Ius et Securitas 1/2024 | ISSN 3071-799X

Tomasz Wojciechowski
Wydział Humanistyczny
Politechnika Koszalińska
ORCID: 0000-0002-0675-4474
t_wojciechowski1@poczta.onet.pl

Cyberbezpieczeństwo i dezinformacja we współczesnym świecie: strategie ochrony i zarządzania kryzysowego

Streszczenie

Współczesne zagrożenie w cyberprzestrzeni skupia się na wzroście cyberataków na infrastrukturę krytyczną i ich konsekwencjach społecznych, wskazując na potrzebę skutecznych strategii ochrony i zarządzania kryzysowego. Autor w niniejszym tekście podkreśla znaczenie edukacji cyfrowej i świadomości społecznej w przeciwdziałaniu dezinformacji oraz w minimalizowaniu ryzyka wystąpienia sytuacji kryzysowych, także w kontekście współczesnych konfliktów politycznych i wojskowych. Podjęto próbę określenia czynników związanych z cyberbezpieczeństwem, dezinformacją i ochroną infrastruktury krytycznej. Podane zostały również przykłady strategii walki z rosnącym poziomem cyberzagrożeń, podkreślając konieczność dostosowania podejść obronnych do dynamicznie zmieniającego się środowiska zagrożeń. Celem niniejszego artykułu jest analiza podatności społeczeństw na zagrożenia wynikające z cyfryzacji w kontekście wystąpienia sytuacji kryzysowej. Szczególna uwaga jest poświęcona dezinformacji w kontekście poziomu kompetencji informacyjnych i cyfrowych społeczeństw oraz możliwości zaistnienia sytuacji kryzysowej będącej skutkiem bezkrytycznego podejścia do treści cyfrowych i rozwiązań proponowanych przez algorytmy. Zastosowane metody badawcze to analiza treści oraz studia przypadków (z ang. case studies) uzupełnione metodami: porównawczą oraz systemową i jakościową.

Słowa kluczowe: cyberbezpieczeństwo, dezinformacja, infrastruktura krytyczna, zarządzanie kryzysowe, edukacja cyfrowa.

Wprowadzenie

Obecny postęp technologiczny wpływa na wiele różnych aspektów życia społecznego i działania państw, odgrywając istotną rolę w niemal każdej sferze ich funkcjonowania[1]. W kontekście tej ewolucji technologicznej, szczególnie znaczącą rolę odgrywa cyfryzacja, która umożliwia transformację tradycyjnych metod pracy, komunikacji oraz dostępu do informacji. Proces ten, charakteryzujący się przenoszeniem danych i usług do przestrzeni wirtualnej, stał się fundamentem nowoczesnych społeczeństw. Cyfryzacja, poprzez implementację zaawansowanych technologii takich jak sztuczna inteligencja, big data czy Internet rzeczy (ang. Internet of Things, IoT), przyczynia się do automatyzacji i optymalizacji procesów w różnych sektorach – od przemysłu po usługi publiczne. Takie zmiany mają bezpośredni wpływ na codzienne życie obywateli oraz na efektywność funkcjonowania państw. Ponadto rozwój technologii komunikacyjnych, w tym szerokopasmowego dostępu do Internetu, umożliwia eliminację barier geograficznych i społecznych, umożliwiając większą integrację na poziomie globalnym.

Obecnie Internet stał się kluczowym narzędziem, niezbędnym do codziennego działania nowoczesnych społeczeństw i państw. Służy jako ogromne źródło wiedzy, oferując dostęp do niemal wszystkich informacji ludzkości, i jest często uważany za wszechstronną bazę danych, zawierającą informacje na każdy możliwy temat[2]. Warto zaznaczyć jednak, że posługując się tym narzędziem należy uważać na prawdziwość podawanych informacji, ich wiarygodność i potwierdzenia w źródłach.

W kontekście ewolucji cyfrowej Internet przekształcił się w platformę, która nie tylko dostarcza informacji, ale także kształtuje sposób, w jaki społeczeństwa je przyswajają i wykorzystują. W tej nowej rzeczywistości, algorytmy personalizacji i filtracja treści stają się coraz bardziej powszechne, co z jednej strony pozwala na dostosowanie przepływu informacji do indywidualnych potrzeb i preferencji użytkowników, ale z drugiej strony rodzi obawy dotyczące tworzenia tzw. baniek informacyjnych, prowadzących do izolacji społecznej i ograniczenia ekspozycji na różnorodne punkty widzenia, co ma

[1] K. Kaczmarek, *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, nr 1, s. 144.

