jest brak wspólnej wizji polityki cyberbezpieczeństwa, osłabia Grupę Wyszehradzką i powoduje, że staje się ona trzeciorzędnym graczem w obszarze *cybersecurity*. Symptomatyczne, że nawet Środkowoeuropejska Platforma Cyberbezpieczeństwa utworzona w 2013 r. nie była przedsięwzięciem podjętym w ramach Grupy V4, lecz powstała z inicjatywy Austrii i Czech, do których dołączyły później Słowacja, Polska i Węgry. W istocie kraje Grupy V4 wykazują bierność – realizują kierunki rozwoju cyberbezpieczeństwa wytyczone rekomendacjami zawartymi w dokumentach strategicznych NATO oraz Unii Europejskiej i rozwijają swoją cyberobronę m.in. z pomocą narodowych zespołów

reagowania na zagrożenia komputerowe, czyli CERT-ów (Computer Emergency Response Team), ale nie robią nic ponadto[35]. Jak twierdzi Bogusław Olszewski, można postawić tezę, że w sferze cyberbezpieczeństwa Grupa V4 stanowi wtórną platformę współpracy państw Europy Środkowej, przy czym każde z państw członkowskich ma ambicje zaistnienia w tej dziedzinie i zamiast pełnego współdziałania w regionie jest widoczna wyraźna konkurencja[36].

Symptomatyczna dla braku konsolidacji w obszarze *cybersecurity* w Grupie V4 jest tzw. afera Huawei. Z całą ostrością uwidoczniły sie tu nie tylko kwestie związane z cyberbezpieczeństwem, lecz także ze stosunkiem do polityki amerykańskiej, co doprowadziło do licznych międzynarodowych napięć. Koncern utworzony w latach 80. XX w. we współpracy z chińskimi wojskami inżynieryjnymi jest obecnie największym na świecie producentem sprzętu telekomunikacyjnego, a także dostawcą technologii IT. Stany Zjednoczone, Australia i Kanada uznały w 2012 r., że współpraca z Huawei stanowi zagrożenie ich cyberbezpieczeństwa i oskarżyły koncern o cyberszpiegostwo przez umieszczanie w swoich urządzeniach oprogramowania umożliwiającego ich zdalną kontrolę. Wielka Brytania, USA, Japonia, Australia i Nowa Zelandia zdecydowały o zablokowaniu prac Huawei nad rozwojem sieci 5G na swoich rynkach cyfrowych. Prezydent USA dodatkowo zadekretował zakaz korzystania z technologii koncernów Huawei i ZTE przez administrację amerykańską i firmy z nią współpracujące. Departament Sprawiedliwości USA przedstawił Huawei 13 zarzutów, dotyczących m.in. łamania amerykańskich sankcji nałożonych na Iran, a także oszustw bankowych i elektronicznych oraz szpiegostwa przemysłowego. Stany Zjednoczone wystąpiły również z formalnym wnioskiem o ekstradycję wiceprezes koncernu Meng Wanzhou aresztowanej w Kanadzie, oskarżanej o oszustwa.

Na rynku środkowoeuropejskim firma Huawei jest obecna od 2011 r. W Polsce miała wspierać rozwój sieci 5G przez dostarczenie komponentów do budowy jej infrastruktury i podjęcie w 2018 r. współpracy z operatorami Orange i T-Mobile. Podobnie działo się w Czechach, gdzie chińskie inwestycje i współpraca Huawei z koncernem telekomunikacyjnym PPF oraz energetycznym ČEZ cieszą się poparciem prezydenta państwa Miloša Zemana. Jednakże pod koniec 2018 r. Narodowy Urząd ds. Bezpieczeństwa Cybernetycznego i Informatycznego Republiki Czeskiej (NUKIB) wydał ostrzeżenie o możliwym zagrożeniu bezpieczeństwa państwa związanym z urządzeniami produkowanymi przez firmy Huawei i ZTE. Premier Czech Andrej Babisz zwołał posiedzenie Rady Bezpieczeństwa Państwa, która krytycznie odniosła się do enuncjacji NUKIB, zalecając Krajowemu Urzędowi ds. Bezpieczeństwa Sieci i Informacji (NUCK) wydawanie ostrzeżeń dotyczących wyłącznie systemów sklasyfikowanych

[35] J. Dereń, A. Rabiej, *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*, w: *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, M. Górka (red.), Warszawa 2014, s. 202–221; *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014*, Warszawa 2015.

