

Zagrożenia i wyzwania BEZPIECZEŃSTWA w cyberprzestrzeni

REDAKCJA NAUKOWA
Marta Pomykała
Izabela Oleksiewicz

Niniejszy pdf zawiera 5 tekstów w dostępie otwartym. Całą monografię można zakupić w formie e-booka, korzystając z poniższych linków.

Oficina Wydawnicza Politechniki Rzeszowskiej współpracuje z firmą OSDW Azymut, zapewniając bezpieczną dystrybucję publikacji elektronicznych na rynku księgarskim i bibliotecznym. Dzięki temu publikacje docierają do księgarni Grupy Wydawniczej PWN:

www.ksiegarniapwn.pl, <https://pzw1.pl/> i wielu indywidualnych księgarni internetowych, m.in.: gandalf.com.pl, inbook.pl, bookmaster.pl, virtualo.pl, woblink.com, publio.pl, ebookpoint.pl, a także do największej wypożyczalni i księgarni internetowej z e-bookami i audiobookami w Polsce – IBUK.pl.



**OFICyna
WYDawnicza**
POLITECHNIKI RZESZOWSKIEJ

Wydano za zgodą Rektora

Recenzent

dr hab. Wojciech GONET, prof. UwS

Redaktor naczelny

Wydawnictw Politechniki Rzeszowskiej
dr hab. inż. Lesław GNIEWEK, prof. PRz

Redaktor

Piotr CYREK

Skład i łamanie tekstu

Mariusz TENDERA

Projekt okładki

Joanna MIKUŁA

*cyberbezpieczeństwo, zagrożenia i wyzwania cyberbezpieczeństwa,
polityka cyberbezpieczeństwa, cyberprzestrzeń
cybersecurity, cybersecurity threats and challenges, cybersecurity policy, cyberspace*

© Copyright by Oficyna Wydawnicza Politechniki Rzeszowskiej
Rzeszów 2024

Wszelkie prawa autorskie i wydawnicze zastrzeżone. Każda forma powielania oraz przenoszenia na inne nośniki bez pisemnej zgody Wydawcy jest traktowana jako naruszenie praw autorskich, z konsekwencjami przewidzianymi w *Ustawie o prawie autorskim i prawach pokrewnych* (Dz.U. z 2018 r., poz. 1191 t.j.). Autor i Wydawca dołożyli wszelkich starań, aby rzetelnie podać źródło zamieszczonych ilustracji oraz dotrzeć do właścicieli i dysponentów praw autorskich. Osoby, których nie udało się ustalić, są proszone o kontakt z Wydawnictwem.

p-ISBN 978-83-7934-711-7

e-ISBN 978-83-7934-715-5

Oficyna Wydawnicza Politechniki Rzeszowskiej
al. Powstańców Warszawy 12, 35-959 Rzeszów
<https://oficyna.prz.edu.pl>

Ark. wyd. 22,17. Ark. druk. 21,50.
Wydrukowano w maju 2024 r.
Drukarnia Oficyny Wydawniczej,
al. Powstańców Warszawy 12, 35-959 Rzeszów
Zam. nr 12/24

SPIS TREŚCI

Wstęp	5
-------------	---

I. Cyberbezpieczeństwo – istota i problemy definiowania

Marta Pomykała, Izabela Oleksiewicz: Cyberbezpieczeństwo jako nowy wymiar współczesnego bezpieczeństwa państwa	11
Edyta Dubois: Rozwój technologii informatycznych w administracji publicznej a bezpieczeństwo państwa	23
Małgorzata Polkowska, Marzena Toumi: Społeczność międzynarodowa wobec zagrożeń cyberatakami i terroryzmem kosmicznym	43
Dagmara Florek-Klęsk: Współczesne zagrożenia bezpieczeństwa lotnictwa cywilnego – wybrane zagadnienia	57

II. Zwalczanie cyberprzestępczości

Beata Gocko: <i>Phising</i> wyzwaniem współczesnego świata – skala zjawiska oraz odpowiedzialność prawna	69
Andrzej Kieltyka: Przestępstwa z ustawy o zwalczaniu nadużyć w komunikacji elektronicznej	85
Bogusław Olewiński: Zadania organów ścigania w zwalczaniu cyberprzestępstw	95
Zygmunt Dudek: Współpraca organów ścigania z operatorami logistycznymi i internetowymi platformami handlowymi w zakresie zwalczania przestępczości	107

III. Problemy cyberbezpieczeństwa w obszarze ochrony danych osobowych i informacji

Elżbieta Kosior: Naruszenie ochrony danych osobowych jako incydent bezpieczeństwa informacji – wybrane aspekty prawne i praktyczne	123
Sylwia Zaborska: Wykorzystanie biometrii głosu – szanse i zagrożenia	137
Julia Mazurkiewicz: <i>Sharenting</i> – problem społeczny czy luka prawna?	143

IV. Wyzwania cyberbezpieczeństwa a współczesna gospodarka

Bogusław Bembenek: Cyberbezpieczeństwo w warunkach Przemysłu 4.0 jako współczesne wyzwanie w zarządzaniu klastrem	153
Teresa Piecuch, Agata Ziemiakowicz, Karolina Płachta: Problemy przedsiębiorców prowadzących biznes on-line	171
Agnieszka Pieniążek: Cyberbezpieczeństwo w programach Interreg: NEXT Polska-Ukraina i Słowacja-Polska w perspektywie finansowej 2021–2027 ...	187
Bożydar Ziółkowski: Aspekty bezpieczeństwa w kontekście etykiet i deklaracji środowiskowych	195
Jacek Meissner: Technologie kwantowe a bezpieczeństwo państwa	205

V. Problemy cyberbezpieczeństwa w obszarze obronności

Krzysztof Chochowski: Szpiegostwo maszynowe szansą i wyzwaniem dla służb specjalnych	223
Markus Bresinsky, Francesca Elena Strat: ChatGPT supporting intelligence analysis in strategic forecasting	231
Andrzej Żebrowski: Bezpieczeństwo osobowej przestrzeni informacyjnej w wojnie informacyjnej. Wybrane aspekty	259
Waldemar Krztoń: Broń cyfrowa istotnym elementem walki w epoce Internetu	293
Kacper Mazurek, Piotr Padula, Seweryn Walas: Charakterystyka i wyzwania armii IT Ukrainy	303
Bibliografia	315
Streszczenie	341
Summary	342

WSTĘP

Cyberprzestrzeń według definicji wprowadzonej przez rząd Wielkiej Brytanii to: „wirtualna przestrzeń wszystkich systemów technologii informacyjnej powiązanych na poziomie danych w skali globalnej. Fundament cyberprzestrzeni stanowi Internet jako uniwersalna oraz powszechnie dostępna sieć oferująca połączenia oraz transport, która może być uzupełniana oraz rozszerzana dalej przez dowolną ilość dodatkowych sieci danych. Systemy IT działające w wyizolowanej przestrzeni wirtualnej nie stanowią części cyberprzestrzeni”¹.

Zagrożenia w cyberprzestrzeni stają się coraz poważniejsze i obejmują coraz więcej obszarów, stając się istotnym problemem nie tylko bezpieczeństwa wewnętrznego, ale też bezpieczeństwa poszczególnych państw. Bezpośrednie zagrożenia dla bezpieczeństwa cybernetycznego stwarza państwo rosyjskie, a wiele gangów zajmujących się przestępczością zorganizowaną przeprowadzających ataki oprogramowania ransomware na cele zachodnie ma swoje siedziby na terenie Rosji. Chiny pozostały wysoce wyrafinowanym aktorem w cyberprzestrzeni z rosnącymi ambicjami wysunięcia swoich wpływów poza swoje granice. Rozwój Chin w następnej dekadzie będzie prawdopodobnie najważniejszym czynnikiem wpływającym na przyszłe bezpieczeństwo cybernetyczne Europy. Iran i Korea Południowa, choć mniej wyrafinowane niż Rosja i Chiny, w dalszym ciągu wykorzystują włamanie cyfrowe do osiągnięcia swoich celów, w tym poprzez kradzież i sabotaż.

Wydaje się, że zagrożenia w cyberprzestrzeni będą dalej ewoluować i różnicować się, w miarę jak zaawansowane możliwości cybernetyczne będą utowarowione i rozprzestrzeniane na więcej państw i grup przestępczych. Będzie też wzrastać liczba podmiotów zdolnych i zamierzających obrać za cel państwo w cyberprzestrzeni, a państwa będą stosować szerszy zakres działań zakłócających, w tym z wykorzystaniem podmiotów zastępczych. Przyspieszone przejście na pracę hybrydową i ograniczenia w podróżach międzynarodowych, będące skutkiem pandemii COVID-19, doprowadziło do większego uzależnienia od usług cyfrowych i zachęciło zorganizowane grupy przestępcze do podejmowania cyberprzestępczości. Analizując statystyki przestępczości za ostatnie lata można zaobserwować znacznie szybszy wzrost liczby cyberprzestępstw².

Po części można dokonać ekstrapolacji zagrożeń przypisanych dotychczas do funkcjonowania państwa na pozostałe płaszczyzny. Jednak w przypadku cyberzagrożeń w większym stopniu są one generowane przez podmioty pozapaństwowe –

¹ National Cyber Strategy 2022 (www.gov.uk) (dostęp: 27.02.2024 r.).

² Raport ENISA 2023, Bruksela 2023, s. 11–12.

grupy terrorystyczne i zorganizowaną przestępczość, które ciężko zidentyfikować. Wymaga to określenia potencjalnych wymiarów narażonych na ich występowanie w kontekście funkcjonowania państwa. Przyjmując, że bezpieczeństwo w cyberprzestrzeni jest procesem, który będzie ewoluował w czasie, zagrożenia w tej płaszczyźnie funkcjonowania państwa mogą być generowane bez konieczności fizycznego połączenia między sieciami czy systemami.

Zagrożenia bezpieczeństwa w cyberprzestrzeni można podzielić w oparciu o wiele kryteriów. Zagrożenia mogą odnosić się do sytuacji mających wpływ na bezpieczeństwo wewnętrzne państwa, ład i porządek publiczny, albo jako zagrożenia zewnętrzne stanowić kategorię zjawisk, które mają odniesienie do zdarzeń poza granicami państwa. Przyjmując jako kryterium podmiot zagrożenia można wyróżnić co najmniej trzy grupy: zagrożenia państwa w cyberprzestrzeni, zagrożenia podmiotów pozapaństwowych, zagrożenia obywateli. Do pierwszej grupy, zagrożeń państwa należą: cyberprzestępczość, cyberdemonstracje o charakterze destrukcyjnym, zakłócającym realizację istotnych zadań administracji publicznej oraz sektora prywatnego, zagrożenia dla infrastruktury krytycznej, cyberszpiegostwo, cyberkonflikt, cyberwojna. Zagrożenia dla podmiotów pozapaństwowych – do nich można zaliczyć: cyberdemonstracje, kradzież danych, naruszenie poufności prowadzonych działań czy dostępności usług, cyberszpiegostwo, incydenty związane z bezpieczeństwem informacji. Ostatnią kategorią jest zagrożenie obywateli: cyberprzemoc, cyberdemonstracje, usługi teleinformatyczne, kradzież danych, kradzież tożsamości, przejmowanie kontroli nad prywatnymi komputerami czy sprzętem podłączonym do sieci, cyberprzestępczość.

Redaktorzy niniejszej publikacji zwrócili uwagę na cybernetyczne aspekty bezpieczeństwa państwa, jak również na transgraniczny wymiar tego zjawiska. Biorąc pod uwagę fakt, że cyberprzestrzeń stanowi złożony obszar badawczy opracowanie tak szerokiego spektrum zagadnień wymagało zaproszenia do współpracy przedstawicieli różnych ośrodków akademickich, badających różnorodne zagadnienia, jak również praktyków, którzy z poruszaną problematyką spotykają się w codziennej pracy.