[2] K. Kaczmarek, *Darknet jako przedmiot badań nauk społecznych*, „Cybersecurity and Law" 2024, nr 2, s. 106.

kluczowe znaczenie dla demokratycznych społeczeństw. W konsekwencji, choć Internet służy jako narzędzie do dystrybucji i wymiany wiedzy, jego rola w kształtowaniu opinii publicznej i wpływanie na decyzje polityczne staje się coraz bardziej złożona i wielowymiarowa. W tym kontekście, potrzeba zrozumienia i zarządzania tymi procesami staje się kluczową kwestią zarówno dla jednostek, organizacji społecznych i samych społeczeństw jak i państw. Stworzenie wirtualnego środowiska, które umożliwia gromadzenie wiedzy o osobistych upodobaniach jednostek, znacząco osłabiło autorytet polityczny państw. To jednak nie przekłada się na wzrost zaufania do przedstawicieli sfery publicznej czy efektywną realizację międzynarodowych interesów publicznych. Zamiast tego wykształciły się mechanizmy kontrolowania opinii publicznej, która tego nie zauważa, ponieważ w zamian otrzymuje narzędzia, które udoskonalają kulturę codziennych interakcji, szczególnie w sytuacjach kryzysowych[3]. Należy również podkreślić, że uzależnienie społeczeństw od powszechnego dostępu do informacji i usług sieciowych niesie za sobą również szereg zagrożeń takich jak dezinformacja czy brak dostępu do większości usług w przypadku awarii infrastruktury telekomunikacyjnej.

Bezpieczeństwo cyfrowe: implikacje dla administracji publicznej w epoce ICT

W ostatnim czasie technologie informacyjno-komunikacyjne (ang. information and communication technologies – ICT) zyskały na znaczeniu, a procesy cyfryzacji i digitalizacja przyczyniły się do rozwoju i zmian w sektorze publicznym[4]. W związku z postępującymi zmianami technologicznymi oraz powszechną cyfryzacją życia publicznego i prywatnego, wszystkie państwa muszą chronić swoich obywateli i instytucje przed cyberzagrożeniami, które mogą mieć daleko idące konsekwencje, w tym wprost przyczyniać się mogą do destabilizacji gospodarki czy wadliwego funkcjonowania władzy publicznej[5].

W obliczu tych procesów zaobserwować można znaczącą transformację w sposobie, w jaki sektor publiczny funkcjonuje i świadczy usługi ICT.

[3] S. Mishra, *Digital cultures,* Londyn 2021, s. 121-124.

[4] K. Kaczmarek, *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją,* „Cybersecurity and Law" 2021, s. 67.

[5] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, Maribor 2023, s. 1.

Wprowadzenie technologii ICT w administracji publicznej i usługach obywatelskich nie tylko zwiększyło efektywność i dostępność tych usług, ale również wprowadziło nowe wyzwania w zakresie bezpieczeństwa danych i prywatności. Wzrost zależności od systemów cyfrowych sprawia, że rządy i instytucje publiczne stają się bardziej podatne na ataki cybernetyczne, które mogą zakłócać kluczowe funkcje państwa, także systemy obronne oraz narażać bezpieczeństwo danych osobowych obywateli. Dodatkowo, przenoszenie coraz większej ilości danych do przestrzeni cyfrowej również w postaci magazynowania plików w tzw. chmurach (ang. clouds) wymaga rozwijania nowych strategii zarządzania i ochrony informacji, co staje się kluczowym elementem w utrzymaniu zaufania publicznego oraz integralności struktur państwowych. W tym kontekście, zarówno rozwój infrastruktury cyfrowej, jak i wdrażanie skutecznych polityk bezpieczeństwa stają się nieodzownymi elementami strategii rozwoju każdego państwa. Budowanie społeczeństwa cyfrowego to nie jedynie tworzenie infrastruktury i możliwość dostępu do sieci, ale przede wszystkim dostępność usług społecznych online[6].

