Dominika Skoczylas

Rozwój teleinformatyczny państw Europy Wschodniej w kontekście cyberbezpieczeństwa. Zagrożenia a ochrona cyberprzestrzeni – wybrane zagadnienia

ICT Development in Eastern European Countries in the Context of Cybersecurity. Threats and Cyberspace Protection – Selected Issues

The author considers the use of electronic means of communication in Eastern European countries and an indication of the threats to cyberspace and the measures ensuring its protection. The author aims to determine how the use of ICT affects the socio-economic development of Eastern European countries. In connection with the above, based on examples of cyberspace security breaches, consideration should be given to the effectiveness of actions taken to protect or minimize the negative consequences of attacks. The author answers the question of how important the cybersecurity policy in the context of the socio-economic development of Eastern European countries is. The author uses a formal-legal and comparative research method, which makes confirming the research hypothesis that socio-economic development is closely related to information and communication technologies possible. The research carried out has a special dimension as part of the evaluation of ICT development in Eastern European countries. Research methods include the analysis of materials: selected cases, and basic legal acts with the use of the literature on the subject.

Dominika Skoczylas

doktor nauk prawnych
Uniwersytet Szczeciński

ORCID – 0000-0003-1231-8078

e-mail: dominika.skoczylas@usz.edu.pl

Słowa kluczowe:
cyberbezpieczeństwo, cyberprzestępczość, cyberterroryzm, informatyzacja, rozwój teleinformatyczny, technologie informacyjno-komunikacyjne

Key words:
cybersecurity, cybercrime, cyberterrorism, computerization, ICT development, information and communication technologies

https://doi.org/10.36128/priw.vi41.220

1. Wprowadzenie

Niewątpliwie, początek XXI wieku to okres ogromnych przemian w życiu społeczno-gospodarczym i politycznym, które można zauważyć w obszarze ekonomii, praw i wolności człowieka i obywatela, kultury czy nauki. W przypadku ostatniego z nich ogromną rolę odgrywają technologie informacyjno-komunikacyjne. Co więcej, skutecznie i efektywnie działający sektor teleinformatyczny stanowi wyznacznik innowacyjnego i nowoczesnego państwa, zaawansowanego technologicznie, posiadającego wysokie

wskaźniki ekonomiczne[1]. Biorąc pod uwagę to, że środki komunikacji elektronicznej znajdują zastosowanie w administracji (e-administracja) czy usługach (e-usługi), należy wykazać ich szczególne znaczenie w kwestii rozwoju społeczno-gospodarczego.

O ile pojęcie technologii informacyjnych i komunikacyjnych (*information and communication technologies* – ICT) obejmuje swoim zakresem techniki i technologie ICT, o tyle określenie: technologia informacyjna (*information technology* – IT), determinuje istotę działań obejmujących zarządzanie informacją, dokładniej e-informacją w e-zbiorach. Metody informatyczne i teleinformatyczne, odpowiedni system łączności i sprzęt komputerowy umożliwiają bowiem nieprzerwany, ogólnodostępny, łatwy i szybki dostęp do informacji czy realizacji e-usług[2]. Zresztą przetwarzanie informacji i świadczenie usług za pomocą środków komunikacji elektronicznej stanowią główną potrzebę społeczeństwa informacyjnego. Nie sposób nie zgodzić się z twierdzeniem, że: „Technologie informacyjno-komunikacyjne to środki, których ludzie używają do tworzenia, udostępniania i wykorzystywania informacji, (…) pozwalają nie tylko na konsumpcję informacji, ale też na ich produkcję, koprodukcję i rozpowszechnianie"[3].

Rozwój teleinformatyczny to rozwój zgodny z założeniami nowoczesnego modelu administracji i świadczenia usług na odległość, w skali globalnej. Państwo podobnie jak społeczeństwo informacyjne powinno efektywnie wykorzystywać narzędzia teleinformatyczne w urzędach, zakładach użyteczności publicznej, jednostkach rządowych i samorządowych, stale podnosić jakość świadczonych usług, dbać o rozwój teleinformatyczny, stosować elastyczne regulacje prawne, poszukiwać nowoczesnych rozwiązań technologicznych[4]. Wszystko po to, aby umożliwić ciągłą realizację e-usług o wysokim standardzie oraz stworzyć skuteczny system zabezpieczający przed cyberzagrożeniami.

Państwa Europy Wschodniej, podobnie jak państwa Europy Zachodniej, zauważyły w technologii informacyjno-komunikacyjnej możliwość rozwoju społeczno-gospodarczego. Środki komunikacji elektronicznej pozwalają na efektywniejsze administrowanie państwem, umożliwiają swobodny

1 Ursula Holtgrewe, „Invited Commentary New New Technologies: The Future and the Present of Work in Information and Communication Technology" *New Technology, Work and Employment*, nr 1 (2014): 9.

2 Grażyna Szpor, *Jawność i jej ograniczenia*, t. I, *Idee i pojęcia* (Warszawa: C. H. Beck, 2016), 118-119.

3 Christian Fuchs, „Information Technology and Sustainability in the Information Society" *International Journal of Communication*, nr 11 (2017): 2433.

4 Ewa Ziemba, „Discussion on a Sustainable Information Society" *Business Informatics*, nr 1 (2014): 18.

przepływ towarów i usług poza granice kraju. Perspektywy rozwoju państwa w kontekście rozwoju teleinformatycznego niestety są narażone na różnego rodzaju zagrożenia, do których należą cyberprzestępczość oraz cyberterroryzm. Polityka bezpieczeństwa cybernetycznego w kontekście rozwoju społeczno-gospodarczego państw Europy Wschodniej powinna być przemyślaną strategią państwa, zakładającą z góry potencjalne istnienie zagrożenia i środki, które mogą skutecznie chronić cyberprzestrzeń. Państwa Europy Wschodniej, zdominowane przez tradycyjny model administracji, nie są aż tak doświadczone w kwestii zarządzania bezpieczeństwem w cyberprzestrzeni. Podstawowe zasady, którymi muszą się kierować organy administracji publicznej, dotyczą określenia „(...) wymagań dotyczących identyfikacji i uwierzytelniania" przy zachowaniu „(...) ochrony swobodnego przepływu informacji (…)" oraz „(…) przejrzystości w programie cyberbezpieczeństwa (…) i wsparcia dla środków bezpieczeństwa cybernetycznego"[5].