[36] B. Olszewski, *Perspektywy regionalizacji cyberbezpieczeństwa w ramach Grupy Wyszehradzkiej*, w: *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa*, H. Chałupczak, M. Pietraś, J. Misiągiewicz (red.), Zamość 2016, s. 203–215.

jako infrastruktura krytyczna lub ważne systemy informacyjne, lecz nie w odniesieniu do zwykłych użytkowników oraz urządzeń końcowych. Ostatecznie premier opowiedział się za tym, aby kwestię obecności Huawei na rynku europejskim rozwiązywała Unia Europejska. Tymczasem Węgry odrzuciły amerykańską propozycję przyłączenia się do walki z chińskim szpiegostwem cybernetycznym. Premier Viktor Orbán oświadczył, że zamierza prowadzić neutralną politykę zagraniczną na wzór Austrii, a nie spełniać żądania USA. Analogiczne stanowisko zajęła Słowacja, która nie podjęła żadnych kroków przeciwko Huawei. Premier Peter Pellegrini ogłosił, że brakuje dowodów na szpiegowską działalność chińskiego koncernu, w związku z czym Słowacja nie uznaje go za zagrożenie bezpieczeństwa i nie nałoży na niego restrykcji, dopóki nie pojawią się przeciwko niemu konkretne dowody. Podkreślił też, że słowackie organy nadzorcze i służby bezpieczeństwa nie wydały podobnego ostrzeżenia jak służby czeskie. Eksperci wskazują, że afera Huawei jest elementem rozgrywki w amerykańsko-chińskich sporach handlowych. W tym miejscu warto przypomnieć, że w styczniu 2019 r. w Polsce Agencja Bezpieczeństwa Wewnętrznego zatrzymała dwie osoby pod zarzutem z art. 130 ust. 1 *Kodeksu karnego*[37], który mówi o szpiegostwie przeciw RP. Wśród zatrzymanych był dyrektor polskiego oddziału Huawei, który w latach 2006–2011 piastował stanowisko w konsulacie generalnym Chińskiej Republiki Ludowej w Gdańsku. Zdaniem dr Justyny Szczudlik (kierownik programu Azji i Pacyfiku w Polskim Instytucie Spraw Międzynarodowych): (…) *firma Huawei prawdopodobnie realizuje interesy chińskiego rządu i może być narzędziem wpływu stosowanym przez Chiny w innych państwach. Nie można wykluczyć scenariusza, że nasza część Europy może stać się miejscem rywalizacji USA i Chin*[38].

Polityczny charakter rywalizacyjnych posunięć Warszawy, Pragi, Bratysławy i Budapesztu powoduje, że nie ma spójnej i konsekwentnej współpracy Grupy V4 w dziedzinie cyberbezpieczeństwa. Przyczyn słabości należy szukać w różnicach polityki wobec Rosji i Ukrainy, polityki energetycznej i zakupów gazu ziemnego oraz polityki wobec Brukseli. Widoczne jest, że Polska skłania się do regionalizacji cyberbezpieczeństwa w kierunku północnym, a nie wyszehradzkim, tj. do współpracy z państwami bałtyckimi, z wiodącym centrum CCDCOE w Tallinie, które jest wielonarodowym, interdyscyplinarnym ośrodkiem cyberobrony. Konceptualizacje cyberbezpieczeństwa w dokumentach strategicznych poszczególnych państw Grupy V4 różnią się od siebie i dotychczas nie podjęto żadnej próby ujednolicenia podejścia do tego problemu w obrębie Grupy. Nie można więc mówić o jej wspólnej i spójnej polityce dotyczącej cyberbezpieczeństwa. Współpraca w tym zakresie jest słabo rozwinięta i nawet w sferze deklaratywnej nie widać wyraźnej woli elit państw tej Grupy, aby ją budować, rozwijać i pogłębiać.

---

[37] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

[38] *Dyrektor Huawei i były funkcjonariusz ABW zatrzymani pod zarzutem szpiegostwa*, „Newsweek", 11 I 2019 r., https://www.newsweek.pl/polska/dyrektor-huawei-i-byly-funkcjonariusz-abw-zatrzymani-pod-zarzutem-szpiegostwa/rp8vxq5 [dostęp: 29 VI 2020].

Bibliografia

Banasiński C., *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, Wolters Kluwer.