Dodatkowo, rosnąca penetracja Internetu oraz jego udział w codziennym życiu obywateli napędza dalsze, permanentne wdrażanie technologii ICT w administracji publicznej. Ten trend wiąże się z rosnącym oczekiwaniem na cyfrową dostępność usług publicznych oraz na transparentność i efektywność działania instytucji państwowych. Zwiększenie udziału narzędzi cyfrowych w sektorze publicznym przyczynia się do szybszego przetwarzania danych, usprawnia komunikację między obywatelami a urzędami oraz pozwala na bardziej elastyczne zarządzanie zasobami publicznymi. W tym kontekście, inicjatywy takie jak e-administracja czy e-usługi stają się nie tylko narzędziem optymalizacji procesów administracyjnych, ale również środkiem do zacieśniania relacji między państwem a jego obywatelami. Jednakże, rozwój tych cyfrowych rozwiązań wymaga równoczesnego wzmocnienia mechanizmów ochrony danych i systemów bezpieczeństwa, aby zapewnić ochronę przed potencjalnymi zagrożeniami cyfrowymi.

Zwiększający się udział Internetu wpływa na rosnące wykorzystanie ICT zarówno w administracji publicznej jak i przez podmioty publiczne[7]. Należy

[6] K. Kaczmarek, *Transformacja Estonii po rozpadzie Związku Radzieckiego. Determinanty historyczne i analiza porównawcza skutków,* „Acta Politica Polonica" 2022, nr 2, s. 13.

[7] E.M. Włodyka, *Dostępność cyfrowa w Unii Europejskiej – praktyka i założenia teoretyczne*, „Rocznik Integracji Europejskiej" 2022, nr 16, s. 356.

przy tym zauważyć, iż większość skutecznych cyberataków to wynik błędu użytkownika, a nie systemu[8]. Często są one skutkiem nie tyle nieznajomości zasad i procedur, ale ich lekceważenia. Taki stan rzeczy wskazuje na konieczność położenia większego nacisku na praktyczną edukację cyfrową na każdym poziomie edukacji, poczynając od szkolnictwa podstawowego.

Dezinformacja a sytuacje kryzysowe

Rozwój nowoczesnych technologii i ciągle zwiększające się moce obliczeniowe sztucznej inteligencji pozwalają na połączenie wiedzy z zakresu socjologii, psychologii, neurobiologii, matematyki czy kulturoznawstwa. Takie wielowymiarowe analizy i ich wyniki pozwalają wpływać na zachowania jednostek i społeczeństw na niespotykaną wcześniej skalę[9]. Jednym ze sposobów wywierania takiego wpływu jest dezinformacja. Jednocześnie jest ona jednym z największych cyfrowych zagrożeń na jakie narażone są społeczeństwa, ponieważ dezinformacja może kreować i eskalować sytuacje kryzysowe, zagrażając wewnętrznej stabilności państwa[10]. W związku z tym, istotne staje się zrozumienie mechanizmów, które stoją za rozprzestrzenianiem się dezinformacji oraz rozwijanie metod jej przeciwdziałania. Dzięki zaawansowanym algorytmom i uczeniu maszynowemu, możliwe jest identyfikowanie i analizowanie wzorców rozprzestrzeniania fałszywych informacji w czasie rzeczywistym. Narzędzia te pozwalają na szybką interwencję i ograniczenie szkodliwego wpływu dezinformacji na społeczeństwo. Ponadto, edukacja cyfrowa i podnoszenie świadomości społecznej w zakresie krytycznego myślenia i weryfikacji informacji są kluczowe w walce z dezinformacją. Tylko poprzez połączenie technologicznych rozwiązań z edukacją i świadomością społeczną można skutecznie stawiać czoła temu wyzwaniu.

W państwach demokratycznych dezinformacja może powodować np. zakłócenia w demokratycznych wyborach. W wyniku skoordynowanej kam-

[8] E.M. Włodyka, *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewnienia cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, nr 1, s. 216.

[9] K. Kaczmarek, *Appealing to compassion as an element of Russia's hybrid warfare against the West*, „Cybersecurity and Law" 2022, nr 1, s. 52.