Celem monografii jest przekrojowa i interdyscyplinarna analiza bezpieczeństwa państwa w cyberprzestrzeni oraz jej zagrożeń. Dlatego też autorzy tekstów podjęli próbę wskazania zarówno istoty cyberprzestrzeni jako nowej kategorii badań nad bezpieczeństwem państwa, jak również identyfikacji uwarunkowań cyberbezpieczeństwa państwa, głównych przestępstw powiązanych z cyberprzestrzenią i ochroną danych osobowych oraz wyzwań, jakie pociąga za sobą gospodarka funkcjonująca w obszarze cybersfery. Przedmiotem badawczym są zatem zagrożenia w cyberprzestrzeni, natomiast podmiotem badawczym jest państwo, obywatele i podmioty pozapaństwowe. W pracy zostaną przedstawione i przeanalizowane zależności oraz rozbieżności problemów bezpieczeństwa wewnętrznego państwa i organizacji międzynarodowych, a tym samym zostaną poruszone zagadnienia związane z polityką cyberbezpieczeństwa państwa.

Na strukturę monografii składa się pięć części. Pierwsza z nich, stanowiąca punkt wyjścia dla podjętych w pracy badań, obejmuje analizę zagadnień związanych ze specyfiką cyberbezpieczeństwa jako elementu współczesnego bezpieczeństwa państwa. Tekst autorstwa Izabeli Oleksiewicz i Marty Pomykała pt. *Cyberbezpieczeństwo jako nowy wymiar współczesnego bezpieczeństwa państwa* zwraca uwagę na specyfikę cyberprzestrzeni jako nowego wymiaru rzeczywistości, złożoność i wieloaspektowość zagrożeń w cyberprzestrzeni oraz na uniwersalność cyberbezpieczeństwa. Edyta Dubois omawia rozwój technologii informatycznych w administracji publicznej w kontekście bezpieczeństwa państwa. Małgorzata Polkowska i Marzena Toumi w swoich rozważaniach na temat społeczności międzynarodowej wyjaśniają wielorakie podejście nauki wobec zagrożeń cyberatakami i terroryzmem kosmicznym. Dagmara Florek-Klęsk w rozdziale pt. *Współczesne zagrożenia bezpieczeństwa lotnictwa cywilnego – wybrane zagadnienia* przedstawia na przykładzie danych statystycznych z ostatnich lat prawdopodobieństwo zaistnienia w przestrzeni powietrznej zjawiska terroryzmu i omawia na podstawie obowiązujących przepisów prawnych szczegółowe procedury postępowania w takich sytuacjach.

Przedmiotem analizy drugiej części publikacji są problemy cyberprzestępczości oraz jej zwalczania. Na początku Beata Gocko omawia przestępstwo *phishingu*, będącego poważnym wyzwaniem współczesnego świata, pokazując jego skalę statystyczną oraz zasady odpowiedzialności w polskim prawie karnym. Andrzej Kiełtyka analizuje przestępstwa z ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. Bogusław Olewiński przedstawia zadania polskich organów ścigania w zwalczaniu cyberprzestępstw. Zygmunt Dudek zwraca uwagę na znaczenie współpracy organów ścigania z operatorami logistycznymi i internetowymi platformami handlowymi w zakresie zwalczania cyberprzestępczości.

W obliczu rosnących zagrożeń informacyjnych, wraz ze złożonością problemów występujących w obszarze ochrony danych osobowych i informacji ważną rolę dla bezpieczeństwa wewnętrznego każdego państwa pełnią również problemy cyberbezpieczeństwa w zakresie ich ochrony. To one przyczyniają się także do wzrostu bezpieczeństwa na poziomie państwowym, jak i międzynarodowym. W związku z powyższym, trzecia część została poświęcona wyżej wymienionym zagadnieniom. Część tę rozpoczyna tekst Elżbiety Kosior pt. *Naruszenie ochrony danych osobowych jako incydent bezpieczeństwa informacji – wybrane aspekty prawne i praktyczne*. Autorka omawia w nim incydenty prawne na podstawie ustaw i wybranych orzeczeń sądownictwa. Sylwia Zaborska w swoim materiale wskazuje na szanse i zagrożenia wykorzystania sztucznej inteligencji w rozpoznawalności głosu nie tylko w życiu codziennym, ale również na przykładzie innych jednostek jak np. banki. Julia Mazurkiewicz zwraca uwagę na problem shareingu stawiając jednocześnie pytanie, czy mamy tu do czynienia z luką prawną, czy może jedynie z nowym zjawiskiem społecznym.

W czwartej części pt. *Wyzwania cyberbezpieczeństwa a współczesna gospodarka* poddano analizie zagadnienia z zakresu ekonomii. Określono w niej

przyczyny zaistnienia zjawiska cyberterroryzmu (czynniki wewnętrzne i czynniki zewnętrzne), co pozwoliło na stwierdzenie, jaki wpływ wywiera zjawisko cyberterroryzmu na politykę bezpieczeństwa państwa i przedsiębiorców. Przedstawiono również analizę zmian w polityce cyberbezpieczeństwa UE po 2020 roku oraz zaproponowano nowe rozwiązania mające służyć wzmocnieniu polityki państwa, tym samym wpływające na wzrost bezpieczeństwa wewnętrznego i zewnętrznego dzisiejszej Europy. Bogusław Bemberek w swoim rozdziale zaprezentował istotę cyberbezpieczeństwa w warunkach Przemysłu 4.0, jako współczesne wyzwanie w zarządzaniu klastrem. Teresa Piecuch, Agata Ziemiakowicz, Karolina Płachta ukazały w rozdziale problemy przedsiębiorców prowadzących biznes online. Agnieszka Pieniążek przeanalizowała cyberbezpieczeństwo w programach Interreg: Next Polska-Ukraina i Słowacja-Polska w perspektywie finansowej 2021–2027. Bożydar Ziółkowski zwrócił uwagę na aspekty bezpieczeństwa w kontekście etykiet i deklaracji środowiskowych, natomiast Jacek Meissner zbadał zależność technologii kwantowych od bezpieczeństwa państwa.

Ocena problemów cyberbezpieczeństwa w obszarze obronności jest przedmiotem analizy części piątej, gdzie Krzysztof Chochowski przedstawia szpiegostwo maszynowe i sztuczną inteligencję jako szansę, a zarazem wyzwanie dla służb specjalnych. Markus Bresinsky i Francesca Elena Strat ukazali możliwość wykorzystania AI w polityce zwalczania cyberterroryzmu jako narzędzia przewidyującego różnorakie scenariusze. Andrzej Żebrowski określa czym jest bezpieczeństwo osobowe w przestrzeni informacyjnej w wojnie informacyjnej na wybranych przykładach. Waldemar Krztoń porusza w swoim opracowaniu zagadnienie broni cyfrowej jako istotnego elementu walki w epoce Internetu, a Kacper Mazurek, Piotr Padula, Seweryn Walas podjęli temat charakterystyki i wyzwań armii IT Ukrainy.

Warto podkreślić, że niniejsze opracowanie stanowi kompleksowy przegląd literatury naukowej o tematyce bezpieczeństwa w cyberprzestrzeni. Polski i zagraniczny dorobek badawczy w tym zakresie pozwala na dokonanie syntezy wielu ważnych zjawisk. Konieczna jest jednak refleksja, że wiele obszarów szczegółowych nie zostało jak dotąd poddanych wystarczającej analizie, co powinno stanowić wyzwanie na przyszłość dla środowiska akademickiego. Analizie poddane zostały również akty normatywne regulujące przedmiotową materię. Autorzy oparli poszczególne rozdziały na dorobku prawnym wybranych państw, jak również źródłach prawa międzynarodowego, danych statystycznych i netografii.

*Marta Pomykała³
Izabela Oleksiewicz⁴*

³ Marta Pomykała, dr hab., prof. PRz. Politechnika Rzeszowska im. Ignacego Łukasiewicza. ORCID: 0000-0002-2557-1876.

⁴ Izabela Oleksiewicz, dr hab., prof. PRz. Politechnika Rzeszowska im. Ignacego Łukasiewicza. ORCID: 0000-0002-1622-7467.

I.
Cyberbezpieczeństwo
– istota i problemy definiowania

Izabela OLEKSIEWICZ, dr hab., prof. PRz¹
Marta POMYKAŁA, dr hab., prof. PRz²

CYBERBEZPIECZEŃSTWO JAKO NOWY WYMIAR WSPÓŁCZESNEGO BEZPIECZEŃSTWA PAŃSTWA

1. Geneza cyberprzestrzeni

Powstanie i rozwój cyberprzestrzeni są nierozdzielnie związane z rozprzestrzenianiem się sieci Internet, która najczęściej określana jest jako globalna sieć komputerowa, czyli sieć sieci. Cyberprzestrzeń jest równoległą przestrzenią niefizyczną, niekonkurencyjną w stosunku do przestrzeni trójwymiarowej. Budulcem cyberprzestrzeni są dane i informacje, które przez wzajemne oddziaływania między sobą kreują mikrokorelacje. Między przestrzenią trójwymiarową a cyberprzestrzenią zachodzą natomiast makrokorelacje. Ich charakter jest interpersonalny.

Kluczowymi cechami cyberprzestrzeni, które odróżniają ją od tradycyjnie rozumianej przestrzeni, są aterytorialność i globalność³. Aktywność w cyberprzestrzeni nie jest ograniczona poprzez granice geograficzne czy polityczne. Połączenia z siecią możliwe są z każdego miejsca na świecie, a ich ograniczeniem może być co najwyżej przepustowość łącza i możliwości techniczne. Aspekt globalny cyberprzestrzeni wyraża się natomiast w tym, że łączy ona cały świat, dając możliwość szybkiej i efektywnej wymiany informacji pomiędzy różnymi regionami i kulturami. Jej użytkownicy mogą nawiązywać relacje w czasie rzeczywistym.

W konsekwencji powstania cyberprzestrzeni pojawiło się społeczeństwo informacyjne. Jest ono sprzęgnięte z przemianami technologicznymi, mającymi niewątpliwie humanistyczne i przyrodnicze (antropologiczne) konsekwencje⁴. Za początek społeczeństwa informacyjnego i źródło jego powstania uważa się lata 1956–1957, czyli rozwój gospodarki Stanów Zjednoczonych oraz wstąpienie Japonii do Organizacji Narodów Zjednoczonych (ONZ), a także wystrzelenie w 1956 roku radzieckiego sputnika w Kosmos. Zapoczątkowało to erę globalnej

¹ Politechnika Rzeszowska im. Ignacego Łukasiewicza. ORCID: 0000-0002-1622-7467.

² Politechnika Rzeszowska im. Ignacego Łukasiewicza. ORCID: 0000-0002-2557-1876.

³ M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny” 2018, nr 1–2, s. 60.

⁴ *Ibidem*, s. 60 i n.

komunikacji satelitarnej⁵. W roku 1999 prof. Hubert Kubicek⁶ określił społeczeństwo informacyjne jako formację społeczno-gospodarczą, w której decydującą rolę odgrywają produktywne wykorzystanie informacji oraz intensywna produkcja nakierowana na wiedzę. Według Kubickiego społeczeństwo można nazwać informacyjnym wtedy, gdy obywatele intensywnie korzystają z informacji.

Należy zgodzić się z Piotrem Delą, że „cyberprzestrzeń to przestrzeń kooperacji międzyludzkich z wykorzystaniem urządzeń elektronicznych do wytwarzania, przechowywania, przekazywania i przetwarzania informacji”⁷. Współdziałanie to może odbywać się w trzech relacjach:

- człowiek – człowiek,
- człowiek – cyberprzestrzeń,
- cyberprzestrzeń – człowiek.

W pierwszej relacji cyberprzestrzeń jest tylko środowiskiem informacyjnym umożliwiającym wymianę informacji między jej użytkownikami. W drugim przypadku cyberprzestrzeń jest środowiskiem, w którym odbiorca i nadawca tworzą własny wirtualny świat, czyli świat wirtualnej rzeczywistości. Trzecia relacja dotyczy wykorzystania sztucznej inteligencji jako elementu cyberprzestrzeni zdolnego do samodzielnego rozwiązywania problemów odnoszących się do użytkowników⁸.