Bayuk J.L. i in., *Cyber Security Policy Guidebook*, Hoboken 2012, Wiley-Blackwell.

Bezpieczeństwo teleinformatyczne państwa, M. Madej, M. Terlikowski (red.), Warszawa 2009, Polski Instytut Spraw Międzynarodowych.

Borkowski R., *Cywilizacja, technika, ekologia. Wybrane problemy rozwoju cywilizacyjnego u progu XXI wieku*, Kraków 2001, Wydawnictwa AGH.

Bógdał-Brzezińska A., Gawrycki F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, Oficyna Wydawnicza ASPRA-JR.

Cyberbezpieczeństwo jako podstawa bezpieczeństwa państwa i społeczeństwa w XXI wieku, M. Górka (red.), Warszawa 2016, Difin.

Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna, A. Podraza, P. Potakowski, K. Wiak (red.), Warszawa 2013, Difin.

Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa, H. Chałupczak, M. Pietraś, J. Misiągiewicz (red.), Zamość 2016, Wydawnictwo „Officina Simonidis".

E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni, M. Zwierżdżyński i in. (red.), Kraków 2015, Akademia Ignatianum.

Jańczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, Akademia Obrony Narodowej.

Jaźwiński J., Ważyńska-Fiok K., *Bezpieczeństwo systemów*, Warszawa 1993, Wydawnictwo Naukowe PWN.

Korzeniowski L.F., *Securitologia: nauka o bezpieczeństwie człowieka i organizacji społecznych*, Chorzów 2009, Wydawnictwo Wyższej Szkoły Bankowej WZ w Chorzowie.

Kossecki J., *Cybernetyka społeczna*, Warszawa 1981, PWN.

Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Katowice 2015, Wydawnictwo Uniwersytetu Śląskiego.

Lakomy M., *Dylematy polityki cyberbezpieczeństwa Polski*, w: *Dylematy polityki bezpieczeństwa Polski na początku drugiej dekady XXI wieku*, K. Czornik, M. Lakomy (red.), Katowice 2014, Wydawnictwo Regionalnego Ośrodka Debaty Międzynarodowej, s. 425–454.

Lichocki E., *Cyberterroryzm jako nowa forma zagrożeń dla bezpieczeństwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, Difin, s. 63–80.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2009, Wydawnictwo Naukowe PWN.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2015, Wydawnictwo Naukowe PWN.

Liedel K., *Bezpieczeństwo informacyjne państwa*, w: *Transsektorowe obszary bezpieczeństwa narodowego*, K. Liedel (red.), Warszawa 2011, Difin, s. 45–62.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2014, Wydawnictwo Adam Marszałek.

Liedel K., *Cyberbezpieczeństwo – wyzwania przyszłości. Działania społeczności międzynarodowej*, w: *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, K. Liedel, P. Piasecka, T. Aleksandrowicz (red.), Warszawa 2011, Difin, s. 437–448.

Ochrona informacji niejawnych w XXI wieku, S. Topolewski (red.), Siedlce 2016, Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego.

Pączkowski T., *Słownik cyberbezpieczeństwa,* Katowice 2017, Szkoła Policji w Katowicach.

Przestępczość w XXI wieku: zapobieganie i zwalczanie: problemy technologiczno-informatyczne, E. Pływaczewski, W. Filipkowski, Z. Rau (red.), Warszawa 2015, Wolters Kluwers.

Pręgiel R., Buchwald P., *Internet w społeczeństwie informacyjnym – nowoczesne systemy informatyczne i ich bezpieczeństwo*, Dąbrowa Górnicza 2014, Wydawnictwo Wyższej Szkoły Biznesu.

Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2014, Warszawa 2015, CERT ABW.

Singer P.W., Friedman A., *Cybersecurity and Cyberwar. What Everyone Needs to Know*, Oxford 2014, Oxford University Press.

Strnád O., *Riadenie rizík informačnej bezpečnosti*, Ostrava 2010, Amos.

Współpraca państw Grupy Wyszehradzkiej w zapewnianiu cyberbezpieczeństwa – analiza i rekomendacje, J. Świątkowska (red.), Kraków 2012, Instytut Kościuszki.

Źródła internetowe

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej, Biuro Bezpieczeństwa Narodowego, Warszawa 2015, www.bbn.gov.pl/ftp/dok/01/DCB.pdf [dostęp: 14 VIII 2020].