Celem niniejszego artykułu jest ustalenie jak zastosowanie ICT wpływa na rozwój społeczno-gospodarczy państw Europy Wschodniej. Przedstawione zostaną również przykłady naruszeń bezpieczeństwa cyberprzestrzeni, które wystąpiły w krajach Europy Wschodniej, ich konsekwencje oraz działania zmierzające do ochrony czy minimalizacji negatywnych skutków ataków. Badania pozwolą na potwierdzenie hipotezy badawczej, która głosi, że rozwój społeczno-gospodarczy jest ściśle związany z technologiami informacyjno-komunikacyjnymi.

W pierwszej części pracy zostanie przedstawiony wpływ technologii informacyjno-komunikacyjnych na rozwój społeczno-gospodarczy państw Europy Wschodniej. Druga zaś obejmuje rozważania na temat polityki bezpieczeństwa cybernetycznego w kontekście rozwoju społeczno-gospodarczego państw Europy Wschodniej ze wskazaniem przykładów zagrożeń cyberprzestrzeni mających miejsce w XXI wieku. Przeprowadzone badanie pozwoli na ocenę rozwoju teleinformatycznego państw Europy Wschodniej i zasadność aktualnej polityki cyberbezpieczeństwa.

2. Wpływ technologii informacyjno-komunikacyjnych na rozwój społeczno-gospodarczy państw Europy Wschodniej

Wykorzystywanie nowoczesnych środków komunikacji elektronicznej przez administrację, ma ogromny wpływ na rozwój państw, nie tylko pod względem technologicznym, ale przede wszystkim społeczno-gospodarczym. Odejście od tradycyjnych metod administrowania, wymaga stworzenia i dostosowania infrastruktury teleinformatycznej, wdrożenia oprogramowań i systemów, a także zmian legislacyjnych. Unowocześnianie gospodarki, w szczególności w państwach Europy Wschodniej, w których całościowa

5 Gregory T. Nojeim, „Cybersecurity and Freedom on the Internet" *Journal of National Security Law & Policy*, nr 1 (2010): 120.

informatyzacja administracji i usług publicznych nie jest w pełni ukończonym procesem, jest kluczowym elementem osiągnięcia optymalnej pozycji na rynku międzynarodowym. Co do zasady znaczenie ICT należy rozpatrywać pozytywnie, uwzględniając chociażby ich wpływ na konsumpcję czy wskaźniki gospodarcze. Rozwój gospodarczy państwa, współcześnie łączony jest ze zinformatyzowaniem sektorów publicznych i inwestowaniem w infrastrukturę teleinformatyczną[6]. Główny kontekst, przejawia się w zwalczaniu ograniczeń pomiędzy użytkownikiem administracji publicznej a administracją (w skali mikro), natomiast szerzej (w skali makro) w budowaniu relacji na poziomie ponadnarodowym, w sferze e-komunikacji, e-zarządzania i e-planowania.

Szerokie wykorzystywanie ICT umożliwia zmianę w kierowaniu sektorem publicznym, sposobu zarządzania informacją i wdrażania coraz to nowocześniejszych rozwiązań technologicznych. Rosną również oczekiwania co do skutków społeczno-gospodarczych zastosowania nowego modelu e-zarządzania. Tak administracja publiczna jak i jej użytkownicy upatrują w e-informacji, e-usługach i e-handlu możliwość długotrwałego rozwoju państwa, w tym wzrostu gospodarczego, podniesienia jakości usług i przyśpieszenia realizacji zadań publicznych. Bardzo istotny jest kontekst informatyzacji na poziomach: informacyjnym (ciągły i bezpośredni dostęp do informacji), interakcyjny (zapewnienie stałego kanału e-komunikacji pomiędzy nadawcą a adresatem komunikatu, usługodawcą a usługobiorcą), oraz transakcyjnym (załatwienie sprawy, realizacja usługi)[7]. Nie bez znaczenia jest także aspekt ekonomiczny.

Uwzględniając znaczenie stosunków międzynarodowych, konkretnie w zakresie handlu i komunikacji, ICT wydaje się być podstawowym (choć nie jedynym) źródłem utrzymania relacji pomiędzy nawet najbardziej odległymi terytorialnie partnerami gospodarczymi. Niepodważalną rolę przypisuje się tzw. gospodarce opartej na wiedzy. Popularyzacja ICT w gospodarce i wśród społeczeństwa, wpisuje się w trend wzrostu kompetencji cyfrowych oraz zmian o charakterze technologicznym. Przyjęcie, że gospodarka XXI wieku jest oparta na wiedzy oznacza, że to właśnie informacja, umiejętności oraz kompetencje przesądzają o rozwoju społeczno-gospodarczym. Trafne jest stwierdzenie, że: „podstawę rozwoju gospodarki opartej na wiedzy upatruje się w rosnącym znaczeniu globalizacji oraz rozwoju technik informatycznych", a „wykorzystanie nowych technologii stwarza większe możliwości,

6 Raéf Bahrini, Alaa A. Qaffas, „Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries" *Economies*, nr 21 (2019): 2-3.

7 Grzegorz Sibiga, „Informatyzacja administracji publicznej w Polsce" *Edukacja Prawnicza*, nr 3 (2011): 3.

przynosi pozytywne efekty”[8]. Mając na uwadze wszechobecną informatyzację sektorów prywatnego i publicznego, warto odnieść się do wpływu technologii informacyjno-komunikacyjnych na rozwój społeczno-gospodarczy państw Europy Wschodniej (i Środkowo-Wschodniej). Zagadnienie jest o tyle interesujące, o ile w takich krajach jak Białoruś, Ukraina czy Rosja internet jako narzędzie wspierające rozwój społeczno-gospodarczy traktowany jest marginalnie kosztem tradycyjnego modelu zarządzania. Z kolei w państwach położonych w Europie Środkowo-Wschodniej, np. w Polsce, w Czechach czy na Słowacji, koncepcja cyfryzacji i informatyzacji usług jest zdecydowanie popularniejsza. Być może różnice wynikają z uwarunkowań kulturowych, historycznych, członkostwa w organizacjach międzynarodowych (NATO, Unii Europejskiej), relacji z państwami Europy Zachodniej i Stanami Zjednoczonymi. Językiem u wagi jest wpływ ICT na transformację gospodarki, w zakresie budowy tzw. globalnej gospodarki informacyjnej, której trzon stanowią innowacyjność, nowoczesna infrastruktura i technologie[9] oraz społeczeństwo informacyjne.