Z cyberprzestrzenią bezpośrednio związana jest przestrzeń informacyjna, będąca złożoną całością interakcji, wartości i funkcji łączących światy: realne, wirtualne, indywidualne, społeczne, przeszłe, obecne i przyszłe⁹. To nie tylko narzędzie wymiany informacji między elementami składowymi systemu bezpieczeństwa podmiotu, lecz także odbicie ich wzajemnych powiązań i relacji¹⁰. Na początku przestrzeń informacyjna obejmowała zasięgiem tylko społeczności lokalne, lecz z upływem czasu, rozwojem struktur społecznych, umiejętnością wykorzystania narzędzi komunikacyjnych zwiększał się obszar jej powiązań. Rozwój informatyki, telekomunikacji i teleinformatyki doprowadził do tego, że obecnie obejmuje ona swoim zasięgiem całą kulę ziemską, skracając czas obiegu informacji do minimum. To cyberprzestrzeń przeobraziła przestrzeń informacyjną, nadając jej globalny charakter.

⁵ I. Oleksiewicz, *Ochrona cyberprzestrzeni Unii Europejskiej. Polityka. Strategia. Prawo*, Warszawa 2021, s. 18–20.

⁶ Por.: J. Wrona, *Przestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Białystok 2017, s. 23.

⁷ Urządzenia elektroniczne wchodzące w skład infrastruktury teleinformatycznej niezbędnej do należytego gromadzenia, przetwarzania, przechowywania i wymiany informacji. Infrastrukturę tę tworzą przede wszystkim sieć Internet i inne sieci teleinformatyczne. P. Dela, *Teoria walki w cyberprzestrzeni*, Warszawa 2020.

⁸ P. Dela, *Zasady sztuki wojennej w cyberprzestrzeni* [w:] *Wojny i konflikty zbrojne XXI wieku – podejście polemologiczne*, red. A. Polak, J. Lasota, M. Palczewska, Warszawa 2016, s. 314.

⁹ P. Sienkiewicz, *Wizje i modele wojny informacyjnej* [w:] L.S. Haber, *Spółczesność informacyjna – wizja czy rzeczywistość*, Kraków 2004, s. 375.

¹⁰ R. Kwećka, *Strategia bezpieczeństwa informacyjnego państwa*, Warszawa 2014, s. 25.

Współcześnie cyberprzestrzeń jest przestrzenią wzmożonego ryzyka. Im więcej wiedzy, tym bardziej rośnie niepewność i ryzyko, tym bardziej złożone stają się struktury społeczne. Skutkami ubocznymi są kradzieże, włamania, spam i wirusy. Globalizacja spowodowała, że wszyscy bez wyjątku bezustannie zaczęli się wzajemnie obserwować i porównywać. W erze globalizacji cybernetyka sieci jest nie tyle technologią, ile raczej technosystemem strategicznej komunikacji, którego działanie pociąga za sobą systemowe ryzyko niszczącej wszystko wokół reakcji.

Cyberprzestrzeń to miejsce, które pojedynczym osobom i całym społeczeństwom daje możliwość tworzenia nowych relacji. To specyficzna przestrzeń, w której można działać niezależnie od otoczenia, a zasadniczym elementem cyberprzestrzeni jest informacja. Informacje w cyberprzestrzeni mogą być wykorzystywane do różnych celów. Za pomocą informacji prowadzona może być walka informacyjna, której celem jest uzyskanie wpływu na zachowanie podmiotów będących celem ataku, zakłócanie lub uniemożliwienie funkcjonowania zaatakowanego systemu informatycznego, a także fizyczne niszczenie infrastruktury informatycznej przeciwnika.

Zagrożenia w cyberprzestrzeni

Wraz z pojawieniem się cyberprzestrzeni pojawiły się nowe, nieznane dotąd zagrożenia i wyzwania dla bezpieczeństwa państwa oraz bezpieczeństwa jednostek. Zjawiska te szybko uzyskały miano cyberzagrożeń, a ich swoistość dostrzegana jest zarówno w nauce, jak i w praktyce. Jako cyberzagrożenie wskazuje się zjawisko, w którym za pośrednictwem Internetu lub innych technologii informacyjnych dochodzi do złośliwego ataku na pojedynczą jednostkę lub też organizację¹¹. Może to być zbiór czynności, które zmierzają do przejęcia danych, wyłudzenia pieniędzy lub haseł, a także zniszczenia informacji przechowywanych na dysku komputera. Autorzy aktualnej Strategii Cyberbezpieczeństwa RP cyberzagrożenia określają jako wszelkie potencjalne okoliczności, zdarzenia lub działania, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów teleinformatycznych, użytkowników takich systemów oraz innych osób¹².

M. Górka słusznie jednak zwraca uwagę na brak standardowej definicji cyberzagrożeń. Wielość definicji oraz interpretacji zjawisk mających charakter cybernetyczny powoduje, że trudno przyporządkować określone zdarzenia do opracowanych dużo wcześniej pojęć. Sporym wyzwaniem badawczym jest też zrozumienie, jak zjawiska z obszaru polityki, ekonomii, kultury i psychologii

¹¹ M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015, s. 115 i n.

¹² Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (MP. z 2019 r., poz. 1037).

wzajemnie się krzyżują i jakie mają konsekwencje na funkcjonowanie społeczeństwa¹³.

Cyberprzestrzeń, jako globalna sieć połączonych urządzeń i systemów, jest narażona na szereg różnych rodzajów zagrożeń. Odmienny jest nie tylko ich przedmiot, metody działania, organizacja ataku, zagrożone dobro, konsekwencje, ale również podmioty inicjujący takie ataki. Są wśród nich ataki ukierunkowane na kradzież danych, zablokowanie dostępu do systemów informatycznych, kradzież tożsamości, czy też zniszczenie infrastruktury. Ataki mogą też obejmować próby wyłączenia kluczowych usług: jak sieci energetyczne, systemy wodociągowe, systemy transportowe. Cyberprzestrzeń stała się też nowym polem dla rozwoju przestępczości, zyskującej w ten sposób dodatkowy wymiar. Z kolei państwa i organizacje cyberterrorystyczne wykorzystują cyberprzestrzeń do prowadzenia działań wojennych, szpiegowskich bądź terrorystycznych.

Jednym z najstarszych cyberzagrożeń jest haking, czyli wykorzystanie błędów i luk w zabezpieczeniach komputerowych. Jest to proces zdalnego uzyskiwania nieautoryzowanego dostępu do systemów komputerowych, sieci lub danych. Osoba, która dopuszcza się takiego zachowania, w żaden sposób nie jest upoważniona do uzyskania dostępu do komputera ani do znajdujących się w nim danych. Celem hakingu może być usunięcie bądź kradzież danych, zainfekowanie komputera złośliwym oprogramowaniem, ale także utrudnienie osobie uprawnionej dostępu do danych. Zdarza się, że celem hakera jest również wykorzystanie swoich umiejętności w celu przetestowania i podniesienia sprawności zabezpieczeń systemu komputerowego. Haking jest zagrożeniem o stosunkowo niskim stopniu zorganizowania, najczęściej są to działania pojedynczych osób, przez co znaczenie tego zjawiska pozostaje dość ograniczone¹⁴.

Odmianą hakingu jest hakywizm, polegający na wykorzystaniu komputerów i sieci w celu promowania spraw społecznych i politycznych, takich jak wolność słowa, prawa człowieka i dostęp do informacji. Zjawisko to pojawiało się już w latach 80. XX wieku, choć właściwą formę przybrało dopiero na początku XXI wieku. W 2001 roku opublikowany został *Hacktivism Declaration*¹⁵, będący swoistym kodeksem postępowania opartym na Powszechnej Deklaracji Praw Człowieka. Zaakcentowano w nim znaczenie wolności słowa i informacji, wskazując jednocześnie, że rządy państw w coraz większym stopniu ograniczają je poprzez cenzurę Internetu.

Haktywista działa za pomocą takich samych narzędzi jak haker, jego celem jest jednak zwrócenie uwagi na jakiś cel polityczny lub społeczny. Działalność

¹³ M. Górka, *Współczesne zagrożenia cybernetyczne na przykładzie zjawiska cyberwojny. Analiza teoretyczna*, „Acta Politica Polonica” 2021, nr 1, s. 7.

¹⁴ M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, hakywizm i cyberterroryzm* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009, s. 98–99.

¹⁵ *The Hacktivism Declaration*. cDc communications, http://www.cultdeadcow.com/cDc_files/declaration.html (dostęp: 29.02.2024 r.).

haktywistów „ma na celu nie tyle zniszczenie zasobów przeciwnika, ale przede wszystkim zwrócić uwagę na dany problem”¹⁶. T. Trejderowski zauważa, że są to „działania hakerskie mające podłoże lub cele destrukcyjne, ale nie przynoszące żadnych strat lub przynoszące relatywnie minimalne; można do tej grupy zaliczyć blokowanie stron, podmienianie treści, zamieszczanie własnych apeli itp.”¹⁷.

Haktywiści częściej niż hakerzy działają w grupach, jednak zwykle nie posiadają sformalizowanych struktur, ani ustalonej hierarchii. Wykorzystują różnorodne metody działania, jak blokowanie, modyfikacje lub kradzież danych w formie cyfrowej, stosując techniki DDoS. Na przestrzeni ostatnich lat liczba tego typu ataków znacząco wzrosła. Jedną z najbardziej rozpoznawalnych grup haktywistów jest Anonymus¹⁸.

Coraz poważniejszym zagrożeniem w cyberprzestrzeni staje się dzisiaj cyberprzestępczość. Cyberprzestępczość określana jest jako podkategoria przestępczości komputerowej, obejmująca wszelkie rodzaje przestępstw, do których popełnienia użyto Internetu lub innych sieci komputerowych, przy czym komputery i sieci komputerowe mogą służyć do popełniania przestępstw na kilka sposobów: jako narzędzie przestępstwa, jako cel przestępstwa lub do realizacji innych zadań dodatkowych (np. przechowywania danych uzyskanych w wyniku przestępstwa)¹⁹. Mieszczą się tu zatem wszelkie ataki kierowane przeciwko połączonym systemom komputerowym i mające na celu uniemożliwienie im prawidłowego działania lub przeciwko danym przechowywanym w formie elektronicznej na pojedynczym komputerze bądź też kilku połączonych wspólną siecią. Najbardziej charakterystyczną cechą cyberprzestępczości jest to, że poszczególne czyny mogą być dokonywane za pomocą komputera podłączonego do Internetu lub sieci intranetowych²⁰.

Mianem cyberprzestępczości określa się takie formy posługiwania się sieciami telekomunikacyjnymi, siecią komputerową, Internetem, których celem jest naruszenie jakiegokolwiek dobra chronionego prawem²¹. Cyberprzestępczość odróżnia od klasycznej przestępczości przede wszystkim działanie w środowisku

¹⁶ A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003, s. 60.

¹⁷ T. Trejderowski, *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa 2013, s. 172.

¹⁸ Początki działalności Anonymus sięgają 2006 roku. Jest to globalna, zdecentralizowana grupa aktywistów sprzeciwiająca się ograniczaniu wolności obywatelskich, korupcji, konsumpcjonizmowi, cenzurze, fair use, praktykom Kościoła scjentologicznego oraz łamaniu praw zwierząt. W Polsce Anonymus stali się rozpoznawalni na skutek protestów przeciw ACTA. W 2022 roku, po rozpoczęciu inwazji na Ukrainę grupa wypowiedziała „cyberwojnę” Federacji Rosyjskiej, podejmując działania na szkodę Rosji i rosyjskich firm.

¹⁹ D. Littlejohn Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004, s. 25.

²⁰ D. Skowera, *Akademia Cyberpolicyjna – Policja i organizacje międzynarodowe wobec wyzwań przestępczości internetowej*, „Zarządzanie Publiczne” Zeszyty Naukowe ISP UJ 2006, nr 2, s. 142. Por.: W. Barfield, *Cyber-Humans. Our Future with Machines*, New York 2015, s. 19–21.

