

Daria Krzewniak

ORCID: 0000-0003-1085-8361

daria.krzewniak@uph.edu.pl

Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach
Wydział Nauk Społecznych

Cyberprzesterzeń jako środowisko bezpieczeństwa

Henryk Wyrębek, *Cyberprzestrzeń. Zagrożenia. Strategie cyberbezpieczeństwa*, Wydawnictwo Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce 2021, ss. 219

DOI: 10.34739/doc.2022.19.16

Rozwój technologii informacyjno-komunikacyjnych napędza postęp cywilizacyjny, społeczny i gospodarczy. Wdrażane innowacje sprawiają, że współczesny świat stał się dualny i symultaniczny – realny i wirtualny zarazem¹. Te dwa wymiary tworzą środowisko, w którym kształtuje się i nieustannie rozwija społeczeństwo informacyjne. Istotnym atrybutem tego społeczeństwa jest traktowanie informacji jako kluczowego zasobu, szczególnego rodzaju dobra niematerialnego, porównywalnego wartością do dóbr materialnych bądź cenniejszego od nich. Informacja w społeczeństwie informacyjnym stanowi źródło przewagi konkurencyjnej, a jednocześnie zapewnia wzrost poziomu adaptacyjności społecznej, w wymiarze jednostkowym i ogólnym, w kontekście dynamicznie zmieniającej się rzeczywistości.

Współcześnie ważną sferą generowania, przetwarzania i wymiany informacji jest cyberprzestrzeń. Termin ten po raz pierwszy został użyty w 1984 roku przez Williama Gibsona – amerykańskie-

¹ J. Grubicka, A. Kamińska-Nawrot, *Wstęp*, [w:] *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni*, red. J. Grubicka, A. Kamińska-Nawrot, Słupsk 2020, s. 5.

go autora powieści science-fiction pt. *Neuromancer*. Pojęciem tym określił on rodzaj przestrzeni „zbiorowej halucynacji”, doświadczanej przez użytkowników wirtualnej, trójwymiarowej przestrzeni elektronicznego medium komunikacyjnego². Pisał, że cyberprzestrzeń to: „konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczone pojęć matematycznych... Graficzne odwzorowanie danych pobieranych z banku wszystkich komputerów świata. Niewyobrażalna złożoność...”³. W momencie, kiedy w umyśle autora zrodziła się ta koncepcja, nie miał on dostępu ani do komputera, ani tym bardziej do internetu. Swoim pomysłem sprowokował jednak dyskusję, w następstwie której pojęcie „cyberprzestrzeń” zaczęto odnosi do sieci komputerowych i telekomunikacyjnych, określanych poprzez jej elementarne atrybuty środowiskowe, jak gigantyczna przestrzeń danych, współużytkowanie różnorodnych zasobów, globalny zasięg traktowany jako tzw. bezprzestrzenność, czyli niemożność zwymiarowania itd.⁴

Słowo to na stałe zagościło nie tylko w mowie potocznej, ale także na gruncie naukowym. W literaturze przedmiotu funkcjonuje szereg definicji wyjaśniających termin „cyberprzestrzeń”. P. Levy pod pojęciem tym rozumie „przestrzeń otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących w całym świecie”⁵. M. Golka natomiast stoi na stanowisku, że istotą cyberprzestrzeni jest „przestrzeń komunikowania się przez internet oraz wszelkie nośniki danych cyfrowych. Jest to oczywiście przestrzeń nieokreślona, bez możliwości wyobrażenia jej sobie w wymiarze fizycznym”⁶. W ustawodawstwie polskim z kolei omawiany termin definiuje się jako „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatycz-

² M. Koziński, *Cyberprzestrzeń. Poszukiwanie bezpieczeństwa w obliczu współczesnych zagrożeń*, Słupsk 2015, s. 32.

³ W. Gibson, *Neuromancer*, przekł. P.W. Cholewa, Poznań 2006, s. 43.

⁴ G. Pilarski, *Cyberprzestrzeń – relacje w wojnie hybrydowej*, Warszawa 2020, s. 16.

⁵ P. Levy, *Drugi potop*, [w:] *Nowe media w komunikacji społecznej w XX wieku*, red. P. Hopfinger, Warszawa 2002, s. 380.