Technologie informacyjno-komunikacyjne umożliwiają zmianę dotychczasowych nawyków i sposobu zarządzania, głównie w sektorze usług publicznych i administracji. Ciekawe zjawisko gwałtownego wzrostu kompetencji cyfrowych wśród mieszkańców Europy Środkowo-Wschodniej zauważono podczas pandemii COVID-19. Głównymi wyznacznikami powstrzymania kryzysu gospodarczego i społecznego w trakcie pandemii były: dobrze rozwinięta infrastruktura i łączność, usieciowienie społeczeństwa i usług oraz umiejętności teleinformatyczne. Jak zauważono, państwa Europy Środkowo-Wschodniej zarówno pod kątem możliwości świadczenia e-usług jak i kwestii technologicznych były zdecydowanie słabiej przygotowane do obsługi teleinformatycznej niż leżące w Europie Zachodniej. Nie przeszkodziło to jednak takim krajom jak chociażby Rumunia uruchomić medycznej platformy mobilnej zapewniającej konsultacje online[10]. Jednak było to znacznie trudniejsze działanie niż w krajach, w których telemedycyna jest powszechnym zjawiskiem.

8 Dominik Rozkrut, Monika Rozkrut, „Umiejętności cyfrowe jako czynnik rozwoju gospodarki opartej na wiedzy” *Studia i prace wydziału nauk ekonomicznych i zarządzania*, nr 42 (2015): 78.

9 Maciej Smętkowski, Piotr Wójcik, *Regiony w Europie Środkowo-Wschodniej: tendencje i czynniki rozwojowe* (Warszawa: Centrum Europejskich Studiów Regionalnych i Lokalnych Uniwersytet Warszawski, 2008), 54.

10 Marlena Gołębiowska, „COVID-19 a cyfryzacja Europy Środkowej” *Komentarze Instytutu Europy Środkowej,* nr 162 (2020). https://ies.lublin.pl/pub/publikacje/komentarze/ies-komentarze-162-65-2020.pdf. [dostęp: 03.07.2020].

Do zalet zastosowania ICT należy wolność masowej komunikacji, a zatem ogólnodostępność rozwiązań teleinformatycznych. Innowacyjność i nowoczesne technologie stanowią odzwierciedlenie standardów gospodarki wolnorynkowej, uczciwej konkurencji i swobody gospodarczej. Zatem nie dziwi, że to w państwach demokratycznych internet i infrastruktura teleinformatyczna są postrzegane jako podstawowe warunki rozwoju społeczno-gospodarczego[11]. Widoczne jest to głównie w relacjach organ-obywatel (e-administracja, e-urząd) i sektorze e-usług publicznych. Państwa uznane za tzw. rozwinięte czy rozwijające się to głównie te posiadające ustrój demokratyczny, gdzie zdecydowanie łatwiej o wypracowanie standardów wolnościowych w e-handlu, e-usługach czy e-komunikacji. Co istotne, w przypadku samego już użytkowania sieci, to zagadnienie bezpieczeństwa i odporności systemów teleinformatycznych na ataki cybernetyczne. Zachodnie demokracje, mając na uwadze pozytywne aspekty cyfryzacji, dbają także o cyberbezpieczeństwo. Kraje Europy Wschodniej powinny wypracować długofalową strategię rozwoju społeczno-gospodarczego w kontekście polityki cyberbezpieczeństwa.

W analizach porównawczych rozwoju ICT w krajach Europy Środkowej i Wschodniej, można zauważyć, że co prawda popularyzacja środków komunikacji elektronicznej przyczyniła się w znaczącym stopniu do rozwoju społeczno-gospodarczego, ale niestety również unaoczniła problem nierówności technologicznych a wręcz wykluczenia cyfrowego poszczególnych krajów. Dla przykładu można podać Estonię, która posiada wysoki poziom rozwoju ICT, z drugiej strony zaś Rumunię czy Bułgarię, w których zjawisko wykluczenia cyfrowego jest najbardziej widoczne[12]. Wdrożenie zasad cyfryzacji i informatyzacji może stać się w państwach Europy Środkowo-Wschodniej, głównie tzw. byłego Bloku Wschodniego, szansą na wzrost gospodarczy i konkurencyjność przede wszystkim w ramach wymiany międzynarodowej. Wpływ technologii informacyjno-komunikacyjnych na rozwój społeczno-gospodarczy państw Europy Wschodniej, należy upatrywać z jednej strony w ramach wyrównania szans i wykluczenia nierówności cyfrowych tak administracji publicznej jak i społeczeństwa, z drugiej traktować jako stymulator procesów gospodarczych. Efektywna prowadzona polityka cyfryzacji i informatyzacji zapewnia konkurencyjność i swobodę świadczenia e-usług na skalę ponadnarodową. Ponadto, pozwala zacieśniać współpracę i wymianę handlową, budować relacje międzypaństwowe, daje możliwość kreowania popytu

11 Sergiu Gherghina, Joakim Ekman, Olena Podolian, „Democratic Innovations in Central and Eastern Europe: Expanding the Research Agenda" *Contemporary Politics*, nr 1 (2019): 12-13. https://eprints.gla.ac.uk/173343/7/173343.pdf. [dostęp: 07.07.2020].

12 Paweł Ziemba, Jarosław Becker, „Analysis of the Digital Divide Using Fuzzy Forecasting" *Symmetry*, nr 2 (2019): 22.

i podaży na rynku, wyznacza kierunek zmian gospodarczych. Tym samym urzeczywistnia zasady tzw. gospodarki opartej na wiedzy. Niezbędne dla rozwoju społeczno-gospodarczego, będzie w tym przypadku:

– budowa i utrzymanie odpowiedniej infrastruktury teleinformatycznej,
– wdrożenie nowoczesnych i innowacyjnych technologii, zapewnienie sprzętu i oprogramowania teleinformatycznego,
– rozwijanie umiejętności informatycznych wśród społeczeństwa i doskonalenie zawodowe specjalistów w dziedzinie teleinformatyki,
– wprowadzenie ogólnodostępnych środków komunikacji elektronicznej (szerokopasmowy internet),
– zwiększenie wydatków w celu obsługi teleinformatycznej, realizacji e-usług i e-administrowania,
– przygotowanie strategii bezpieczeństwa cyberprzestrzeni[13].