²¹ Por.: A. Becla, *Spółczesność informacyjna i społeczeństwo pseudoinformacyjne – problemy pojęciowe i metodyczne identyfikacji*, „Handel Wewnętrzny” 2012, t. 3, s. 151–153.

związanym z technologią komputerową i wykorzystanie sieci komputerowych do popełniania przestępstwa²². Jej wyróżnikiem nie jest natomiast ochrona wspólnego dobra²³. Dzisiaj niemal każda nielegalna działalność ma odzwierciedlenie w Internecie. Jego globalny charakter umożliwił niezwykle szybką komunikację i przeniesienie większości form aktywności człowieka do sieci, także i tych negatywnie odbieranych. Coraz powszechniej mówi się o cyberprzestrzeni jako nowej przestrzeni społecznej, w której występują te same problemy co w świecie rzeczywistym. Cyberprzestępczość jest zatem nowoczesną odmianą przestępczości, wykorzystującą możliwości technik cyfrowych i środowiska sieci komputerowych.

Cyberprzestępczość jest zjawiskiem stosunkowo nowym, rozprzestrzeniającym się w zawrotnym tempie w społeczeństwach dobrze z informatyzowanych i usieciowionych. Stanowi zagrożenie bardzo poważne i trudne do zwalczania. Decydują o tym szczególne właściwości, jakimi cechuje się to zjawisko²⁴. Pierwsza z cech powoduje, że działania cyberprzestępców z łatwością przenikają bariery, jakimi są granice państw. Bardzo często cyberprzestępcy prowadzą swoje działania w jednym miejscu, ich skutki zaś ujawniają się zupełnie gdzie indziej, w miejscu oddalonym o setki kilometrów, nierzadko w innym kraju, na innym kontynencie. Uniemożliwia to określenie systemu prawnego, według którego miałyby następować ściganie takich przestępstw, a jednocześnie znacznie utrudnia wyznaczenie podmiotów odpowiedzialnych za podejmowanie działań ochronnych i zapobiegawczych. Kolejna cecha to anonimowość, która nie ułatwia szybkiego ustalenia sprawców przestępstw oraz wykrycia sposobów ich działania²⁵. Nie jest to jednak niemożliwe, ale wymaga podjęcia żmudnych poszukiwań i wdrożenia dobrze przemyślanych i zaplanowanych działań. Wygoda i szybkość, które zapewnia korzystanie z nowoczesnych technik komputerowych i sieciowych, sprzyjają błyskawicznemu upowszechnianiu tej formy przestępczości w państwach najbardziej rozwiniętych²⁶.

Wszystko to sprawia, że ochrona przed zagrożeniami związanymi z cyberprzestępczością jest niezwykle trudna i wiąże się z podejmowaniem licznych przedsięwzięć, w tym także wymagających wieloaspektowej i szeroko zakrojonej współpracy międzynarodowej. Dla skuteczności tej ochrony niezbędna jest współpraca poszczególnych państw w celu ustalenia wspólnej polityki przeciwdziałania cyberprzestępczości, a następnie jej konkretyzacja przez określenie niezbędnych priorytetów oraz jednolitych zasad wspólnego działania. Tak wyznaczone zasady

²² Zob.: P. Daniluk, *Kultura strategiczna Unii Europejskiej. Podejście normatywne*, „Rocznik Bezpieczeństwa Międzynarodowego” 2015, t. 9(2), s. 14–17.

²³ A. Berlin, L. Brotherson, *Bezpieczeństwo defensywne. Podstawy i najlepsze praktyki*, Gliwice 2018, s. 73.

²⁴ V. Pitts, *Cyber Crimes: History of World's Worst Cyber Attacks*, Marousi 2017, s. 126.

²⁵ Zob.: M. Szczygieł, *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe” 2018, nr 71(2), s. 161.

²⁶ Szerzej: B. Olewiński, *Zadania organów ścigania w zwalczaniu przestępstw przeciwko bezpieczeństwu publicznemu* [w:] *Aktualne zagrożenia i wyzwania w obszarze bezpieczeństwa społecznego i gospodarczego*, red. M. Pomykała, I. Oleksiewicz, Rzeszów 2022, s. 214–215.

ogólne muszą zostać wprowadzone do prawa wewnętrznego państw, stając się podstawą instytucjonalnego i funkcjonalnego systemu instrumentów do walki z cyberprzestępczością. Stworzenie skutecznego systemu przeciwdziałania cyberprzestępczości nie jest proste, wymaga pogłębionej analizy zjawiska w dłuższej perspektywie, a przy tworzeniu takiego systemu mogą wystąpić liczne problemy z dostosowaniem ogólnych wytycznych prawa międzynarodowego bądź unijnego do prawa wewnętrznego poszczególnych państw.

Kolejnym zagrożeniem bezpieczeństwa w cyberprzestrzeni, które dosyć często pojawia się w debatach publicznych, jest cyberterrorizm. Pojęcie to stało się modne, jednak niewiele osób wie, co ono właściwie oznacza. Wielu uważa, że to jedynie teoretyczne pojęcie, działanie, które prawdopodobnie nigdy nie będzie miało miejsca. Jednak nikt nie wie, co przyniesie przyszłość.

Zdefiniowanie cyberterrorizmu jako połączenia cyberprzestrzeni i terroryzmu oznacza, że taka aktywność wiąże się nie tylko z wrogim użyciem IT i działaniem w sferze wirtualnej, ale także cechuje się wszystkimi elementami konstytuującymi aktywność terrorystyczną²⁷. Pojęcie to odnosi się do bezprawnych ataków i zagrożeń wobec komputerów, sieci i informacji przechowywanych w nich, których celem jest zastraszenie lub zmuszenie rządu albo jego ludzi do pewnych działań, aby osiągnąć pewne korzyści polityczne lub społeczne. Ponadto, aby móc zakwalifikować atak jako cyberterrorizm, powinien on być dokonany w wyniku przemocy wobec osób lub mienia lub przynajmniej powodować znaczne szkody, aby wywołać strach. Przykładami takich ataków mogłyby być te, które prowadzą do śmierci lub obrażeń ciała, powodują eksplozje lub straty gospodarcze. D.E. Denning²⁸ twierdzi, że poważne ataki na infrastrukturę krytyczną mogą być również uznane za akty cyberterrorizmu, w zależności od ich wpływu. Z kolei ataki, które zakłócają nieistotne usługi lub są przede wszystkim kosztowne, do nich nie należą.

Należy stwierdzić, że pojęcie „cyberterrorizm” jest używane w kontekście politycznie umotywowanego ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów w szerokim rozumieniu tego słowa²⁹. Przytoczone definicje dowodzą, że to pojęcie³⁰ może być

²⁷ J. Ching, *Cyberterrorism*, New York 2010, s. 56–58.

²⁸ D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, s. 78.

²⁹ Szerzej: Z. Husak, *Ochrona bezpieczeństwa państwa przed zagrożeniami cybernetycznymi w Unii Europejskiej* [w:] *Bezpieczeństwo państwa. Zagadnienia podstawowe*, red. W. Lis, Lublin 2014, s. 54–57.

³⁰ Zdefiniowanie cyberterrorizmu jako połączenia cyberprzestrzeni i terroryzmu oznacza, że taka aktywność wiąże się nie tylko z wrogim użyciem IT i działaniem w sferze wirtualnej, ale także cechuje się wszystkimi elementami konstytuującymi aktywność terrorystyczną. Pojęcie to odnosi się do bezprawnych ataków i zagrożeń wobec komputerów, sieci i informacji przechowywanych w nich celem, których jest zastraszenie lub zmuszenia rządu albo jego ludzi po to, aby osiągnąć pewne korzyści polityczne lub społeczne. Ponadto, aby móc zakwalifikować atak jako cyberterrorizm, powinien on być dokonany w wyniku przemocy wobec osób lub mienia, lub przynajmniej powodować znaczne szkody po to, aby wywołać strach. Jak twierdzi D.E. Denning, za poważne

pojmowane w dwojaki sposób. Według jednej koncepcji od terroryzmu klasycznego odróżnia go jedynie użycie technologii informatycznych w celu przeprowadzenia zamachu, druga koncepcja kładzie nacisk na systemy komputerowe jako cel ataków, a nie narzędzie do ich przeprowadzenia. Wydaje się, że prawdziwa definicja powstaje dopiero po połączeniu obu tych podejść³¹.

Ponieważ zjawisko cyberterroryzmu ma charakter transgraniczny, polityka ochrony cyberprzestrzeni powinna nie tylko zwalczać zagrożenia cyberbezpieczeństwa, ale opierać się na współpracy międzypaństwowej i koordynacji działań, które stanowią nieodzowny element skutecznej odpowiedzi na zagrożenie, jakim jest cyberterroryzm. Złożoność natury tego zjawiska powoduje jednak, że państwa muszą być elastyczne w reakcji na to zjawisko i zdolne do adaptacji zmieniających się warunków. Podjęto próbę wykazania, że pierwszoplanową rolę w skuteczności zwalczania zjawiska cyberterroryzmu odgrywa współpraca na poziomie zarówno państw członkowskich, jak i międzyinstytucjonalnym w poszczególnych państwach. Zostało to udowodnione, ponieważ w analizowanych strategiach państw największy nacisk położono właśnie na współpracę i tworzenie partnerstw publiczno-prywatnych (PPP) oraz reguł usprawniających współpracę międzypaństwową³².

Polityka cyberbezpieczeństwa państwa

Zapewnienie odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni to coraz ważniejsze wyzwanie. We współczesnym świecie, w którym technologia odgrywa coraz większą rolę, cyberbezpieczeństwo systematycznie staje się jednym z kluczowych obszarów bezpieczeństwa państwa. Pojęcie „cyberbezpieczeństwo” w wąskim ujęciu obejmuje jedynie ochronę systemów komputerowych, sieci i danych przed atakami cyfrowymi i tak też zostało ujęte w ustawie z o krajowym systemie cyberbezpieczeństwa z 2018 roku³³. W art. 2 pkt 4 tej ustawy cyberbezpieczeństwo zdefiniowano jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Ustawa wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii³⁴.

ataki na infrastrukturę krytyczną mogą być również uznane za akty cyberterroryzmu, w zależności od ich wpływu. Natomiast ataki, które zakłócające nieistotne usługi lub są przede wszystkim kosztowne do nich nie należą. Zob.: D.E. Denning, *Cyberterrorism*, Global Dialogue, Autumn 2000.

³¹ Por. M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo” 2012, nr 7–8, s. 242.

³² Por. S. Biscop, *The EU Global Strategy 2020*, „Security Policy Brief” 2019, nr 108, s. 3.

³³ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r., poz. 913 ze zm.).

³⁴ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L z 2016 r., nr 194, s. 1).

Warto podkreślić, że cyberbezpieczeństwo jest nie tylko kwestią techniczną, ale także społeczną i ekonomiczną. Cyfryzacja wszystkich obszarów życia współczesnego człowieka, powszechny dostęp do Internetu, nieograniczony zasięg sieci komunikacyjnych sprzyjają bowiem powstawaniu kolejnych form zagrożeń. Są to już nie tylko zagrożenia związane ze złamaniem zabezpieczeń i nieuprawnionym dostępem do danych i informacji, ale także różne działania przestępcze, w tym przestępczość kryminalna, gospodarcza, narkotykowa, pedofilska, a także działania terrorystyczne. Bez odpowiedniej ochrony w tym zakresie, zarówno jednostki, jak i organizacje mogą ponieść poważne straty finansowe i reputacyjne. Pojmowanie cyberbezpieczeństwa jeszcze cały czas ewoluuje, stale się poszerzając, niewątpliwie wymaga ono ciągłego zaangażowania i szczególnej uwagi ze strony wielu podmiotów³⁵.