⁶ M. Golka, *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Warszawa 2008, s. 99.

ne, (...) wraz z powiązaniem pomiędzy nimi oraz relacjami z użytkownikami”⁷.

Cyberprzestrzeń tworzy szereg nowych możliwości, m.in. w zakresie komunikacji, edukacji, realizacji zobowiązań zawodowych czy wypoczynku, ale jednocześnie wprowadza chaos – będący rezultatem nadmiaru dostępnych informacji (powodując m.in. stres informacyjny) oraz rozluźnienie więzi międzyludzkich. Korzystanie z cyberprzestrzeni przyczyniło się także do pojawienia się wielu chorób informacyjnych (np. uzależnienie od internetu) czy atomizacji społeczeństwa⁸, jak również do szeregu innych trudności, problemów i niebezpieczeństw, zarówno w wymiarze personalnym, jak i strukturalnym.

W celu ograniczenia skutków zagrożeń wynikających z funkcjonowania w cyberprzestrzeni podejmowane są liczne próby zapewnienia nad jej zawartością oraz określenia zasad jej funkcjonowania. Aktywność tę podejmują podmioty na różnych szczeblach i o różnym charakterze, np. poszczególne kraje czy organizacje międzynarodowe, ale także administratorzy witryn internetowych. Formułują one zapisy w postaci rezolucji, rozporządzeń, dyrektyw, decyzji, regulaminów, komunikatów, konwencji, doktryn, programów czy strategii ukierunkowanych na ochronę i obronę w cyberprzestrzeni ważnych wartości z punktu widzenia społeczności międzynarodowej, poszczególnych państw i ich obywateli. Wspólnym bowiem mianownikiem wymienionych podmiotów jest dążenie do ograniczenia i zwalczania wszelkich zagrożeń dla ich egzystencji, tożsamości, przetrwania, stabilności i rozwoju.

Obecnie rozwój mediów cyfrowych i interaktywnych technologii informacyjno-komunikacyjnych jest wyjątkowo dynamiczny. Najnowsze urządzenia cyfrowe, tworzące świat nowych technologii, w sposób globalny wpływają na przemiany w zakresie odmiennych od dotychczasowych możliwości zapewniania bezpieczeństwa podmiotom fizycznym i prawnym w cyberprzestrzeni. Cenną pozycję naukową w kontekście przywołanej problematyki stanowi mono-

⁷ Ustawa z 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. 2002 nr 156, poz. 1301 z późn. zm., art. 2 ust. 1b.

⁸ B. Taraszkiewicz, *Znaczenie ekologii informacji w cyberprzestrzeni*, [w:] *Współczesny człowiek wobec zagrożeń...*, s. 80.

grafia naukowa pt. *Cyberprzestrzeń. Zagrożenia. Strategie cyberbezpieczeństwa* autorstwa Henryka Wyrębka, wydana nakładem Wydawnictwa Naukowego Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Celem opracowania jest analiza uwarunkowań funkcjonowania cyberprzestrzeni wraz z zagrożeniami cyberbezpieczeństwa oraz prawną jej ochroną na poziomie międzynarodowym, europejskim i krajowym – polskim⁹.

Problem badawczy przyjął następującą postać: W jakim zakresie zagrożenia cyberbezpieczeństwa wpływają na funkcjonowanie cyberprzestrzeni, a także czy jej ochrona prawna jest wystarczająca do zapewnienia bezpieczeństwa? Omawiana monografia wpisuje się w szeroki kontekst rozważań poświęconych różnicowanemu aspektom bezpieczeństwa w cyberprzestrzeni. Autor podjął się niebywale trudnego zadania – przedstawienia w sposób uporządkowany dotychczasowej wiedzy z zakresu cyberbezpieczeństwa, funkcjonującej na gruncie nauk o bezpieczeństwie, nauk prawnych oraz nauk o polityce i administracji z zachowaniem należytą sekwencji przekazywanych treści.