[10] K. Kaczmarek, *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, nr 2, s. 20.

panii dezinformacyjnej, prowadzonej przez wewnętrzne lub zagraniczne podmioty, w społeczeństwie pojawia się fala fałszywych informacji mających na celu zdyskredytowanie jednego z głównych kandydatów. Plotki i fałszywe oskarżenia o korupcję, nadużycia lub niekompetencje są rozpowszechniane za pośrednictwem mediów społecznościowych, co prowadzi do powszechnej dezorientacji i niewiary w autentyczność procesu wyborczego. Po wyborach, w których kandydat zdyskredytowany przez dezinformację przegrywa, dochodzi do masowych protestów, oskarżeń o fałszerstwa wyborcze i długotrwałego kryzysu politycznego, który osłabia zaufanie obywateli do instytucji demokratycznych. Przykładem takiego zjawiska jest skandal Cambridge Analytica z 2018 roku, który ujawnił, że dane nawet do 87 milionów profili na portalu społecznościowym Facebook zostały zebrane bez zgody użytkowników i wykorzystane do celów reklamowych w kampaniach prezydenckich w USA (Ted Cruz, Donald Trump), referendum w sprawie Brexitu, oraz w wyborach w ponad 200 krajach. Wykorzystanie tych danych miało na celu coraz bardziej wyrafinowaną dezinformację wyborców i tłumienie ich głosów, co podważa sens istnienia demokracji [11]. Dezinformacja może również wywołać skutecznie konflikt etniczny lub religijny w państwie o złożonej mozaice etnicznej i religijnej. Dezinformacja celowo rozpowszechniana przez ekstremistyczne grupy doprowadza do eskalacji napięć. Fałszywe wiadomości o rzekomych atakach i dyskryminacji jednej grupy wobec drugiej mogą być masowo udostępniane w mediach społecznościowych, co może prowadzić do wzajemnych oskarżeń i wzrostu nienawiści. W konsekwencji może dojść do lokalnych zamieszek, ataków na miejsca kultu i wzrostu przemocy na tle etnicznym i religijnym.

Przykładów takich skutków dezinformacji jest wiele, np.: w Afryce ekstremistyczne organizacje, takie jak Państwo Islamskie w Nigerii czy Al-Kaida w Mali, oraz rządy narodowe na Rogu Afryki, wykorzystywały dezinformację do wzmacniania swojej pozycji w trwających konfliktach. Szczególnie dotkliwe było to w konflikcie w regionie Tigraj w Etiopii, gdzie dezinformacja była wykorzystywana do podsycają i podtrzymywania etnicznych i regionalnych starć. Z kolei w konflikcie etiopskim grupy etniczne, takie jak Amha-

[11] S. Lai, *Data misuse and disinformation: Technology and the 2022 election*, https://www.brookings.edu/articles/data-misuse-and-disinformation-technology-and-the-2022-elections/, [dostęp: 31.12.2023].

rowie i Qemant, przeniosły swoją rywalizację do przestrzeni wirtualnej, a dezinformacja stała się głównym narzędziem konfliktu. Fałszywe doniesienia medialne o zajęciu miasta przez siły Tigraju doprowadziły do aresztowania dziennikarzy za fałszywe raportowanie, co ujawniło zależność rządu od cenzury w kształtowaniu narracji o konflikcie. Dezinformacja doprowadziła również do ofiar wśród mniejszości etnicznych, gdy rozpowszechniane online fałszywe informacje prowadziły do rzeczywistych aktów przemocy, jak w przypadku mniejszości Qemant w regionie Amhara. Fałszywe oskarżenia o sojuszu z Tigrajczykami i ataki w tamtym regionie doprowadziły do przemocy ze strony większościowej populacji Amharów[12].