Rozwój teleinformatyczny podobnie jak rozwój społeczno-gospodarczy składa się z wielu etapów. Realizacja każdego z nich przybliża do osiągnięcia realnego sukcesu gospodarczego i zadowolenia społeczeństwa informacyjnego.

3. Polityka bezpieczeństwa cybernetycznego w kontekście rozwoju społeczno-gospodarczego państw Europy Wschodniej: zagrożenia a ochrona cyberprzestrzeni

Współcześnie rozwój społeczno-gospodarczy w dużej mierze zależy od wprowadzenia efektywnych i nowoczesnych rozwiązań teleinformatycznych oraz wdrożenia szczególnych zasad bezpieczeństwa sieciowego. Dzięki środkom komunikacji elektronicznej zdecydowanie łatwiejsze stało się m.in. załatwianie spraw urzędowych czy realizowanie usług publicznych. Co ważne, zmienił się również zasięg i kanał komunikacji. Z krajowego na międzynarodowy i z tradycyjnego na informatyczny (on-line). ICT stały się szansą na wzrost i rozwój gospodarczy, przy jednoczesnym zachowaniu i poszanowaniu zasady zrównoważonego rozwoju i swobody działalności gospodarczej. Obie z nich mają niemałe znaczenie szczególnie w kontekście rozwoju społeczno-gospodarczego państw Europy Wschodniej i Środkowo-Wschodniej, w których przez długi czas determinantą sukcesu gospodarczego był przeważnie krajowy potencjał gospodarczy, a rola środków komunikacji elektronicznej była praktycznie znikoma. Państwa Europy Wschodniej, które zamierzają rozwijać swój potencjał gospodarczy, powinny wziąć przykład z krajów Europy Zachodniej, w szczególności gdy mowa o bezpiecznej i długofalowej polityce w zakresie łączności, infrastruktury krytycznej (w tym teleinformatycznej)

13 Joanna Kos-Łabędowicz, „Wykorzystanie ICT w wybranych państwach zachodniej hemisfery" *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, nr 336 (2017): 123.

oraz wymiany handlowej. Unia Europejska, mając na uwadze zapewnienie trwałego wzrostu gospodarczego, dobrobytu społeczeństwa a jednocześnie utrzymania optymalnych warunków środowiskowych, dużo miejsca poświęca na określenia zasad w zakresie: nauki, technologii i innowacji[14] i ich wpływu na rozwój społeczno-gospodarczy. Odnosi się do nich bezpośrednio m.in. w Strategii na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu – Europa 2020[15], wskazując z jednej strony na – rozwój inteligentny, czyli rozwój gospodarki opartej na wiedzy i innowacji oraz rozwój zrównoważony, którego wyznacznikiem jest wspieranie gospodarki efektywniej korzystającej z zasobów, bardziej przyjaznej środowisku i bardziej konkurencyjnej.

Państwa Europy Wschodniej posiadają ogromny rynek zbytu surowców naturalnych, jednakże brak optymalnych rozwiązań zapewniających wymianę międzynarodową, może opóźnić a nawet uniemożliwić rozwój społeczno-gospodarczy. Nie dziwią zatem inwestycje w infrastrukturę teleinformatyczną czy przekształcenia modelu zarządzania informacją oraz popularyzowanie e-usług w byłych krajach Bloku Wschodniego. W zależności od możliwości finansowych a także uczestnictwa w organizacjach międzynarodowych zastosowanie ICT w poszczególnych państwach Europy Wschodniej wygląda często zupełnie inaczej. Dzieje się tak, ze względu na proces transformacji gospodarczo-ustrojowej. W zależności od produktywności, posiadanego kapitału, otoczenia instytucjonalnego, prowadzonej polityki rynkowej – wzrost innowacyjności występuje w mniej lub bardziej ograniczonym zakresie. W XXI wieku rozwój społeczno-gospodarczy nie jest możliwy bez rozwoju teleinformatycznego. Do organów władzy publicznej należy wdrożenie zasad gospodarki opartej na wiedzy oraz skorzystanie z innowacyjnych rozwiązań i technologii dających szanse na poprawę wydajności i efektywności gospodarczej oraz ekonomicznej. Wkład państwa w rozwój ICT umożliwi szybszy postęp teleinformatyczny[16].

14 Ewa Latoszek, „Agenda na Rzecz Zrównoważonego Rozwoju 2030 i jej wpływ na wybrane polityki Unii Europejskiej" *Studia Europejskie*, nr 3 (2017): 105-106.

15 Komunikat Komisji Europejskiej z 3 marca 2010 r., Europa 2020: Strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu [COM(2010) 2020 wersja ostateczna].

16 Aleksandra Skorupinska, Joan Torrent-Sellens, „The Role of ICT in the Productivity of Central and Eastern European Countries: Cross-Country Comparisons, Conference Paper 2013". Conference: XV Reunión de Economía Mundial, At Santander (Spain). https://www.researchgate.net/publication/268576747_The_role_of_ICT_in_the_productivity_of_Central_and_Eastern_European_countries_cross-country_comparison. [dostęp: 15.07.2020].

Powyższe wskazuje na to, że kluczowe zadanie spoczywa na organach władzy publicznej w zakresie określenia zasad polityki bezpieczeństwa cyberprzestrzeni. Jak owa polityka powinna wyglądać? Po pierwsze, fundamentalne jest określenie podstawowych wymagań w wymiarze gospodarczym, technologicznym i społecznym. Po drugie, państwa Europy Wschodniej, jako aspirujące do tzw. państw rozwiniętych, powinny przygotować odpowiednie rozwiązania prawne, sprzyjające innowacyjności i zastosowaniu technologii informacyjno-komunikacyjnych w sektorze publicznym i prywatnym, zainwestować w infrastrukturę teleinformatyczną oraz popularyzować zasady społeczeństwa informacyjnego, w tym edukację i umiejętności informatyczne. W wymiarze gospodarczym (ekonomicznym), należy podjąć działania umożliwiające efektywne funkcjonowanie e-gospodarki. Przede wszystkim istotna będzie relokacja kapitału poza granicami, która może wspomóc wymianę międzynarodową i transfer funduszy, w tym interakcję z partnerami biznesowymi i reprezentantami władzy publicznej innych państw tak w sektorze prywatnym, jak i publicznym[17]. Narzędzia ICT nie tylko mogą wspomóc sam przepływ środków, ponadnarodową wymianę towarów i świadczenia usług, m.in. w takich dziedzinach jak e-transport, e-finanse, e-bankowość, e-praca, e-zdrowie, ale również wpłynąć na postrzeganie (prestiż) państwa i uwiarygodnić jego pozycję w skali globalnej.