Przyjęta struktura opracowania odzwierciedla tok analizy konieczny dla udzielenia rzetelnej odpowiedzi na sformułowany problem badawczy. Wyniki dociekań naukowych autor przedstawił w dwóch częściach, obejmujących łącznie dziewięć rozdziałów. Pierwsza omawia istotę cyberprzestrzeni oraz zasadnicze zagrożenia cyberbezpieczeństwa, druga zaś opisuje prawną ochronę cyberprzestrzeni na poziomie Organizacji Narodów Zjednoczonych, Unii Europejskiej oraz Polski. Recenzowana pozycja opatrzona jest wstępem, zakończeniem oraz bibliografią. Autor zawarł w niej także streszczenie oraz słowa kluczowe w języku polskim i angielskim, wykaz zastosowanych skrótów i dwa załączniki – strukturę organizacyjną krajowego systemu cyberbezpieczeństwa oraz chronologiczne zestawienie dokumentów w zakresie ochrony prawnej cyberbezpieczeństwa Polski. Dzieło, poza licznymi, interesującymi poznawczo zagadnieniami, charakteryzuje się również wartościami prakseologicznymi. Stwarza bowiem podbudowę teoretyczną do podejmowania działań na rzecz czynienia cyberprzestrzeni bardziej bezpieczną.

⁹ H. Wyrębek, *Cyberprzestrzeń. Zagrożenia. Strategie cyberbezpieczeństwa*, Siedlce 2021.

H. Wyřbek wskazuje, że cyberprzestrzeń stała się nowym, niezwykle ważnym środowiskiem bezpieczeństwa, czego konsekwencją jest konieczność dokonania szeregu zmian zarówno w zakresie pragmatyki, jak i prawno-organizacyjnego wymiaru funkcjonowania systemów bezpieczeństwa na świecie. W jego opinii konieczne jest zatem zrozumienie dynamiki i kierunku przeobrażeń tego środowiska¹⁰. Punktem wyjścia do rozważań nad tymi kwestiami autor czyni pojęcie cyberprzestrzeni (rozdział 1). Badacz przywołuje liczne definicje wskazanego zagadnienia, zaznaczając, że „termin ten może być największym wyzwaniem zarówno dla analizy badawczej, jak i interpretacji”¹¹.

Faktem jest, że znaczne rozbieżności w wyjaśnianiu istoty cyberprzestrzeni stanowią przeszkodę – z perspektywy formalno-prawnej – w uregulowaniu kwestii bezpieczeństwa na poziomie państwowym i międzynarodowym. Przegląd stanowisk polskich i zagranicznych badaczy oraz instytucji kreujących środowisko bezpieczeństwa, stwarzający szeroką perspektywę badawczą, pozwolił H. Wyřbkowi wysnuć wniosek, że przywołane interpretacje pojęcia *cyberprzestrzeń* koncentrują się przede wszystkim na komponencie narzędziowym, pomijając bądź ignorując społeczny wymiar tego środowiska, wskazujący na jego użytkowników¹². Ich rola w zapewnianiu bezpiecznego korzystania z sieci i informacji jest przecież niebagatelna. To często człowiek stanowi najsłabsze ogniwo w procesie ochrony i obrony cyberprzestrzeni, ale jednocześnie jego kwalifikacje pozwalają niejednokrotnie uniknąć wielu trudnych sytuacji czy ograniczyć ich potencjalnie negatywne oddziaływanie na bezpieczeństwo różnych podmiotów. Liczne sytuacje kłopotliwe wynikają m.in. ze specyficznych ograniczeń cyberprzestrzeni, do których H. Wyřbek (za P. Sienkiewiczem) zalicza: prawo, przestrzeń, zagrożenia, bezpieczeństwo¹³.

Cyberprzestrzeń powstała w wyniku upowszechniania się technologii informatycznych. Stanowi dla jej użytkowników zupełnie nową płaszczyznę aktywności – środowisko działań o bardzo specyficznym charakterze. Odnosi się to nie tylko do podmiotów

¹⁰ Ibidem, s. 8.

¹¹ Ibidem, s. 14.

¹² Ibidem, s. 22.