Dezinformacja może wywołać również kryzys ekonomiczny. Przykładem jest rozpowszechnianie dezinformacji na temat rzekomego upadku ważnych banków lub kryzysu w kluczowych sektorach gospodarki, w skutek czego inwestorzy i konsumenci mogą wpaść w panikę. Szerzące się plotki o niestabilności finansowej mogą spowodować gwałtowny spadek wartości akcji, wycofywanie inwestycji i masową wyprzedaż aktywów. W efekcie rynki finansowe doświadczyć mogą wstrząsów, a niektóre firmy i instytucje finansowe rzeczywiście zaczynają borykać się z problemami, tworząc błędne koło kryzysu. Ten sztucznie wywołany kryzys gospodarczy może mieć długotrwałe skutki dla gospodarki narodowej i globalnej, prowadząc do wzrostu bezrobocia, spadku PKB i ogólnego spowolnienia wzrostu gospodarczego. Jako przykład można podać to, że w 2022 roku, w wyniku działania fałszywego konta na Twitterze, udającego firmę farmaceutyczną Eli Lilly, które ogłosiło, że insulina będzie rozdawana za darmo, cena akcji firmy spadła o 4,37%. Inwestorzy zostali wprowadzeni w błąd, a firma musiała podjąć wiele działań, aby odzyskać ich zaufanie[13].

Nie ma jednak możliwości przeciwdziałania wystąpieniu wszystkich sytuacji kryzysowych. Jednak dzięki podnoszeniu kompetencji informacyjnych społeczeństwa można zmniejszyć ich skalę i zmniejszyć poziom spowodo-

[12] J. Burnham, *From The Internet To Ashes: Disinformation And The Tigray War*, https://natoassociation.ca/from-the-internet-to-ashes-disinformation-and-the-tigray-war/, [dostęp: 31.12.2023].

[13] G. Di Domenico, *Subtle misinformation can affect what we buy, trust in brands*, https://www.upi.com/Voices/2024/01/04/misinformation-shopping-brands/4911704373576/#:~:text=For%20example%2C%20in%20late%202022%2C,statements%20to%20regain%20their%20trust, [dostęp: 7.01.2024].

wanych przez takie działania strat. Podsumowując należy zauważyć, że dezinformacja może mieć głębokie i rozległe skutki w różnych obszarach życia społecznego, politycznego i gospodarczego.

Ewolucja cyberbezpieczeństwa w kontekście nowoczesnych konfliktów: strategie ochrony infrastruktury krytycznej i zarządzania kryzysowego w obliczu zmieniających się zagrożeń dywersyjnych i terrorystycznych

Dezinformacja jest jednym z możliwych aktywności, które wykorzystują ICT i są skierowane przeciwko państwom. W kontekście współczesnych konfliktów politycznych i wojskowych, zauważalnym zjawiskiem jest wzrost liczby cybernetycznych działań wymierzonych w infrastrukturę krytyczną, w tym szczególnie sieci energetyczne. Ta tendencja, obserwowana w ostatnich dekadach, jest odzwierciedleniem ewolucji strategii wojennych, gdzie działania w cyberprzestrzeni nabierają równie istotnego znaczenia, co tradycyjne operacje militarne. Cybernetyczne ataki na infrastrukturę krytyczną, będące często trudne do jednoznacznej identyfikacji i przypisania konkretnemu sprawcy, mają na celu nie tylko wywołanie bezpośrednich szkód materialnych, ale również sianie niepokoju i destabilizację społeczną. Stanowią one nowe wyzwanie dla bezpieczeństwa narodowego, wymuszając rozwój zaawansowanych metod obrony cyfrowej oraz adaptację strategii bezpieczeństwa do zmieniającego się środowiska zagrożeń. Cyberataki przeprowadzane na infrastrukturę krytyczną, w tym sieci energetyczne, miały miejsce niemal we wszystkich ostatnich kryzysach politycznych i wojskowych[14].

W odpowiedzi na te zagrożenia, rządy i organizacje na całym świecie intensyfikują swoje działania w zakresie ochrony infrastruktury krytycznej. Opracowywane są nowe strategie i systemy, które mają na celu nie tylko wykrywanie i neutralizowanie cyberataków, ale również zabezpieczanie kluczowych zasobów przed ich skutkami. Działania te obejmują wdrażanie zaawansowanych systemów monitorowania i analizy danych, co pozwala na szybsze identyfikowanie potencjalnych zagrożeń i reagowanie na nie w odpowiedni

[14] K. Kaczmarek, *Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, „Cybersecurity and Law" 2023, nr 1, s. 208.