Inne ważne zagadnienie, które powinno zostać ujęte w polityce cyberbezpieczeństwa dotyczy wymiaru społecznego. Tutaj należy skoncentrować na jakości świadczonych usług i możliwości ich realizacji. Przeobrażenia strukturalne, wynikające z postępu technologicznego, wymagają wprowadzenia zmian także w edukacji, co do wiedzy i umiejętności informatycznych wśród społeczeństwa. Budowa społeczeństwa informacyjnego jest nieodłącznym elementem rozwoju teleinformatycznego, gospodarki opartej na wiedzy. Polityka cyberbezpieczeństwa państw Europy Wschodniej nie może pominąć takich zadań jak: zapewnienie powszechnego dostępu do informacji publicznej i e-administracji czy szerokopasmowego internetu[18].

Gospodarczy oraz społeczny wymiar polityki cyberbezpieczeństwa państw Europy Wschodniej integruje aspekt technologiczny oraz związane z nim bezpieczeństwo cyberprzestrzeni. Powszechne zastosowanie urządzeń komunikacji elektronicznej w administracji publicznej, umożliwia realizację zadań publicznych w przestrzeni wirtualnej. Całościowa informatyzacja przyczynia się do poprawy jakości usług świadczonych przez podmioty publiczne, zapewnia interoperacyjność działań oraz obsługę usług kluczowych.

17 Piotr Szkudlarek, Aleksandra Milczarek, „Rola społeczeństwa informacyjnego w kreowaniu zrównoważonego rozwoju" *Ekonomia i Środowisko*, nr 3 (2014): 237-238.

18 Hiranya K. Nath, „The Information Society" *Space and Culture, India*, nr 3 (2017): 20.

Istotą zmian organizacyjnych i strukturalnych jest ich konsolidacja z wymogami systemowymi, technologicznymi, informatycznymi. Tutaj bardzo ważna rola spoczywa na organach władzy publicznej, a jest nią wprowadzenie odpowiednich środków bezpieczeństwa, zabezpieczających w maksymalnym stopniu cyberprzestrzeń przed zagrożeniami[19]. Kraje Europy Wschodniej tworząc politykę cyberbezpieczeństwa, muszą zaplanować długofalową strategię działania, dzięki której będzie możliwa identyfikacja zagrożeń, uwierzytelnianie danych, stosowanie odpowiednich zapór sieciowych i szyfrowanie informacji, oraz utrzymanie ciągłości funkcjonowania infrastruktury krytycznej i świadczenia e-usług, pomimo wystąpienia zagrożenia. Opracowanie szczegółowych ram interoperacyjności systemów teleinformatycznych, tj. procedur mających na celu utrzymanie infrastruktury teleinformatycznej, należy uznać za pewien standard bezpieczeństwa sieciowego, podobnie jak samą obsługę incydentu[20]. Polityka cyberbezpieczeństwa powinna być dostosowana do rodzaju incydentów, ich ilości, skali zagrożeń oraz skutków. Zagrożeniem są nie tylko ataki hakerskie czy spamming, ale także działania zakwalifikowane jako cyberprzestępczość czy cyberterroryzm. Bardzo groźne są m.in. cyberataki na infrastrukturę krytyczną, oszustwa internetowe, dezorganizacja stron internetowych zarządzanych przez administrację, pobieranie i przetwarzanie danych szczególnie chronionych czy informacji niejawnych[21]. Dodatkowe utrudnienia powoduje co do zasady anonimowy i niespodziewany charakter cyberataków. Dlatego też szczególnie kraje Europy Wschodniej, w których proces informatyzacji jest na etapie początkowym, powinny wprowadzić skuteczne narzędzia monitoringu, analizy i nadzoru cyberzagrożeń. Niewykluczona jest w tym przypadku współpraca z państwami Europy Środkowo-Wschodniej i Europy Zachodniej.

W polityce cyberbezpieczeństwa państw Europy Wschodniej i Środkowo-Wschodniej nie może zabraknąć rozwiązań obejmujących działania związane z pojawieniem się ryzyka, tj. zagrożeń bezpieczeństwa cybernetycznego. W XXI wieku, przykładów naruszających cyberprzestrzeń państw

19 Dominika Skoczylas, „Postępowanie administracyjne a bezpieczeństwo systemów informatycznych e-administracji", [w:] *Fenomen prawa administracyjnego. Księga jubileuszowa Profesora Jana Zimmermanna,* red. Wojciech Jakimowicz, Mariusz Krawczyk, Iwona Niżnik-Dobosz (Warszawa: Wolters Kluwer, 2019), 773.

20 Dominika Skoczylas, „Znaczenie cyberbezpieczeństwa w administracji publicznej", [w:] *Wzorce i działania współczesnej administracji publicznej*, red. Barbara Jaworska-Dębska, Przemysław Kledzik i Janusz Sługocki (Warszawa: Wolters Kluwer, 2020), 952-953.

21 Adam M. Bossler, and Tamar Berenblum, „Introduction: New Directions in Cybercrime Research" *Journal of Crime and Justice*, nr 5 (2019): 496-497.

Europy Wschodniej i Środkowo-Wschodniej nie brakowało. Incydenty miały różne skutki (mniej lub bardziej dotkliwe), niemniej jednak ich pojawienie się spotkało się z natychmiastową reakcją organów. Wzorcowym jest przykład Blackout'u w zachodniej Ukrainie, który wystąpił 23 grudnia 2015 roku. Cyberatak spowodował odcięcie dostaw energii elektrycznej obiektów mieszkalnych w obwodzie iwano-frankowskim. Atak trwający od czterech do sześciu godzin, według władz Ukrainy był prawdopodobnie działaniem Rosji, a był o tyle groźny, o ile mógł wpłynąć na zmiany w zakresie sterowania infrastrukturą krytyczną i doprowadzić do zatrzymania ciągłości dostaw energii. W roku 2016 stwierdzono, że podobne ataki tzw. trojana „BlackEnergy" miały miejsce także w amerykańskim sektorze energetycznym w 2014 r. oraz we wrześniu 2014 r. w Polsce[22]. Ataki na ukraińską cyberprzestrzeń, stały się początkiem zmian legislacyjnych. Cyberbezpieczeństwo ma zapewnić m.in. ustawa z 5 października 2017 r. o podstawowych zasadach zapewnienia bezpieczeństwa cybernetycznego Ukrainy, ustawa z dnia 21 czerwca 2018 r. o bezpieczeństwie narodowym Ukrainy. Przepisy wprowadzone na Ukrainie wskazują „podmioty, środki prawne i zasoby organizacyjne wyznaczone do ochrony cyberprzestrzeni" oraz „przyznają szczególną i silną pozycję Prezydentowi Ukrainy jako organowi odpowiedzialnemu za koordynację polityki zapewnienia cyberbezpieczeństwa w Ukrainie"[23].