¹³ Ibidem, s. 24.

korzystających z zasobów informatycznych i informacyjnych zgodnie z obowiązującymi zasadami i w myśl litery prawa, lecz również i tych, którzy mogą wykorzystywać najnowsze technologie w celach z pogranicza patologii społecznych, działań o charakterze przestępczym, terrorystycznym czy militarnym. Niewątpliwym atutem omawianej publikacji jest zatem zwrócenie uwagi na kategorie użytkowników cyberprzestrzeni, którzy stanowią zagrożenie dla jej stabilnego, harmonijnego, bezpiecznego funkcjonowania. Autor monografii wymienia cyberchuliganów, cyberaktywistów, cyberprzestępców, cyberterrorystów, cyberszpiegów oraz cyberżołnierzy¹⁴.

Współczesna cyberprzestrzeń stanowi przestrzeń otwartego komunikowania się, bazującego na połączeniach systemów komputerowych i powiązaniach informatycznych oraz informacyjnych – funkcjonujących w zglobalizowanym systemie geostrategicznych stosunków o charakterze polityczno-gospodarczo-społecznym. Współzależność ta wykreowała szereg nowych wyzwań i zagrożeń dla bezpieczeństwa pojedynczych ludzi, ale także całych narodów, państw i społeczności międzynarodowej¹⁵. W tym kontekście H. Wyrębek w sposób uporządkowany przedstawia charakterystykę najistotniejszych zagrożeń cyberbezpieczeństwa, przejrzysto dyskontuje dotychczasowy dorobek teoretyczny i eksploracyjny w tym zakresie. Badacz odwołuje się zarówno do uregulowań prawnych, jak i ustaleń innych autorów. Na tej podstawie dokonuje wnikliwej analizy takich niebezpieczeństw, jak: cyberprzestępczość, wirusy komputerowe, złośliwe programy, włamania do systemów informatycznych oraz ataki cyber-fizyczne (rozdział 2).

Równocześnie H. Wyrębek wyodrębnia kategorię zagrożeń społecznych o podłożu kulturowym, wynikających z konstruowania wirtualnej tożsamości czy interakcji w sieciach społecznościowych. Podkreśla znaczenie zagrożeń zdrowia fizycznego i psychicznego, zagrożeń dla moralności, zagrożeń społeczno-wychowawczych, a także zagrożeń związanych z różnymi postaciami uzależnień (infoholizm, uzależnienie od tradycyjnych i nowych substancji che-

¹⁴ Ibidem, s. 29-30.

¹⁵ C. Marcinkowski, *Cyberprzestrzeń a istota wybranych zagrożeń społecznych dla bezpieczeństwa współczesnego człowieka*, [w:] *Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*, red. D. Morańska, Dąbrowa Górnicza 2015, s. 114.

micznych z inspiracji sieci oraz uzależnienie od gier komputerowych – rozdział 3)¹⁶.

Wymienione przez autora zagrożenia z pewnością nie wyczerpują katalogu niebezpieczeństw wynikających z obecności w cyberświecie, niemniej w sposób jednoznaczny kierują uwagę także na społeczno-kulturowy wymiar zagrożeń. Charakter i znaczenie cyberprzestrzeni w kształtowaniu zachowań niepożądanych doskonale oddają m.in. słowa J. Bednarka, który pisze: „wraz z zastosowaniem coraz doskonalszych komputerów, wirtualne doświadczenia związane z prezentacją różnych zjawisk i procesów nabierają jeszcze większego realizmu. Jednocześnie (...) cyberprzestrzeń jest wykorzystywana do manipulacji człowiekiem. Jest ona źródłem różnorodnych patologii społecznych”¹⁷. W tym kontekście „jawi się pilna potrzeba rozwijania zdolności świadomego, dojrzałego, aktywnego i twórczego korzystania z zasobów i możliwości sieciowych, mieszczących się w granicach wartości i norm społecznych. Właściwe korzystanie z sieci powinno być więc poparte wiedzą i umiejętnościami rozpoznawania i odpowiedniego reagowania na problematyczne aspekty tego obszaru działalności człowieka”¹⁸.