Ochronie zasobów cyfrowych i unikaniu skutków potencjalnych zagrożeń służy polityka cyberbezpieczeństwa. Definiuje ona sposoby korzystania z kont użytkowników i danych przechowywanych w systemie, zapewniając właściwą ochronę informacji instytucji. W każdej organizacji są informacje chronione, np. dane osobowe, informacje finansowe oraz informacje jawne, w tym informacje marketingowe. Dlatego też przedmiotem polityki bezpieczeństwa państwa jest również informacja znajdująca się w systemie teleinformatycznym. Celem polityki bezpieczeństwa informacyjnego jest opracowanie procedur i wymagań niezbędnych do zapewnienia właściwej ochrony informacji danego państwa czy organizacji międzynarodowej takiej jak Unia Europejska czy NATO. Używając pojęcia polityki cyberbezpieczeństwa, ustala się zbiór praw, reguł i wskazówek praktycznych, które określają takie kwestie, jak zasoby teleinformatyczne, w tym informacje wrażliwe, które są zarządzane, chronione i dystrybuowane w samej organizacji i państwach członkowskich, w ich systemach teleinformatycznych. Ochronie na tym poziomie podlegają:

- zasoby informacji,
- oprogramowanie,
- sprzęt,
- kadry,
- dokumenty³⁶.

W każdej organizacji występują informacje chronione, np. dane osobowe, informacje finansowe oraz informacje jawne, np. informacje marketingowe³⁷. Polityka ochrony cyberprzestrzeni państwa kierowana jest do wszystkich użytkowników cyberprzestrzeni w obrębie danego państwa i poza jego terytorium, w miejscach, gdzie funkcjonują jego przedstawiciele. Jej zadaniem jest zobowiązanie organów administracji rządowej do stworzenia systemu ochrony cyberprzestrzeni

³⁵ E. Żywucka-Kozłowska, R. Dziembowski, *Wokół definicji cyberbezpieczeństwa*, „Cybersecurity and Law” 2023, nr 2(10), s. 125.

³⁶ Por.: wyrok ETS z w sprawie C-176/03 Komisja p. Radzie.

³⁷ Por.: S. Koziej, *Transsektorowy charakter cyberbezpieczeństwa. Strategiczne wyzwania dla Polski i NATO*, Warszawa 2016.

państwa, który będzie szybko reagował i zapobiegał powstaniu cyberataku, a w przypadku dojścia do tego zdarzenia potrafił sprawnie pokonać przeprowadzony atak cybernetyczny.

Polityka cyberbezpieczeństwa państwa³⁸ jest reakcją na zaistniałe zagrożenie, jakim nie jest ochrona jakiegoś wspólnego dobra³⁹. Dzisiaj niemal każda nielegalna działalność ma odzwierciedlenie w Internecie. Globalny charakter Internetu dał natomiast szansę ludziom na zmianę wymiaru komunikacji i aktywności życiowych. Cyberprzestrzeń jest obecnie postrzegana jako przestrzeń polityczno-społeczna, w której odbijają się te same problemy, co w świecie rzeczywistym. Cyberprzestępczość jest również odmianą przestępczości, wykorzystującą możliwości technik cyfrowych i środowiska sieci komputerowych.

Przyczyną powstania polityki cyberbezpieczeństwa jest również brak odpowiednich mechanizmów i regulacji w tym zakresie, dlatego mamy tu do czynienia z procesem instytucjonalizacji. Cyberprzestępczość od klasycznej przestępczości odróżnia przede wszystkim element wirtualności⁴⁰.

Polityka cyberbezpieczeństwa definiuje sposoby korzystania z kont użytkowników i danych przechowywanych w systemie, zapewniając właściwą ochronę informacji instytucji⁴¹. W każdej organizacji występują informacje chronione, np. dane osobowe, informacje finansowe oraz informacje jawne, np. informacje marketingowe⁴². Polityka ochrony cyberprzestrzeni państwa kierowana jest do wszystkich użytkowników cyberprzestrzeni w obrębie danego państwa i poza jego terytorium, w miejscach, gdzie funkcjonują jego przedstawiciele. Jej zadaniem jest zobowiązanie organów administracji rządowej do stworzenia systemu ochrony cyberprzestrzeni państwa, który będzie szybko reagował i zapobiegał powstaniu cyberataku, a w przypadku dojścia do tego zdarzenia potrafił sprawnie pokonać przeprowadzony atak cybernetyczny.

³⁸ Państwa – cyberagresorzy prowadzą zorganizowane działania walki informacyjnej i cyberszpiegostwa. Ocena analizy cyberzagrożeń prowadzonych przez znawców przedmiotu wskazuje, że głównymi państwami przeprowadzającymi ataki w cyberprzestrzeni są: Chiny, Rosja, Stany Zjednoczone, Iran i Korea Północna. Warto zwrócić uwagę, że Izrael, będący strategicznym sojusznikiem USA, wymieniany jest w niej jako strona ofensywna. Strategia Narodowa USA z 12 października 2022 r. (www.whitehouse.gov) (dostęp: 27.02.2024 r.).

³⁹ Por. J. Janowski, *Cybernetyzacja prawa [w:] X-lecie CBKE. Księga pamiątkowa z okazji 10-lecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studentkiego Koła Naukowego*, red. E. Galewska, S. Kotecka, Warszawa 2012, s. 143.

⁴⁰ S. Malešević, *Terrorism. In The Rise of Organised Brutality: A Historical Sociology of Violence*, Cambridge 2017, s. 12–19.

⁴¹ J. Andersson et. al., *Envisioning European Defence: Five Futures*, „Chaillot Paper” 2017, nr 137, s. 122.

⁴² Por.: orzeczenie Sądu Okręgowego w Paryżu z 20 października 2000 roku w sprawie Anit-Semism LICRA v. Yahoo Inc., sygn. akt RG 00/05308.

Wnioski końcowe

Cyberbezpieczeństwo staje się coraz istotniejszym elementem współczesnego bezpieczeństwa państwa. Choć jeszcze nie tak dawno był to marginalny i mocno wyspecjalizowany obszar bezpieczeństwa, dziś w zawrotnym tempie przesuwa się na pierwszy plan. Technologia cyfrowa zdominowała już funkcjonowanie gospodarki i społeczeństwa. Internet, komputery, smartfony, chmura obliczeniowa i sztuczna inteligencja to dzisiaj niezbędne narzędzia do prowadzenia działalności gospodarczej, wzajemnego komunikowania się, edukacji, zapewnienia opieki zdrowotnej, a nawet prowadzenia działań obronnych. Narzędzia cyfrowe wykorzystywane są przez wszystkie podmioty, poczynając od pojedynczych obywateli, przez przedsiębiorców, instytucje publiczne, a nawet państwa.

Wraz z poszerzaniem się obszarów, w których wykorzystywane są zaawansowane narzędzia informatyczne, zwiększa się także różnorodność i złożoność cyberataków, które jednocześnie stają się coraz powszechniejsze i wykorzystują coraz bardziej zaawansowane narzędzia informatyczne. Za pomocą cyberataków realizowane są też różne cele, jak uszkodzenia lub zniszczenia systemów informatycznych, uszkodzenie i wyłączenie kluczowych elementów infrastruktury krytycznej, kradzieże danych, wywoływanie paniki i chaosu, dezinformacja, pozyskiwanie informacji o planach strategicznych przeciwnika. Obrona przed takimi atakami staje się więc coraz bardziej wymagająca, musi uwzględniać zmieniające się warunki i stałą ewolucję zagrożeń. Z pewnością również te stale ewoluujące zagrożenia w cyberprzestrzeni wymagają ciągłego monitorowania i prowadzenia przemyślanej polityki.

Rozwój cybertechnologii w istotny sposób zmienił zasady prowadzenia polityki państwa. Internet stał się nową areną działania oraz przekazu informacji. Jednym z wyzwań dla współczesnego państwa jest duża dynamika tych zdarzeń i konieczność szybkiego reagowania na nie. Nastąpiła swoista decentralizacja komunikacji, a dzięki sieciom komunikacyjnym każdy może dziś rozpowszechnić wszelkie przekazy z pominięciem oficjalnych kanałów informacji. Oznacza to, że opinia publiczna, kształtowana w dużym stopniu dzięki Internetowi, ma znacznie większy wpływ na politykę państwa. Z drugiej zaś strony instytucje publiczne muszą być w coraz większym stopniu obecne w cyberprzestrzeni.

Słusznie stwierdzają E. Żywucka-Kozłowska i R. Dziembowski, że cyberbezpieczeństwo ma uniwersalny charakter, a ta uniwersalność oznacza „obejmujące całość», a cyberprzestrzeń tym właśnie się wyróżnia”⁴³. Współczesne społeczeństwo z powodzeniem przenosi wszelką swoją aktywność do wirtualnej rzeczywistości – cyberprzestrzeni, gdzie nie ma granic, gdzie informacje przepływają swobodnie, bez względu na położenie geograficzne. Ataki w cyberprzestrzeni bardzo często przybierają dziś międzynarodowy charakter. Problem zapewnienia właściwego i bezpiecznego funkcjonowania w tej rzeczywistości nie dotyczy zatem tylko

⁴³ E. Żywucka-Kozłowska, R. Dziembowski, *Wokół definicji cyberbezpieczeństwa...*, *op.cit.*, s. 130–131.

jednego państwa, należy go postrzegać jako problem globalny, który wymaga szeroko zakrojonej współpracy. Państwa zmuszone są więc tworzyć wspólne ramy prawne, współpracować ze sobą na wielu obszarach, aby chronić interesy swoje i swoich obywateli. Aby jednak działania te były efektywne i skuteczne ogromne znaczenia ma trafne prognozowanie przyszłych zagrożeń oraz zaproponowanie odpowiadających im metod i środków działania w ramach globalnych, regionalnych i krajowych polityk bezpieczeństwa.

II. Zwalczanie cyberprzestępczości

PRZESTĘPSTWA Z USTAWY O ZWALCZANIU NADUŻYĆ W KOMUNIKACJI ELEKTRONICZNEJ

Elektroniczna komunikacja (e-komunikacja) to różne rodzaje połączeń przy użyciu środków elektronicznych i związanych z tym technologii (poczta elektroniczna, media społecznościowe, czaty/fora internetowe, krótkie wiadomości tekstowe, wiadomości multimedialne, wideokonferencje itp.).

Według definicji legalnej²: środki komunikacji elektronicznej to rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną.

Elektroniczna komunikacja cechuje się przede wszystkim szybkością i efektywnością. Jest nieodłączną częścią naszego życia. Niestety, oprócz licznych zalet, w związku z elektronicznym komunikowaniem się, coraz częściej mamy do czynienia z nieprawidłowościami, polegającymi głównie na różnego rodzaju nadużyciach.

W dniu 28 lipca 2023 roku uchwalono ustawę o zwalczaniu nadużyć w komunikacji elektronicznej³. Ustawa, w zakresie swojej regulacji, wdrożyła

¹ Politechnika Rzeszowska im. Ignacego Łukasiewicza. ORCID: 0000-0002-6069-3115.

² Art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tj. Dz.U. z 2020 r., poz. 355).

³ Ustawa z dnia 28 lipca 2023 r. (Dz.U. z 2023 r., poz. 1703). Ustawa wchodzi w życie po upływie 30 dni od dnia ogłoszenia, z wyjątkiem:

- 1) art. 2 pkt 1, 6 i 13, art. 20–22 oraz art. 39, które wchodzi w życie z dniem następującym po dniu ogłoszenia;
- 2) art. 23, który wchodzi w życie z dniem 1 listopada 2023 r.;
- 3) art. 17, art. 18 oraz art. 27 ust. 3 pkt 1 i 5, które wchodzi w życie po upływie 6 miesięcy od dnia wejścia w życie ustawy;
- 4) art. 27 ust. 3 pkt 4, który wchodzi w życie po upływie 12 miesięcy od dnia wejścia w życie ustawy.

Jeżeli w niniejszym rozdziale następuje odwołanie do „ustawy” bez jej określenia, chodzi o ustawę z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

Niniejsza ustawa została notyfikowana Komisji Europejskiej w dniu 23 lutego 2023 r. pod numerem 2023/083/PL, zgodnie z § 4 rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz.U. poz. 2039 oraz Dz.U. z 2004 r. poz. 597), które wdraża postanowienia dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 roku ustanawiającej procedurę udzielania

dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 roku ustanawiającą Europejski kodeks łączności elektronicznej⁴. Uważa się, że to krok milowy w zakresie naszego bezpieczeństwa w komunikacji elektronicznej⁵.