Dyrektor Huawei i były funkcjonariusz ABW zatrzymani pod zarzutem szpiegostwa, „Newsweek", 11 I 2019 r., www.newsweek.pl/polska/dyrektor-huawei-i-byly-funkcjonariusz-abw-zatrzymani-pod-zarzutem-szpiegostwa/rp8vxq5 [dostęp: 29 VI 2020].

Glossary of Key Information Security Terms, Kissel R. (red.), NISTIR 7298, rev. 2, 2013, https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [dostęp: 14 VIII 2020].

Internet Organised Crime Threat Assessment (IOCTA) 2018, Europol, Bruksela, 2018 r., www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018 [dostęp: 18 II 2021].

Koncepcia kybernetickej bezpecnosti Slovenskej republiky na roky 2015–2020, Národný bezpečnostný úrad, https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Koncepcia-kybernetickej-bezpecnosti-SR-na-roky-2015-2020-A4.pdf [dostęp: 22 XII 2019].

Národní strategie kybernetické bezpečnosti na období let 2015 až 2020, Národní bezpečnosti úřad, www.cybersecurity.cz/data/navratil2014.pdf [dostęp: 5 IX 2020].

Národní úřad pro kybernetickou a informační bezpečnost, www.govcert.cz/download/legislativa/containernodeid719/20120209strategieprooblastkbnbu.pdf [dostęp: 9 III 2020].

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, https://jakubow.pl/wp-content/uploads/2015/06/Polityka-Ochrony-Cyberprzestrzeni-RP_148x210_wersja-pl.768174_715482.pdf [dostęp: 29 IX 2018].

Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016, Ministerstwo Spraw Wewnętrznych i Administracji, Warszawa 2010 r., www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf [dostęp: 17 X 2020].

Snow B., *What Would a World Without Internet Look Like? A thought experiment*, „The Atlantic", 5 IV 2016 r., www.theatlantic.com/technology/archive/2016/04/a-world-without-internet/476907/ [dostęp: 18 II 2021].

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, Ministerstwo Cyfryzacji, Warszawa 2017 r., www.gov.pl/documents/31305/0/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/f249b627-4050-a6f4-5cd3-351aa025be09 [dostęp: 11 VI 2019].

Abstrakt

W artykule podjęto problematykę cyberbezpieczeństwa w Grupie Wyszehradzkiej. Mimo że w nauce pojawia się wiele terminów dotyczących bezpieczeństwa informacyjnego, jednak w ostatnich latach w dokumentach strategicznych dominuje kategoria pojęciowa „cyberbezpieczeństwo". W *Strategii Bezpieczeństwa Cybernetycznego Unii Europejskiej* z 7 marca 2013 r. stwierdza się, że bezpieczeństwo cybernetyczne odnosi się do zabezpieczeń i działań, które mogą być wykorzystywane do ochrony domeny cybernetycznej, zarówno cywilnej, jak i wojskowej, przed tymi zagrożeniami, które dotyczą

jej współzależnych sieci i infrastruktury informatycznej oraz które mogą te sieci oraz tę infrastrukturę uszkodzić. Państwa Grupy Wyszehradzkiej wypracowały swoje własne strategie cyberbezpieczeństwa na podstawie światowych wzorców w tej dziedzinie. W tych dokumentach deklarują wprawdzie gotowość współpracy międzynarodowej, także środkowoeuropejskiej, jednak widać, że każde z nich ma ambicje odgrywania roli środkowoeuropejskiego lidera.

Słowa kluczowe: cyberbezpieczeństwo, strategie cyberbezpieczeństwa, Grupa Wyszehradzka, bezpieczeństwo teleinformatyczne, bezpieczeństwo informacyjne.

Cybersecurity in the Visegrad Group – concepts and strategies

Abstract

The article discusses the issues of cybersecurity in the Visegrad Group. There is a wide spectrum of information security terminology, but the conceptual category of cybersecurity has dominated strategic documents in recent years. The European Union Cyber Security Strategy of 7, March 2013, claims that cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. The Visegrad Group countries have developed their own cybersecurity strategies based on global models in this field. However, in these strategic documents they declare readiness for broad international cooperation, including Central European, it can be seen that each of them strives to play the role of a leader in Central Europe.

Keywords: cybersecurity, cybersecurity strategies, the Visegrad Group, ICT security, information security.