Część pierwszą rozważań zamyka rozdział poświęcony zagadnieniu cyberterroryzmu. Autor przedstawia charakterystykę i specyfikę tego zjawiska, bazując na rozważaniach polskich i zagranicznych badaczy (rozdział 4). H. Wyrębek, uzasadniając konieczność bliższego przyjrzenia się temu zagrożeniu, wskazuje, iż stwarza ono większe niebezpieczeństwo niż znany od wieków zamach bombowy. Podkreśla przy tym, że „aktualnie można założyć, że w niedalekim czasie [cyberterroryzm] stanie się jednym z najważniejszych ogniw terroryzmu”¹⁹. O wadze podjętego przez autora problemu świadczy chociażby fakt, iż cyberterrorysty mogą doprowadzić do poważnych awarii lub paraliżu newralgicznych obiektów i struktur funkcjonowania państwa, składających się na infrastrukturę krytyczną, wzbudzając przy tym strach i poczucie niepewności wśród społeczeństwa.

¹⁶ Ibidem, s. 57 i nast.

¹⁷ A. Andrzejewska, J. Bednarek, *Cyberświat, możliwości i zagrożenia*, Warszawa 2009, s. 25.

¹⁸ D. Krzewniak, *Selected elements of the internet users' information security culture*, „Roczniki Nauk Społecznych” 2021, nr 2, s. 136.

¹⁹ H. Wyrębek, *Cyberprzestrzeń...*, s. 74.

Internet stał się medium, które jak żadne inne, całkowicie zrewolucjonizowało świat. Jest on interaktywnym, transgranicznym i transnarodowym forum wymiany myśli, poglądów i informacji. Jednak oprócz oczywistych korzyści, które ze sobą pociąga, cyberprzestrzeń stała się również obszarem wielu zagrożeń. Szybki rozwój techniki i komputerów ujawnił „potrzebę regulacji kwestii związanych z funkcjonowaniem cyberprzestrzeni. Nastęcza to wielu trudności, głównie z powodu jej transgraniczności i transnarodowości. Liczne podmioty na poziomie narodowym i międzynarodowym – publiczne i prywatne – podejmują się jednak tego niełatwego zadania. Drugą część monografii H. Wyrębek poświęcił właśnie problematyce prawnej ochrony cyberprzestrzeni. W kolejnych rozdziałach (5-7) opisuje i analizuje treść dokumentów prawnych Organizacji Narodów Zjednoczonych, Unii Europejskiej oraz Polski, pokazując zmiany w sposobie myślenia decydentów odnośnie do informacyjnego wymiaru bezpieczeństwa w sieci. Autor słusznie zauważa, że kwestia cyberbezpieczeństwa z każdym rokiem nabiera coraz większego znaczenia. W jego opinii, dostrzega się to zarówno na poziomie międzynarodowym, jak i krajowym²⁰.

W przedostatnim rozdziale (rozdział 8) autor dokonuje przeglądu strategicznych dokumentów dotyczących cyberbezpieczeństwa Polski i ich znaczenia dla bezpieczeństwa narodowego. Badacz ponownie podkreśla ewolucję i wzrost znaczenia cyberbezpieczeństwa jako transsektorowego wymiaru bezpieczeństwa, akcentując jednocześnie potencjał oraz kierunki działań państwa polskiego w tym zakresie. Dużym walorem recenzowanego wydawnictwa jest scharakteryzowanie krajowego systemu cyberbezpieczeństwa oraz prawnych uwarunkowań jego funkcjonowania (rozdział 9). Prezentowane treści ujęte są syntetycznie, ale rzeczowo i merytorycznie.

H. Wyrębek podjął niezwykle ważną problematykę z punktu widzenia teoretycznego i praktycznego. Na podkreślenie zasługuje aktualność omawianych kwestii dotyczących cyberbezpieczeństwa w złożonej i niezwykle dynamicznej rzeczywistości cechującej się z jednej strony niezwykleymi osiągnięciami w różnych sferach ludzkiego życia, z drugiej zaś – wieloma nowymi zagrożeniami i wyzwaniem w środowisku szeroko rozumianego bezpieczeństwa. W tym

²⁰ Ibidem, s. 118.

kontekście, podejmowanie badań naukowych we wskazanym obszarze wydaje się uzasadnione, a nawet konieczne, co dostrzega i wyraźnie podkreśla sam autor publikacji. Ogromnym walorem monografii jest także całościowe, problemowe ujęcie analizowanych treści. Autor w poszczególnych rozdziałach dowodzi, że jednym z najważniejszych wyzwań współczesnego człowieka i państwa w zakresie cyberbezpieczeństwa jest budowanie świadomości różnorodnych zagrożeń, które czyhają na nich w cyberświecie. Wydawnictwo charakteryzuje się zarówno pewnym uniwersalizmem, jak i konkretnymi ustaleniami odnoszącymi się do bezpieczeństwa i ochrony prawnej użytkowników cyberprzestrzeni.