sposób. Szczególną uwagę przykłada się do zabezpieczania sieci energetycznych, które stanowią kręgosłup działania wielu innych sektorów gospodarki. W tym kontekście, kluczowym elementem jest nie tylko ochrona przed atakami, ale również zapewnienie ciągłości działania i szybkiego reagowania w przypadku wystąpienia zakłóceń[15]. Głównym zadaniem zapewnienia bezpieczeństwa dostaw jest utrzymanie efektywności działania sieci i usług cyfrowych, które są istotne dla kluczowych funkcji oraz ich wytrzymałość i zdolność do szybkiego przywracania normalnego działania. Ponadto, istotne jest także efektywne zarządzanie i dostęp do danych, aby można było mieć do nich dostęp nawet w trakcie poważnych zdarzeń i sytuacji kryzysowych[16]. Aktualna sytuacja międzynarodowa wskazuje, że coraz bardziej prawdopodobne stają się zdarzenia o charakterze dywersyjnym lub terrorystycznym. Można nawet przypuszczać, że ryzyko ataków terrorystycznych, które mogą być inspirowane przez Moskwę wzrasta, a możliwość użycia zdeponowanej na dnie Morza Bałtyckiego broni chemicznej jako narzędzia w takich atakach staje się coraz bardziej prawdopodobna[17]. Jednocześnie pandemia COVID-19 w 2020 roku pokazała, że wcześniejsze schematy społeczno-gospodarcze i polityczne nie sprawdziły się w sytuacji kryzysowej[18]. Koniecznością stało się posiadanie tzw. rezerw strategicznych[19]. Rezerwy te są niezwykle ważne w sytuacjach kryzysowych, ponieważ zapewniają niezbędne zasoby, które mogą być szybko wykorzystane w przypadku awarii, katastrof naturalnych, wojen czy innych poważnych zakłóceń. Dzięki nim rządy i organizacje mogą zachować ciągłość działania kluczowych sektorów.

---

[15] *Narodowy Program Ochrony Infrastruktury Krytycznej*, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej, [dostęp: 7.01.2024].

[16] K. Kaczmarek, *Wyzwania stojące przed rozwojem społeczeństwa informacyjnego w Laponii,* „Cybersecurity and Law" 2022, nr 2, s. 294-295.

[17] K. Kaczmarek*, Zatopione w Morzu Bałtyckim bojowe środki trujące – analiza możliwości ich przez Federację Rosyjską w działaniach terrorystycznych*, „Acta Politica Polonica" 2023, nr 2, s. 79.

[18] E.M. Włodyka*, Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim*, „Acta Politica Polonica" 2021, nr 2, s. 90.

[19] K. Kaczmarek*, Bezpieczeństwo energetyczne państwa w obliczu pandemii COVID-19 na przykładzie Republiki Finlandii*, „Cybersecurity and Law" 2023, nr 1, s. 176-178.

Podsumowanie

W obliczu rosnących wyzwań związanych z cyberbezpieczeństwem i dezinformacją, kluczowe staje się wzmocnienie strategii ochrony infrastruktury krytycznej i rozwój skutecznych metod zarządzania kryzysowego. Także edukacja cyfrowa i związane z nią podnoszenie świadomości społecznej są niezbędne do przeciwdziałania dezinformacji i zwiększania odporności na cyberataki. Owa, wymieniona już wcześniej, edukacja cyfrowa oraz edukacja dla bezpieczeństwa są niezwykle istotne w kontekście rosnących zagrożeń wynikających z postępu technologicznego. W erze cyfryzacji, gdzie technologia przenika każdy aspekt życia, umiejętność bezpiecznego i świadomego korzystania z narzędzi cyfrowych staje się kluczowa. Edukacja w tym zakresie pomaga w rozumieniu ryzyka związanego z cyberzagrożeniami oraz uczy skutecznych metod ich przeciwdziałania.

Współpraca międzynarodowa, innowacje w bezpieczeństwie cyfrowym i ciągłe monitorowanie zagrożeń staną się kluczowymi elementami w zapewnieniu globalnej stabilności i bezpieczeństwa. W tym dynamicznie nas otaczającym, zmieniającym się środowisku, adaptacja i proaktywne działania są niezbędne do ochrony przed nowymi, coraz bardziej zaawansowanymi zagrożeniami.