Z rankingu Global Cybersecurity Exposure Index 2020 wynika, że w Europie najbardziej narażone na ataki cyberprzestępców są: Armenia, Białoruś, Bośnia i Hercegowina, Ukraina i Albania. Z kolei najmniejszy stopień zagrożenia cybernetycznego wskazano dla Finlandii, Danii, Luksemburga, Estonii i Norwegii. Z powyższego raportu wynika, że kraje Europy Wschodniej i Południowo-Wschodniej, które zdecydowanie później rozpoczęły (i jeszcze nie zakończyły) proces informatyzacji powinny podjąć natychmiastowe działania w kwestii poprawy polityki cyberbezpieczeństwa[24]. Niemniej jednak ważne są postanowienia zawarte w Strategii Cyberbezpieczeństwa wprowadzane na wzór strategii państw zachodnich.

---

22 Kamil Gapiński, „Blackout w zachodniej Ukrainie – cyberatak o wymiarze międzynarodowym". https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/. [dostęp: 15.07.2020].

23 Marcin Gołębiowski, „Rola i kompetencje prezydenta Ukrainy w zakresie kształtowania reżimu prawnego ochrony cyberprzestrzeni. Analiza teoretycznoprawna regulacji prawnych z zakresu cyberbezpieczeństwa Ukrainy" *Teka of Political Science and International Relations – OL PAN/UMCS*, nr 2 (2018): 136-137, 139-140.

24 Cybersecurity Exposure Index (CEI) 2020. https://passwordmanagers.co/cybersecurity-exposure-index/#europe. [dostęp: 15.07.2020].

Państwa Europy Wschodniej: Białoruś, Ukraina czy Rosja mogłyby skorzystać z doświadczeń Grupy Wyszehradzkiej (tzw. V4), do której należą Polska, Czechy, Słowacja i Węgry. Każde z ww. państw priorytetowo traktuje kwestie bezpieczeństwa publicznego, szczególnie gdy mowa o bezpieczeństwie cyberprzestrzeni. Na poziomie regionalnym szczególną uwagę przywiązują do współpracy cybernetycznej i rozwoju ICT[25]. Jednym z kluczowych było stanowisko Grupy V4 w kwestii zwalczania zagrożeń cybernetycznych: „bezpieczeństwo cybernetyczne staje się obecnie kwestią kluczową, państwa Grupy Wyszehradzkiej zamierzają zacieśnić współpracę w zakresie zwalczania zagrożeń cybernetycznych na poziomie politycznym i operacyjnym"[26]. Aktualne cele Grupy V4 wydają się potwierdzać i rozszerzać te ustalone na przełomie 2012/2013 roku i dotyczą m.in. współpracy w obszarze agendy cyfrowej, w tym cyfryzacji, sztucznej inteligencji, e-handlu, cyberbezpieczeństwa, wzmocnienia i rozbudowania współpracy V4 w obszarze innowacyjności i stosowania nowych technologii oraz w obszarze technologii w administracji (GovTech)[27]. Kraje Europy Wschodniej, konstruując zasady polityki cyberbezpieczeństwa, mogą wziąć pod uwagę również kwestie współpracy międzynarodowej, chociażby w celu wymiany doświadczeń w zakresie ochrony przed cyberatakami.

Polityka cyberbezpieczeństwa powinna uwzględniać jeszcze jeden bardzo ważny aspekt, szczególnie w tych państwach, których idea centralnego władztwa administracyjnego jest mocno zakorzeniona – ochronę interesu publicznego, przy jednoczesnym zachowaniu ochrony praw człowieka i obywatela. Efektywność i skuteczność działań gwarantujących cyberbezpieczeństwo nie może bowiem bezpodstawnie naruszać dobra jednostki czy społeczeństwa[28]. Warto przeanalizować znaczenie środków komunikacji elektronicznej w kontekście rozwoju społeczno-gospodarczego oraz dobrobytu państwa. Perspektywa ekonomiczna i globalizacja kapitału, wskazuje na to, że także państwa Europy Wschodniej, powinny wdrożyć takie krajowe strategie bezpieczeństwa cybernetycznego, gdzie:

25 Tomasz Klepner, „Współpraca transgraniczna państw Grupy Wyszehradzkiej na rzecz zapewnienia bezpieczeństwa granic" *Poliarchia*, nr 2 (2014): 113.

26 Raport Polskiego Przewodnictwa w Grupie Wyszehradzkiej. Lipiec 2012 – Czerwiec 2013, Warszawa 2013. https://www.visegradgroup.eu › report-pl-v4-pres-07. [dostęp: 15.07.2020].

27 Polska prezydencja w Grupie Wyszehradzkiej, Cele V4. https://www.gov.pl/web/V4prezydencja. [dostęp: 15.07.2020].

28 Kamil Stępniak, „Walka z terroryzmem i cyberterroryzmem a ochrona konstytucyjnych praw i wolności jednostki", [w:] *Internet. Strategie bezpieczeństwa*, red. Grażyna Szpor, Agnieszka Gryszczyńska (Warszawa: C. H. Beck, 2017), 127.

– organy władzy publicznej stworzą odpowiednie regulacje prawne w zakresie cyberprzestrzeni, w tym krajową politykę cyberbezpieczeństwa,
– dostawcy e-usług i administratorzy e-danych będą odpowiedzialni za ochronę cyberprzestrzeni, a w razie zaistnienia zagrożenia za obsługę incydentów,
– obowiązek informacji o zagrożeniach spoczywał będzie na wszystkich użytkownikach sieci internet[29].