W recenzowanej monografii poszerzono i pogłębiono eksploacyjnie zagadnienia wcześniej już analizowane przez innych autorów, najczęściej w odrębnych publikacjach z zakresu cyberprzestrzeni i bezpieczeństwa, wydobywając różnego rodzaju powiązania i interakcje pomiędzy nimi. Zakreślone przez autora horyzonty badawcze otwierają pole do kolejnych opracowań naukowych z zakresu cyberbezpieczeństwa. Interdyscyplinarny model analizy i opracowania poszczególnych zagadnień stanowi przykład rzetelnego postępowania metodologicznego. Trudne treści podawane są w sposób przystępny i z uwzględnieniem reguł obowiązujących w tekstach naukowych. Pewnym mankamentem pracy jest brak wniosków czy też podsumowań kolejnych rozdziałów i części, nie wpływa to jednak na ocenę merytoryczną książki jako całości.

Poszczególne rozdziały nie tylko dostarczają wiedzy na temat istoty cyberprzestrzeni i zagrożeń oraz ich dynamiki, lecz stanowią aktualny kontekst budowania świadomości i poczucia bezpieczeństwa różnych podmiotów, tworzenia nowoczesnych teorii i programów, modyfikacji uregulowań prawnych, mających zasadniczy wpływ na proces kształtowania postaw wobec cyberprzestrzeni. Konkludując, należy podkreślić, że jest to spójna i niezwykle potrzebna pozycja na polskim rynku wydawniczym. Ważkość podjętej tematyki sprawia, że publikacja ta stanowić może cenny materiał poznawczy – nie tylko dla studentów kierunków bezpieczeństwo narodowe i wewnętrzne, ale także dla teoretyków i praktyków problematyki szeroko rozumianego bezpieczeństwa.

Bibliografia / References

- Andrzejewska A., Bednarek J., *Cyberświat, możliwości i zagrożenia*, Warszawa 2009.
- Gibson W., *Neuromancer*, przekł. P.W. Cholewa, Poznań 2006.
- Golka M., *Bariery w komunikowaniu i społeczeństwo (dez)informacyjne*, Warszawa 2008.
- Grubicka J., Kamińska-Nawrot A., *Wstęp*, [w:] *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni*, red. J. Grubicka, A. Kamińska-Nawrot, Słupsk 2020.
- Koziński M., *Cyberprzestrzeń. Poszukiwanie bezpieczeństwa w obliczu współczesnych zagrożeń*, Słupsk 2015.
- Krzewniak D., *Selected elements of the internet users' information security culture*, „Roczniki Nauk Społecznych” 2021, nr 2.
- Levy P., *Drugi potop*, [w:] *Nowe media w komunikacji społecznej w XX wieku*, red. P. Hopfinger, Warszawa 2002.
- Marcinkowski C., *Cyberprzestrzeń a istota wybranych zagrożeń społecznych dla bezpieczeństwa współczesnego człowieka*, [w:] *Patologie w cyberprzestrzeni. Profilaktyka zagrożeń medialnych*, red. D. Morańska, Dąbrowa Górnicza 2015.
- Pilarski G., *Cyberprzestrzeń – relacje w wojnie hybrydowej*, Warszawa 2020.
- Taraszkiewicz B., *Znaczenie ekologii informacji w cyberprzestrzeni*, [w:] *Współczesny człowiek wobec zagrożeń w cyberprzestrzeni*, red. J. Grubicka, A. Kamińska-Nawrot, Słupsk 2020.
- Ustawa z 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej, Dz.U. 2002 nr 156, poz. 1301 z późn. zm.
- Wyřebek H., *Cyberprzestrzeń. Zagrożenia. Strategie cyberbezpieczeństwa*, Siedlce 2021.