Konieczność przygotowania nawet na mało prawdopodobne, ale możliwe sytuacje jest ważna, ponieważ złożoność technologii i dynamika zmian zwiększają ryzyko nieprzewidzianych wydarzeń. Należy wypracować zdolność społecznego szybkiego reagowania i adaptacji do nieoczekiwanych sytuacji, co jest niezbędne w szybko zmieniającym się świecie. Dodatkowo, krytyczne podejście do otrzymywanych informacji jest niezbędne w dobie powszechnej dezinformacji i manipulacji. Rozwijanie w społeczeństwach umiejętności analitycznych, krytycznego myślenia oraz weryfikacji źródeł informacji, co jest kluczowe dla ochrony przed manipulacją i fałszywymi wiadomościami.

Bibliografia

Bencsik A., Karpiuk M., Kelemen M., Włodyka E., *Cybersecurity in the Visegrad Group Countries*, Maribor 2023.

Kaczmarek K. *Możliwości stosowania technologii informacyjno-komunikacyjnych w walce z korupcją,* „Cybersecurity and Law" 2021.

Kaczmarek K., *Appealing to compassion as an element of Russia's hybrid warfare against the West*, „Cybersecurity and Law" 2022, nr 1.

Kaczmarek K.*, Bezpieczeństwo energetyczne państwa w obliczu pandemii COVID-19 na przykładzie Republiki Finlandii*, „Cybersecurity and Law" 2023, nr 1.
Kaczmarek K., *Darknet jako przedmiot badań nauk społecznych*, „Cybersecurity and Law" 2024, nr 2, s. 106.
Kaczmarek K., *Dezinformacja jako czynnik ryzyka w sytuacjach kryzysowych*, „Roczniki Nauk Społecznych" 2023, nr 2.
Kaczmarek K.*, Finland in the light of cyber threats in the context of Russia's aggression against Ukraine*, „Cybersecurity and Law" 2023, nr 1.
Kaczmarek K., *Transformacja Estonii po rozpadzie Związku Radzieckiego. Determinanty historyczne i analiza porównawcza skutków,* „Acta Politica Polonica" 2022, nr 2.
Kaczmarek K., *Wyzwania stojące przed rozwojem społeczeństwa informacyjnego w Laponii,* „Cybersecurity and Law" 2022, nr 2.
Kaczmarek K., *Zapobieganie zagrożeniom cyfrowym na przykładzie Republiki Estońskiej i Republiki Finlandii*, „Cybersecurity and Law" 2019, nr 1.
Kaczmarek K.*, Zatopione w Morzu Bałtyckim bojowe środki trujące – analiza możliwości ich przez Federację Rosyjską w działaniach terrorystycznych*, „Acta Politica Polonica" 2023, nr 2.
Mishra S., *Digital cultures,* Londyn 2021.
Włodyka E.M.*, Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim*, „Acta Politica Polonica" 2021, nr 2.
Włodyka E.M., *Dostępność cyfrowa w Unii Europejskiej – praktyka i założenia teoretyczne*, „Rocznik Integracji Europejskiej" 2022, nr 16.
Włodyka E.M., *Gotowi – do startu – start? Przyczynek do dyskusji nad gotowością jednostek samorządu terytorialnego do zapewnienia cyberbezpieczeństwa*, „Cybersecurity and Law" 2022, nr 1.

* * *

Cybersecurity and disinformation in the modern world: protection strategies and crisis management

Abstract

The contemporary threat in cyberspace focuses on the increase in cyberattacks on critical infrastructure and their social consequences, pointing to the need for effective protection and crisis management strategies. In this text, the author emphasizes the importance of digital education and social awareness in counteracting disinformation and minimizing the risk of crisis situations, also in the context of contemporary political and military conflicts. An attempt was made to identify factors related to cyber-

security, disinformation and protection of critical infrastructure. Examples of strategies to combat the growing level of cyber threats were also provided, emphasizing the need to adapt defense approaches to the dynamically changing threat environment. The aim of this article is to analyze the vulnerability of societies to threats resulting from digitalization in the context of a crisis situation. Particular attention is paid to disinformation in the context of the level of information and digital competences of societies and the possibility of a crisis situation resulting from an uncritical approach to digital content and solutions proposed by algorithms. The research methods used are content analysis and case studies supplemented with comparative, systemic and qualitative methods.

Keywords: cybersecurity, disinformation, critical infrastructure, crisis management, digital education.