W uzasadnieniu do projektu ustawy podniesiono, że komunikacja elektroniczna stanowi narzędzie powszechnie wykorzystywane w życiu codziennym przez współczesne społeczeństwo informacyjne. Z usług dostarczanych przez przedsiębiorców telekomunikacyjnych codziennie korzysta wiele milionów osób. Usługi te są również coraz szerzej i w sposób bardziej wyszukany wykorzystywane przez przestępców w celu wyrządzenia szkód po stronie przedsiębiorców telekomunikacyjnych, użytkowników końcowych lub osiągnięcia nienależnych korzyści. W ostatnim czasie nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych. Przestępcy, stosując specjalne bramki internetowe, podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwoniли z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania bądź w niektórych przypadkach próbowali nawet ich zastraszyć. Innym zagrożeniem dla użytkowników są fałszywe krótkie wiadomości tekstowe (SMS).

Oszuści, podszywając się pod zaufane instytucje, próbują nakłonić nieświadome ofiary do ujawnienia danych osobowych, informacji o karcie kredytowej czy zainfekować urządzenie przez kliknięcie w link w wiadomości. W tej sytuacji konieczne było wprowadzenie odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. W ramach dotychczasowych przepisów nie było możliwości skutecznego przeciwdziałania tym nadużyciom. Proponowane rozwiązania miały służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolą w większym stopniu niż obecnie ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników.

Projekt ustawy miał na celu wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE), zgodnie z którą organy mogą wymagać od podmiotów udostępniających publicznie sieci łączności elektronicznej lub świadczących publicznie dostępne usługi łączności elektronicznej, zablokowania w indywidualnych przypadkach dostępu do numerów lub usług, gdy jest to uzasadnione ze względu na oszustwo lub nadużycie. Szybki wzrost liczby tego typu przestępstw oraz fakt, że regulowana materia znajduje się na styku dziedziny prawa telekomunikacyjnego

informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego (Dz. Urz. UE L 241 z 17.09.2015 r., s. 1).

⁴ Dz. Urz. UE L 321 z 17.12.2018 r., s. 36; Dz. Urz. UE L 334 z 27.12.2019 r., s. 164 oraz Dz. Urz. UE L 419 z 11.12.2020 r., s. 36.

⁵ <https://www.gov.pl/web/cyfryzacja/ustawa-o-zwalczaniu-naduzy-c-w-komunikacji-elektronicznej-juz-niedlugo-wejdzie-w-zycie--sprawdz-korzysci-jakie-niesie-to-dla-ciebie-i-twoich-bliskich> (dostęp: 12.11.2023 r.).

i wyodrębniającego się materialnego prawa administracyjnego z zakresu cyberbezpieczeństwa sprawia, że konieczne stało się ujęcie tego zagadnienia w odrębnej ustawie⁶.

Zakłada się, że wejście w życie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej przełoży się bezpośrednio na nasze bezpieczeństwo. Dzięki tym regulacjom ma zmniejszyć się liczba fałszywych połączeń, SMS-ów oraz domen internetowych. Blokada na poziomie państwowym będzie chroniła nas wszystkich, a w szczególności dzieci i seniorów, którzy nie zawsze potrafią rozpoznać zagrożenie. – „To dobry dzień dla użytkowników nowych technologii, a zły dla oszustów” – mówił minister cyfryzacji Janusz Cieszyński. Dzięki współpracy Naukowej i Akademickiej Sieci Komputerowej, Urzędu Komunikacji Elektronicznej oraz Centralnego Biura Zwalczania Cyberprzestępczości wzrasta skuteczność ochrony Polaków przed utratą pieniędzy i danych osobowych. „Zaproponowane rozwiązania skutecznie ograniczą podszywanie się pod instytucje zaufania publicznego”. Dlaczego to takie ważne? Bo ostatnie lata przyniosły gwałtowny wzrost oszustw elektronicznych. Według danych Krajowego Systemu Informacyjnego Policji szacunkowa wartość strat materialnych spowodowanych przez oszustwa związane z e-bankowością i phishingiem w 2022 roku wyniosła ponad 124 miliony złotych⁷.

Blisko 11 000 zł średnio straciła każda z ofiar w przypadku postępowań dotyczących oszustw z wykorzystaniem wiadomości SMS, prowadzonych w 2023 roku przez Centralne Biuro Zwalczania Cyberprzestępczości. Aż 217 685 podejrzanych wiadomości SMS zgłoszono do CERT Polska w 2022 roku (2023 rok, do października: 116 149). 82 499 wiadomości SMS zgłoszonych do CERT Polska zawierało link przenoszący na niebezpieczną stronę internetową (2023 rok, do października: 55 313). Około 25% zgłoszeń zarejestrowanych w 2022 roku przez CERT Polska dotyczyło różnych odmian phishingu, najwięcej spośród wszystkich odmian zgłaszanych zagrożeń. Odsetek ataków phishingowych wśród wszystkich incydentów bezpieczeństwa obsługanych przez CERT Polska w 2022 roku wyniósł 64%⁸.

W ustawie z dnia 28 lipca 2023 roku został określony cel i charakter podejmowanych działań, które mają zwalczać nadużycia w komunikacji elektronicznej. Zdefiniowane zostały także niektóre pojęcia.

Nadużycie w komunikacji elektronicznej to świadczenie lub korzystanie z usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa. Jest to celowe działanie,

⁶ Z uzasadnienia do projektu ustawy – wnioskodawca Rada Ministrów, Sejm RP IX kadencji, druk nr 3069.

⁷ <https://www.gov.pl/web/cyfryzacja/ustawa-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej-juz-niedlugo-wejdzie-w-zycie--sprawdz-korzysci-jakie-niesie-to-dla-ciebie-i-twoich-bliskich> (dostęp: 12.11.2023 r.).

⁸ Zob. <https://e-prawnik.pl/informacje/ustawa-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej.html> (dostęp: 17.12.2023 r.).

wskutek którego dochodzi do wyrządzenia szkody przedsiębiorcy telekomunikacyjnemu lub użytkownikowi końcowemu. W wyniku tego działania może dojść do uzyskania korzyści przez podmiot dopuszczający się nadużyć. Wejście w życie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej ma za zadanie skutecznie ograniczyć tego typu oszustwa⁹.

Celem przeciwdziałania nadużyciom w komunikacji elektronicznej uznano za konieczne posłużenie się między innymi przepisami karnymi. Normy takie mają za zadanie spowodować, by ich adresaci postępowali zgodnie z nakazami wynikającymi z danej normy. Ponieważ prawo karne uznaje się za swoiste *ultima ratio*, świadczy to o wadze, jaką ustawodawca przywiązuje do zwalczania niektórych nadużyć w komunikacji elektronicznej. Istnieją, już wcześniej wprowadzone w życie, przepisy karne chroniące komunikację elektroniczną, m.in.: art. 190a k.k.¹⁰, art. 287 k.k.¹¹, art. 107a k.w.¹².

W art. 29–32 ustawy z dnia 28 lipca 2023 roku sformułowano cztery nowe typy przestępstw: generowanie sztucznego ruchu, smishing (połączenia słów SMS i phishing), CLI (*calling line identification*), spoofing (naciąganie, szachrajstwo), modyfikacja informacji adresowej.

⁹ <https://www.ifirma.pl/blog/zwalczanie-naduzyc-w-komunikacji-elektronicznej-zmiany-2023.html> (dostęp: 12.11.2023 r.).

¹⁰ Art. 190a ustawy z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2022 r., poz. 1138) (Uporczywe nękanie. Kradzież tożsamości).

§ 1. Kto przez uporczywe nękanie innej osoby lub osoby dla niej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, przez co wyrządza jej szkodę majątkową lub osobistą.

§ 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 15.

§ 4. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

¹¹ Art. 287 k.k. (Oszustwo komputerowe)

§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

§ 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

¹² Art. 107a ustawy z dnia 20 maja 1971 r. Kodeks wykroczeń (t.j. Dz.U. z 2023 r., poz. 2119) (Zakłócanie przebiegu zdalnej komunikacji prowadzonej za pomocą systemów teleinformatycznych).

§ 1. Kto, włączając się bez uprawnienia w transmisję danych prowadzoną przy użyciu systemu teleinformatycznego, umyślnie udaremnia lub utrudnia użytkownikowi tego systemu przekazywanie lub odbiór informacji, podlega karze ograniczenia wolności albo grzywny nie niższej niż 1000 złotych.

§ 2. Jeżeli sprawca czynu określonego w § 1 używa słów powszechnie uznanych za obelżywe lub w inny sposób dopuszcza się nieobyczajnego wybryku, podlega karze aresztu, ograniczenia wolności albo karze grzywny nie niższej niż 3000 złotych.

Sankcja za generowanie sztucznego ruchu (*Artificial Traffic Generating*) – art. 29 ustawy:

1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody wysyła lub odbiera komunikaty lub połączenia głosowe w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych lub przez systemy rozliczeniowe – podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Według definicji ustawowej *generowanie sztucznego ruchu* to wysyłanie lub odbieranie komunikatów lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych lub przez systemy rozliczeniowe (art. 3 ust. 1 pkt 1 ustawy).

Sankcja za *smishing* (art. 30 ustawy):

1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody wysyła krótką wiadomość tekstową (SMS), wiadomość multimedialną (MMS) lub wiadomość za pośrednictwem innych usług komunikacji interpersonalnej, w której podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego, instalacji oprogramowania, przekazania haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej – podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
3. Jeżeli czyn, o którym mowa w ust. 1, popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Według definicji ustawowej *smishing* to wysłanie krótkiej wiadomości tekstowej (SMS), w której nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego zachowania, w szczególności przekazania danych osobowych, niekorzystnego rozporządzenia mieniem, otwarcia strony internetowej, inicjowania połączenia głosowego lub instalacji oprogramowania (art. 3 ust. 1 pkt 2 ustawy).

Sankcja za CLI (*calling line identification*) spoofing (art. 31 ustawy):

1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody, przy wywoływaniu połączenia głosowego

posługuje się, nie będąc do tego uprawnionym, informacją adresową wskazującą na inną osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, aby podszyć się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania, przekazania haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej – podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
3. Jeżeli czyn, o którym mowa w ust. 1, popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Według definicji ustawowej CLI spoofing to nieuprawnione posłużenie się lub korzystanie przez użytkownika lub przedsiębiorcę telekomunikacyjnego wywołującego połączenie głosowe informacją adresową wskazującą na osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej inną niż ten użytkownik lub przedsiębiorca telekomunikacyjny, służące podszyciu się pod inny podmiot, w szczególności w celu wywołania strachu, poczucia zagrożenia lub nakłonienia odbiorcy tego połączenia do określonego zachowania, zwłaszcza do przekazania danych osobowych, niekorzystnego rozporządzenia mieniem lub instalacji oprogramowania (art. 3 ust. 1 pkt 3 ustawy).

Sankcja za *niezgodną z prawem modyfikację informacji adresowej* (art. 32 ustawy):

1. Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej lub wyrządzenia innej osobie szkody dokonuje niezgodnej z prawem modyfikacji informacji adresowej uniemożliwiającej albo istotnie utrudniającej ustalenie, przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu, informacji adresowej użytkownika wysyłającego komunikat - podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.

Według definicji ustawowej *nieuprawniona zmiana informacji adresowej* to niezgodne z prawem modyfikowanie informacji adresowej uniemożliwiające albo istotnie utrudniające ustalenie, przez uprawnione podmioty lub przedsiębiorców telekomunikacyjnych uczestniczących w dostarczeniu komunikatu, informacji adresowej użytkownika wysyłającego komunikat (art. 3 ust. 1 pkt 4 ustawy).