Uwarunkowania rozwoju teleinformatycznego państw Europy Wschodniej można upatrywać także w ramach Partnerstwa Wschodniego, czyli współdziałania Unii Europejskiej z państwami byłego ZSRR (Mołdawia, Białoruś, Ukraina, Armenia, Azerbejdżan i Gruzja). Wspólny rynek towarów i usług, swobodna wymiana handlowa, budowanie wzajemnych relacji gospodarczych, społecznych i politycznych dają możliwość stworzenia solidnej polityki cyberbezpieczeństwa, dzięki której będzie można zaktywizować współpracę w obszarze e-wymiany, e-transportu, e-komunikacji, czy e-usług[30]. Jest to szansa i wzywanie dla państw Europy Wschodniej na równoczesny rozwój teleinformatyczny i społeczno-gospodarczy.

4. Konkluzje

Reasumując, państwa Europy Wschodniej powinny dokonać wnikliwej analizy sytuacji społeczno-gospodarczej. Uwagi wymaga sposób zarządzania administracją publiczną oraz świadczenia usług kluczowych. Obecnie, w związku z informatyzacją zadań publicznych oraz potrzebami społeczeństwa informacyjnego, państwa Europy Wschodniej są nijako zobowiązane podjąć działania zmierzające do pełnego usieciowienia usług tak publicznych, jak i prywatnych. Korzystając z doświadczenia państw Europy Zachodniej oraz Środkowo-Wschodniej maksymalna informatyzacja takich sektorów jak: handel zagraniczny, transport, komunikacja, usługi czy finanse jest podstawowym czynnikiem rozwoju społeczno-gospodarczego. Budowanie wzajemnych relacji gospodarczych i politycznych o ponadnarodowym zasięgu daje możliwość interakcji z partnerami biznesowymi i reprezentantami władzy publicznej innych państw, a tym samym może wspomóc przepływ środków pieniężnych i wpłynąć na dobrobyt całego kraju.

Należy potwierdzić, że współcześnie rozwój społeczno-gospodarczy jest ściśle związany z technologiami informacyjno-komunikacyjnymi.

29 Agnija Tumkevič, „Cybersecurity in Central Eastern Europe: From Identifying Risks to Countering Threats" *Baltic Journal of Political Science*, nr 5 (2016): 74.

30 Beata Piskorska, „Partnerstwo Wschodnie po 10 latach: sukces czy porażka, realizm czy iluzja?" *Rocznik Instytutu Europy Środkowo-Wschodniej*, nr 17, z. 2 (2019): 12.

Wpływ ICT na rozwój społeczno-gospodarczy państw Europy Wschodniej zależy w dużej mierze od działań podejmowanych przez organy władzy publicznej, które powinny dążyć do stworzenia tzw. gospodarki opartej na wiedzy. Filarem takiego stanu rzeczy jest skuteczne i efektywne funkcjonowanie gospodarki wolnorynkowej, swobodna wymiana towarów, informacji, kapitału i świadczenie usług przy zastosowaniu środków komunikacji elektronicznej. Zapewnienie podstawowych wymagań w wymiarze gospodarczym, technologicznym i społecznym, niezbędnych dla wdrożenia ICT i późniejszego rozwoju teleinformatycznego to zabieg pożądany i konieczny.

W przypadku byłych państw Bloku Wschodniego, których umiejętności technologiczne nie są na tak zaawansowanym poziomie jak w państwach Europy Zachodniej, wymagane jest określenie zasad polityki bezpieczeństwa cyberprzestrzeni. Rozwiązania prawne muszą uwzględniać możliwości państwa w zakresie zastosowania ICT w sektorze publicznym i prywatnym, innowacyjność, inwestycje w infrastrukturę krytyczną, zasady społeczeństwa informacyjnego. Efektywność i skuteczność rozwoju społeczno-gospodarczego w kontekście rozwoju teleinformatycznego należy ocenić pod kątem bezpieczeństwa cybernetycznego. Wprowadzenie krajowych strategii bezpieczeństwa cybernetycznego jest warunkiem *sine qua non* długofalowej polityki informatyzacji państwa. Godny przypomnienia jest kazus Ukrainy, która w ostatnich latach, próbuje z jednej strony przeciwstawić się różnego typu cyberatakom, z drugiej proponuje rozwiązania prawne, mające na celu bezpieczeństwo realizacji e-usług kluczowych dla państwa i społeczeństwa oraz ochronę infrastruktury krytycznej.

Informatyzacja usług publicznych i administracji publicznej ułatwia i usprawnia realizację zadań i świadczenie usług publicznych w skali globalnej. Pełne usieciowienie kraju wynikające z postmodernizacyjnych tendencji odzwierciedla poziom rozwoju społeczno-gospodarczego nie tylko w znaczeniu dostępności do infrastruktury teleinformatycznej czy alokacji kapitału, ale także w zakresie wiedzy i umiejętności społeczeństwa informacyjnego[31]. Państwa Europy Wschodniej powinny budować swoją „informatyczną" pozycję na rynku w oderwaniu od idei centralnego władztwa administracyjnego, tzn. w odniesieniu do ochrony interesu publicznego, przy jednoczesnej ochronie praw człowieka i obywatela. Polityka bezpieczeństwa cybernetycznego w kontekście rozwoju społeczno-gospodarczego państw Europy Wschodniej musi być optymalnym narzędziem, zapewniającym tak bezpieczeństwo cyberprzestrzeni, jak i rozwój teleinformatyczny państwa.

31 Karolina Jastrzębska, *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych* (Warszawa: CeDeWu Sp. z o.o., 2018), 61.

Bibliografia

Bahrini Raéf, Qaffas Alaa A., „Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries" *Economies*, nr 21 (2019): 1-13. https://doi.org/10.3390/economies7010021.

Bossler Adam M., Berenblum Tamar, „Introduction: new directions in cybercrime research" *Journal of Crime and Justice*, nr 5 (2019): 495-499. https://doi.org/10.1080/0735648X.2019.1692426.

Cybersecurity Exposure Index (CEI) 2020. https://passwordmanagers.co/cybersecurity-exposure-index/#europe.

Fuchs Christian, „Information Technology and Sustainability in the Information Society" *International Journal of Communication*, nr 11 (2017): 2431-2461.

Gapiński Kamil, „Blackout w zachodniej Ukrainie – cyberatak o wymiarze międzynarodowym". https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/.