Stroną przedmiotową tych przestępstw jest dopuszczanie się sztucznego ruchu, smishingu, CLI spoofingu lub nieuprawnionej modyfikacji informacji adresowej. Przepisem tym wprowadza się penalizację ww. nadużyć w komunikacji elektronicznej. Jednocześnie wprowadza się typ uprzywilejowany tego prze-

stępstwa: w wypadku mniejszej wagi. Jeżeli nadużycia w komunikacji elektronicznej dokonano na szkodę osoby najbliższej, ściganie będzie następować na wniosek pokrzywdzonego. Do tej pory czyny te mogły być kwalifikowane w oparciu o kodeks karny – przykładowo spoofing był kwalifikowany jako czyn określony w art. 190a k.k. Wyodrębnienie tych czynów do odrębnego przepisu ma umożliwić prowadzenie statystyk występowania tych przestępstw¹³, a co za tym idzie, umożliwi zmierzenie skuteczności działań państwa w zwalczaniu tego rodzaju czynów¹⁴.

Przedmiotem ochrony (przedmiotem zamachu), czyli wartości chronionej przez normę prawa karnego jest mienie, bezpieczeństwo informacji oraz systemów informatycznych, teleinformatycznych lub sieci teleinformatycznej. Mieniem w rozumieniu prawa karnego są prawa majątkowe do określonej rzeczy, w tym również stan faktyczny, jakim jest władanie określoną rzeczą. Zakres ochrony zależy od znamion określonych przestępstw¹⁵.

Dane informatyczne to zapisy na komputerowych nośnikach informacji. Definicję legalną danych informatycznych zawiera art. 1 lit. b konwencji o cyberprzestępczości¹⁶. Jest to dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny.

Każdy czyn zabroniony winien wskazywać kto może być jego sprawcą (podmiot czynu zabronionego) Przestępstwa opisane w ustawie mają charakter powszechny, bowiem ich podmiotem może być każdy.

Analizując stronę podmiotową uznać należy, że przestępstwa z ustawy mają charakter umyślny¹⁷. Można je popełnić tylko w zamiarze bezpośrednim (*dolus directus*) o szczególnym zabarwieniu. Świadczy o tym sformułowanie: „Kto w celu osiągnięcia korzyści majątkowej, korzyści osobistej...”. Sprawca musi działać w takim właśnie celu.

Przepisy art. 29 ust. 2, 30 ust. 2, 31 ust. 2 i 32 ust. 2 ustawy określają typy uprzywilejowane zawartych w nich przestępstw (wypadki mniejszej wagi)¹⁸. Ustawodawca zamieścił więc wypadki mniejszej wagi bezpośrednio w treści przepisów określających dany występki, co jest rozwiązaniem słusznym. Ustawy, zwłaszcza kodeks karny nie zawierają definicji wypadku mniejszej wagi.

¹³ Uzasadnienie wprowadzenia nowych typów przestępstw względami statystycznymi, jest co najmniej dziwne.

¹⁴ Z uzasadnienia do projektu ustawy.

¹⁵ T. Tyburcy, *Mienie jako przedmiot ochrony w prawie karnym (na wybranych przykładach)*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2018, R. XXII, z. 3, s. 91.

¹⁶ Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie dnia 23 listopada 2001 roku (Dz.U. z 2015 r., poz. 728).

¹⁷ Używany czasami zwrot: przestępstwo popełnione „z winy umyślnej” jest niepoprawny. To czyn zabroniony może być popełniony umyślnie bądź nieumyślnie.

¹⁸ Występują także poglądy, które traktują wypadek mniejszej wagi jako regułę dotyczącą wymiaru kary nie zaś uprzywilejowany typ przestępstwa (zob. K. Buchała, *Glosa do wyroku Sądu Najwyższego z dnia 9.10.1996 r.*, sygn. akt VKKN 79/96, „Państwo i Prawo” 1999 r., nr 9, s. 111 i n.)

„Przez wypadek mniejszej wagi uznaje się w praktyce te odmiany czynów typu podstawowego, w których stopień społecznej szkodliwości oraz wina sprawcy są znacznie niższe niż w przypadku typu podstawowego, a nie są jeszcze subminimalne, jak w razie znikomości tych znamion, zupełnie odejmującej czynowi charakter przestępczy. Wypadek mniejszej wagi jest stanem pośrednim między brakiem treści materialnej przestępstwa a stanem uznawanym za przestępstwo typu podstawowego. Za wypadki mniejszej wagi uznaje się więc takie zachowania, wyczerpujące znamiona formalne, gdy szkoda wyrządzona lub zamierzona jest niewielka, sprawca działa z niewielką winą, nagle, bez zastanowienia, czasem motywowany wyzywającym zachowaniem pokrzywdzonego. Niektórzy dodają warunek, by poprzednie życie sprawcy bądź jego zachowanie po popełnieniu przestępstwa świadczyły, że przestępstwo było w jego życiu incydentem odbiegającym od linii jego życia¹⁹”. O przyjęciu wypadku mniejszej wagi decydują więc przedmiotowe i podmiotowe znamiona czynu. Odnosić się to będzie przede wszystkim do przestępców działających z przypadku. Grozić im będzie niższa kara, a także możliwość orzeczenia grzywny albo kary ograniczenia wolności zamiast kary pozbawienia wolności (art. 37a k.k.).

Jednym z kryteriów dzielenia czynów zabronionych jest sposób ich ścigania (tryb ścigania). Przestępstwa określone w art. 29 i 32 ścigane są z oskarżenia publicznego, z urzędu przez prokuratora (zob. ust. 3 tych przepisów). Obowiązuje tu zasada legalizmu wynikająca z przepisu art. 10 § 1 k.p.k.²⁰.

Przestępstwa opisane w art. 30 i 31 ustawy, jeśli zostały popełnione na szkodę osoby najbliższej, ścigane są na wniosek pokrzywdzonego. W sprawach o przestępstwa ścigane na wniosek postępowanie z chwilą złożenia wniosku toczy się z urzędu. Organ ścigania poucza osobę uprawnioną do złożenia wniosku o przysługującym jej uprawnieniu. Uzyskanie wniosku o ściganie należy do oskarżyciela. Jeżeli powodem uzyskania wniosku jest wyłącznie uprzedzenie przez sąd stron o możliwości zakwalifikowania czynu według innego przepisu prawnego, przewidującego ściganie na wniosek, uzyskanie wniosku o ściganie należy do sądu. W razie złożenia wniosku o ściganie niektórych tylko sprawców obowiązek ścigania obejmuje również inne osoby, których czyny pozostają w ścisłym związku z czynem osoby wskazanej we wniosku, o czym należy uprzedzić składającego wniosek. Przepisu tego nie stosuje się do najbliższych osoby składającej wniosek. Wniosek może być cofnięty w postępowaniu przygotowawczym za zgodą prokuratora, a w postępowaniu sądowym za zgodą sądu – aż do zamknięcia przewodu sądowego na pierwszej rozprawie głównej. W sprawach, w których akt oskarżenia wniósł oskarżyciel publiczny, cofnięcie wniosku po rozpoczęciu przewodu sądowego jest skuteczne, jeżeli nie sprzeciwi się temu oskarżyciel publiczny obecny na rozprawie lub posiedzeniu. Ponowne złożenie wniosku jest niedopuszczalne (art. 12 k.p.k.).

¹⁹ Por. wyrok SA w Krakowie z dnia 5 czerwca 2002 r., sygn. akt II AKa 128/02, KZS 2002, nr 6, poz. 16, LEX nr 56953.

²⁰ Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz.U. z 2022 r., poz. 1375).

Osobą najbliższą jest małżonek, wstępny, zstępny, rodzeństwo, powinowaty w tej samej linii lub stopniu, osoba pozostająca w stosunku przysposobienia oraz jej małżonek, a także osoba pozostająca we wspólnym pożyciu (art. 115 § 11 k.k.).

Pokrzywdzonym jest osoba fizyczna lub prawna, której dobro prawne zostało bezpośrednio naruszone lub zagrożone przez przestępstwo. Pokrzywdzonym może być także niemająca osobowości prawnej: 1) instytucja państwowa lub samorządowa; 2) inna jednostka organizacyjna, której odrębne przepisy przyznają zdolność prawną. Za pokrzywdzonego uważa się zakład ubezpieczeń w zakresie, w jakim pokrył szkodę wyrządzoną pokrzywdzonemu przez przestępstwo lub jest zobowiązany do jej pokrycia. W sprawach o przestępstwa, którymi wyrządzono szkodę w mieniu instytucji lub jednostki organizacyjnej, jeżeli nie działa organ pokrzywdzonej instytucji lub jednostki organizacyjnej, prawa pokrzywdzonego mogą wykonywać organy kontroli państwowej, które w zakresie swojego działania ujawniły przestępstwo lub wystąpiły o wszczęcie postępowania (art. 49 k.p.k.).

Podsumowując – wprowadzenie nowych typów przestępstw wydaje się zasadne i winno nadążać za stałym postępem w dziedzinie elektronicznej komunikacji oraz związanymi z tym nadużyciami. Są to jednak typy przestępstw pozakodeksowych, co jest wyrazem ciągłego marginalizowania kodeksu karnego, jako podstawowego aktu prawnego z zakresu prawa karnego materialnego. Ze względu na charakter przedstawionych nowych typów przestępstw niezbędne jest, w ramach podejmowanych czynności, przede wszystkim zabezpieczenie (zatrzymanie), na potrzeby późniejszego postępowania sądowego, dowodów elektronicznych przed ich utratą, zniszczeniem lub zniekształceniem²¹. Musi to oczywiście nastąpić w jak najwcześniejszych fazach postępowania.

²¹ Zob. A. Kiełtyka, *Zatrzymanie rzeczy* [w:] *Prawo karne procesowe dla sędziów, prokuratorów, obrońców i pełnomocników. Praxis*, red. M. Olęzałek, Warszawa 2024, s. 974 i n.

III.
Problemy cyberbezpieczeństwa
w obszarze ochrony
danych osobowych i informacji

NARUSZENIE OCHRONY DANYCH OSOBOWYCH JAKO INCYDENT BEZPIECZEŃSTWA INFORMACJI – WYBRANE ASPEKTY PRAWNE I PRAKTYCZNE

Wprowadzenie

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO), funkcjonujące w europejskim porządku prawnym przeszło 5 lat wprowadziło pojęcie „naruszenia ochrony danych osobowych”².

W stanie prawnym poprzedzającym wejście w życie RODO pojęcie to nie miało legalnej definicji, pomimo że naruszenie ochrony danych osobowych jest niezwykle istotne nie tylko z punktu widzenia osoby, której dane zostały ujawnione, zniszczone, bezprawnie pozyskane, ale także z punktu widzenia administratora danych, na którego rozporządzenie nakłada szereg obowiązków w zakresie zapewnienia bezpieczeństwa danym osobowym. W zbliżonym obszarze rozważań pozostają pojęcia „bezpieczeństwo informacji” oraz „incydenty bezpieczeństwa” rozumiane jako niepożądane sytuacje zagrażające bądź zakłócające ten stan. Czym jest incydent bezpieczeństwa, a czym naruszenie ochrony informacji (danych osobowych)? Jakie są wzajemne relacje tych pojęć i skutki prawne ich wystąpienia? Czy naruszenie ochrony danych osobowych jest incydem bezpieczeństwa informacji? Czy odwrotnie rzecz ujmując każdy incydent bezpieczeństwa danych stanowi naruszenie ochrony danych osobowych, definiowane przez RODO, czy też są to pojęcia niezależnie funkcjonujące w obrocie prawnym, wywołujące określone konsekwencje prawne i faktyczne?

Zagadnienia wywołane tak postawionymi pytaniami będą właśnie przedmiotem niniejszego opracowania.

¹ Politechnika Rzeszowska im. Ignacego Łukasiewicza. ORCID: 0000-0001-5572-8291.

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (RODO) (Dz. Urz. UE. L z 4 maja 2016 r., nr 119), s. 1.