Gherghina Sergiu, Joakim Ekman, Olena Podolian, „Democratic Innovations in Central and Eastern Europe: expanding the Research Agenda" *Contemporary Politics,* nr 25 (2019): 1-19. https://eprints.gla.ac.uk/173343/7/173343.pdf. https://doi.org/10.1080/13569775.2018.1543752. [dostęp: 07.07.2020].

Gołębiowska Marlena, „COVID-19 a cyfryzacja Europy Środkowej" *Komentarze Instytutu Europy Środkowej*, nr 162 (2020). https://ies.lublin.pl/pub/publikacje/komentarze/ies-komentarze-162-65-2020.pdf. [dostęp: 03.07.2020].

Gołębiowski Marcin, „Rola i kompetencje prezydenta Ukrainy w zakresie kształtowania reżimu prawnego ochrony cyberprzestrzeni. Analiza teoretycznoprawna regulacji prawnych z zakresu cyberbezpieczeństwa Ukrainy" *Teka of Political Science and International Relations – OL PAN/UMCS*, nr 2 (2018): 129-141. http://dx.doi.org/10.17951/teka.2018.13.2.129-141.

Holtgrewe Ursula, „Invited Commentary New Technologies: The Future and the Present of Work in Information and Communication Technology" *New Technology, Work and Employment*, nr 1 (2014): 9-24. https://doi.org/10.1111/ntwe.12025.

Jastrzębska Karolina, *Elektroniczna administracja jako narzędzie wdrażania zmian organizacyjnych.* Warszawa: CeDeWu Sp. z o.o., 2018.

Klepner Tomasz, „Współpraca transgraniczna państw Grupy Wyszehradzkiej na rzecz zapewnienia bezpieczeństwa granic" *Poliarchia*, nr 2 (2014): 99-122. https://doi.org/10.12797/Poliarchia.02.2014.03.06.

Kos-Łabędowicz Joanna, „Wykorzystanie ICT w wybranych państwach zachodniej hemisfery" *Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach*, nr 336 (2017): 118-133.

Latoszek Ewa, „Agenda na Rzecz Zrównoważonego Rozwoju 2030 i jej wpływ na wybrane polityki Unii Europejskiej" *Studia Europejskie*, nr 3 (2017): 97-116.

Nath Hiranya K., „The Information Society" *Space and Culture, India*, nr 3 (2017): 19-28. http://dx.doi.org/10.20896/saci.v4i3.248.

Nojeim Gregory T., „Cybersecurity and Freedom on the Internet" *Journal of National Security Law & Policy*, nr 1 (2010): 119-137.

Piskorska Beata, „Partnerstwo Wschodnie po 10 latach: sukces czy porażka, realizm czy iluzja?" *Rocznik Instytutu Europy Środkowo-Wschodniej,* nr 17, z. 2 (2019): 9-39. https://doi.org/10.36874/ RIESW.2019.2.1.

Polska prezydencja w Grupie Wyszehradzkiej, Cele V4. https://www.gov.pl/web/V4prezydencja.

Raport Polskiego Przewodnictwa w Grupie Wyszehradzkiej. Lipiec 2012 – Czerwiec 2013, Warszawa 2013. *https://www.visegradgroup.eu › report--pl-v4-pres-07.*

Rozkrut Dominik, Monika Rozkrut, „Umiejętności cyfrowe jako czynnik rozwoju gospodarki opartej na wiedzy" *Studia i prace wydziału nauk ekonomicznych i zarządzania*, nr 42 (2015): 75-88. https://doi.org/10.18276/sip.2015.42/1-05.

Sibiga Grzegorz, „Informatyzacja administracji publicznej w Polsce" *Edukacja Prawnicza*, nr 3 (2011): 3-7.

Skoczylas Dominika, „Postępowanie administracyjne a bezpieczeństwo systemów informatycznych e-administracji", [w:] *Fenomen prawa administracyjnego. Księga jubileuszowa Profesora Jana Zimmermanna,* red. Wojciech Jakimowicz, Mariusz Krawczyk, Iwona Niżnik-Dobosz. 772-784. Warszawa: Wolters Kluwer, 2019.

Skoczylas Dominika, „Znaczenie cyberbezpieczeństwa w administracji publicznej", [w:] *Wzorce i działania współczesnej administracji publicznej*, red. Barbara Jaworska-Dębska, Przemysław Kledzik, Janusz Sługocki. 942-955. Warszawa: Wolters Kluwer, 2020.

Skorupinska Aleksandra, Joan Torrent-Sellens, „The Role of ICT in the Productivity of Central and Eastern European countries: Cross-Country Comparisons, Conference Paper 2013". Conference: XV Reunión de Economía Mundial, At Santander (Spain). https://www.researchgate.net/publication/268576747_The_role_of_ICT_in_the_productivity_of_Central_and_Eastern_European_countries_cross-country_comparison.

Smętkowski Maciej, Piotr Wójcik, *Regiony w Europie Środkowo-Wschodniej: tendencje i czynniki rozwojowe.* Warszawa: Centrum Europejskich Studiów Regionalnych i Lokalnych Uniwersytet Warszawski, 2008.

Stępniak Kamil, „Walka z terroryzmem i cyberterroryzmem a ochrona konstytucyjnych praw i wolności jednostki", [w:] *Internet. Strategie*

bezpieczeństwa, red. Grażyna Szpor, Agnieszka Gryszczyńska. 119-127. Warszawa: C. H. Beck, 2017.

Szkudlarek Piotr, Aleksandra Milczarek, „Rola społeczeństwa informacyjnego w kreowaniu zrównoważonego rozwoju" *Ekonomia i Środowisko*, nr 3 (2014): 231-242.

Szpor Grażyna, *Jawność i jej ograniczenia*, t. I, *Idee i pojęcia*. Warszawa: C. H. Beck, 2016.

Tumkevič Agnija, „Cybersecurity in Central Eastern Europe: From Identifying Risks to Countering Threats" *Baltic Journal of Political Science*, nr 5 (2016): 73-88. https://doi.org/10.15388/bjps.2016.5.10337.

Ziemba Ewa, „Discussion on a Sustainable Information Society" *Business Informatics*, nr 1 (2014): 13-25. https://doi.org/10.15611/ie.2014.1.01.

Ziemba Paweł, Jarosław Becker, „Analysis of the Digital Divide Using Fuzzy Forecasting" *Symmetry*, nr 2 (2019): 1-34. https://doi.org/10.3390/sym11020166.