Istota bezpieczeństwa informacji z perspektywy ochrony danych osobowych

Pojęcie i znaczenie informacji w definiowaniu danych osobowych

Rozważania na temat „bezpieczeństwa informacji” należałoby rozpocząć od przybliżenia pojęcia „informacja” i określenia jego znaczenia dla współczesnego świata. Słowo to wywodzi się z języka łacińskiego, gdzie *informatio* oznacza wyobrażenie, przedstawienie, wizerunek, zarys, pojęcie, a czasownik *in formare* rozumieć należy jako kształtowanie, urabianie, czy też odciskanie formy. Informacja to pojęcie przejawiające się w wielu dziedzinach nauki, w tym w naukach prawnych, ekonomicznych, społecznych, a współcześnie w naukach związanych z cybernetyką. Znaczenie informacji dla człowieka jako jednostki, dla społeczeństwa, instytucji, organizacji czy w końcu dla państwa spowodowało, że stała się ona najbardziej poszukiwanym zasobem w dzisiejszych czasach³. Pomimo tego brak jest legalnej definicji informacji, a stworzenie uniwersalnej, interdyscyplinarnej definicji tego pojęcia stało się niemożliwe wobec różnorodności dziedzin życia i nauki, w których występuje.

Informacja jest niewątpliwie dobrem prawnym, o czym świadczy przyznanie samodzielnej ochrony prawnej niektórym kategoriom informacji⁴. Na użytek rozważań na temat korelacji „bezpieczeństwa informacji” i ochrony danych osobowych warto przytoczyć kilka wybranych definicji informacji, pojawiających się w różnych obszarach nauki. I tak oto P. Sienkiewicz przyjmuje, że: „Informacja to zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów, systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne”⁵. M. Maciejowski, powracając do słownikowego znaczenia informacji określił ją jako „utrwalony w dowolny sposób (także w pamięci człowieka) komunikat (wiedza, świadomość) o jakimś fakcie”⁶. Do tak definiowanej informacji należy odnieść pojęcie „danych osobowych”, które według ustawodawcy europejskiego „oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników

³ J. Łuczak, M. Tyburski, *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2009, s. 7.

⁴ J. Taczkowska-Olszewska, *Dostęp do informacji publicznej w polskim systemie prawnym*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 1.

⁵ Za P. Sienkiewicz, *Ewaluacja informacji w społeczeństwie informacyjnym*, „Ekonomiczne Problemy Usług” 2011, nr 67, s. 127.

⁶ M. Maciejowski: *Prawo informacji – zagadnienia podstawowe* [w:] *Prawo informacji. Prawo do informacji*, red. W. Góralczyk jun., Warszawa 2006, s. 31.

określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej” – art. 4 pkt 1 RODO. „Na gruncie przepisów o ochronie danych osobowych przyjmuje się, że pojęcie informacji oznacza komunikaty (wiadomości, wypowiedzi, prezentacje) wyrażone i zapisane w jakikolwiek sposób: znakami graficznymi, symbolami, w języku komputerowym, na fotografii na taśmie magnetofonowej lub magnetowidowej itd., niezależnie od sposobu, zakresu i swobody ich udostępniania, jak też niezależnie od sposobu ich pozyskania⁷.

Dane osobowe stanowią dobro prawem chronione, co oznacza, że naruszenie tego dobra wywołuje określone skutki prawne. Ochrona prawna informacji dotyczących osób fizycznych zyskała wymiar konstytucyjny. Informacje stanowiące dane osobowe wchodzą w zakres prawa do prywatności, prawa przysługującego każdej osobie fizycznej, a gwarancją tej ochrony jest art. 47 Konstytucji RP z 2 kwietnia 1997 roku „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.”. W artykule 51 Konstytucji ochrona informacji pojawia się jako substrat uregulowanej prawnie prywatności każdego z nas. Zapisy wyrażone w pięciu kolejnych punktach wyrażają nasze prawo do samo decydowania o informacjach na nasz temat, a możliwe ograniczenia w tym zakresie muszą mieć charakter ustawowy. Demokratyczny porządek prawny wskazuje władzy publicznej granice pozyskiwania, gromadzenia i udostępniania informacji osobowych. 1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. 2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. 3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa. 4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. 5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa⁸.

Aspekty prawne bezpieczeństwa informacji oraz bezpieczeństwa danych osobowych i ochrony danych osobowych

Skoro informacja stała się najbardziej pożądanym zasobem nie tylko dla jednostki, społeczeństwa, organizacji, ale i państwa, to zrozumiałe jest to, że

⁷ P. Fajgielski [w:] *Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* [w:] *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, wyd. II, Warszawa 2022, art. 4, <https://sip.lex.pl/#/commentary/587773148/670976/fajgielski-pawel-komentarz-do-rozporzadzenia-nr-2016-679-w-sprawie-ochrony-osob-fizycznych-w...?cm=URELATIONS> (dostęp: 7.01.2024 r.).

⁸ Por. M. Jurgilewicz, E. Kosior, *Ochrona danych osobowych a bezpieczeństwo wewnętrzne państwa* [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Wydawnictwo UPH w Siedlcach, Siedlce 2019, s. 133–146.

bezpieczeństwo informacji i ochrona informacji zyskały szczególny wymiar. Bezpieczeństwo informacji to stosunkowo nowo definiowane pojęcie, z obszaru prawa, techniki i nauki o organizacji, które pojawia się w normach technicznych z grupy ISO 27000. Seria norm z tej grupy, opublikowanych przez Międzynarodową Organizację Normalizacyjną (ISO) oraz Międzynarodową Komisję Elektrotechniczną (IEC) definiuje pojęcia związane z bezpieczeństwem informacji oraz wskazuje jak wdrożyć odpowiednią strategię, zwaną Systemem Zarządzania Bezpieczeństwem Informacji (SZBI) w odniesieniu do ludzi, technologii i procesów.

Bezpieczeństwo informacji definiowane jest jako: ochrona informacji przed różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość w prowadzeniu działalności, minimalizować straty, maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym⁹. Informacja zaś traktowana jest przez wskazaną normę ISO jak aktywa, które podobnie jak inne ważne aktywa biznesowe, są niezbędne do działalności biznesowej organizacji i z tego powodu zaleca się ich odpowiednią ochronę¹⁰. Wyjaśniając istotę systemu zarządzania bezpieczeństwem informacji norma ISO/IEC 27002 wiąże to pojęcie z zachowaniem poufności (*confidentiality*), integralności (*integrity*) i dostępności (*availability*) informacji. Wskazane właściwości informacji stanowią jej fundament, określany w publikacjach jak triada CIA¹¹.

Poufność to cecha oznaczająca niedostępność informacji dla osób nieuprawnionych, innymi słowy – informacja będzie dostępna wyłącznie dla podmiotów uprawnionych do zapoznania się z jej treścią. Poziom poufności może być różny, w zależności od wartości informacji.

Integralność to właściwość polegająca na zapewnieniu dokładności i kompletności informacji, metod ich przetwarzania, koncentrująca się wokół działań uniemożliwiających umyślne bądź nieumyślne nieautoryzowane zmiany informacji¹².

Dostępność oznacza, że osoby uprawnione mogą korzystać z informacji w sposób nieograniczony w każdym czasie¹³.

Stworzenie i doskonalenie środków, procedur i regulaminów optymalizujących bezpieczeństwo informacji nie jest tylko wymogiem działalności biznesowej, ukierunkowanym na osiąganie określonych korzyści z tytułu właściwego zarządzania systemem bezpieczeństwa w organizacji, ale jest również obowiązkiem prawnym.

Określone kategorie informacji wymagają szczególnego traktowania, bowiem naruszenie ich właściwości, a więc poufności, integralności i dostępności

⁹ PN-EN ISO/IEC 27002 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji, <https://www.pkn.pl/informacje/2018/01/zarzadzanie-bezpieczenstwem-informacji> (dostęp: 01.12.2023 r.).

¹⁰ *Ibidem*.

¹¹ Zob. <https://pushsec.pl/bezpieczenstwo-informacji-co-to/> (dostęp: 01.12.2023 r.).

¹² PN-EN ISO/IEC 27002 Technika informatyczna – Techniki bezpieczeństwa..., *op.cit.*, s. 17.

¹³ M. Siergiejczyk, E. Dudek, *Ocena bezpieczeństwa i jakości informacji w systemach telematiki transportu*, „Autobusy” 2016, nr 12, s. 414–415.

może wywołać wyjątkowo negatywne konsekwencje dla dóbr prawnie chronionych. Do takich kategorii informacji należą niewątpliwie: (1) dane osób fizycznych, (2) tajemnica państwowa, (3) tajemnice zawodowe, (4) informacje finansowe czy (5) informacje handlowe przedsiębiorstwa¹⁴.

Ochrona danych osobowych jest kategorią pojęciowo zbliżoną do bezpieczeństwa danych i bezpieczeństwa informacji, niemniej jednak różnice między poszczególnymi pojęciami są zauważalne. Dla dalszych rozważań należy przyjąć, że bezpieczeństwo informacji jest pojęciem najszerszym, bowiem nie każda informacja o osobie fizycznej będzie odpowiadała definicji danych osobowych. Ochrona danych jest jednym z zadań bezpieczeństwa informacji, które poza tym odnosi się do bezpieczeństwa sieci, aplikacji i systemów¹⁵. Ochrona danych dotyczy materii związanej z legalnością procesów przetwarzania danych osobowych, a więc zgodnością z regulacjami prawnymi, przede wszystkim z przepisami RODO. Ochrona danych osobowych to stworzenie prawnych ograniczeń w dostępie do danych osób fizycznych, czemu służą zapisy RODO wskazując kto, kiedy i na jakiej podstawie prawnej może przetwarzać dane osobowe.

Europejskie ustawodawstwo chroni osoby fizyczne w związku z przetwarzaniem ich danych osobowych (vide tytuł aktu prawnego), natomiast bezpieczeństwo informacji chroni te dane już w procesie przetwarzania, optymalizując środki i metody, które zapewnią poufność, integralność i dostępność danych. Nie ma więc wątpliwości, że pojęcia te zazębiają się ze sobą. Na podobnej płaszczyźnie należy porównać pojęcia ochrony danych osobowych i bezpieczeństwa danych osobowych wprost używane w przepisach RODO.

Jak wcześniej wspomniano, ochronę danych osobowych należy utożsamiać z dopuszczalnością przez RODO przetwarzania danych osobowych i zasadami bezpiecznego przetwarzania danych osobowych. Szczegółowe regulacje zawarto w art. 5 – poświęconym zasadom przetwarzania danych oraz 6 ust. 1 RODO, w którym przedstawiono autonomiczne przesłanki legalnego przetwarzania danych osobowych zwykłych, wśród których najczęściej w praktyce występującą jest zgoda podmiotu danych osobowych. Z kolei w art. 9 ust. 1 ustawodawca europejski co do zasady zakazał przetwarzania danych osobowych sensytywnych, pozostawiając jednak w ust. 2, na zasadzie wyjątku, ściśle określone warunki, w jakich przetwarzanie danych szczególnej kategorii jest dopuszczalne. Bezpieczeństwo danych osobowych związane jest z czynnościami, metodami, środkami zabezpieczającymi dane osobowe przed dostępem osób nieuprawnionych – począwszy od zabezpieczeń fizycznych po szyfrowanie danych. Optymalizowanie bezpieczeństwa danych osobowych znalazło swoje miejsce w standardzie międzynarodowej normy ISO 27701, która określa

¹⁴ Por. A. Kasprzak, *System zarządzania bezpieczeństwem informacji*, <https://lexdigital.pl/system-zarzadzania-bezpieczenstwem-informacji> (dostęp: 06.01.2024 r.).

¹⁵ Por. <https://ccit.pl/jaka-jest-roznica-miedzy-ochrona-danych-a-bezpieczenstwem-informacji> (dostęp: 06.01.2024 r.).

system zarządzania i wymagania bezpieczeństwa dla przetwarzania danych osobowych¹⁶.

Niezależnie od międzynarodowych regulacji, wyrażanych w normach ISO, rozszerzających, rozbudowujących i doskonalących standardy systemów zarządzania bezpieczeństwem informacji, jak i systemów zarządzania bezpieczeństwem danych osobowych, w praktyce występują zdarzenia, które zagrażają najważniejszym atrybutom informacji, a więc poufności, integralności i dostępności. Wystąpienie takiego zagrożenia stanowi incydent bezpieczeństwa informacji, co odnosi się również do szczególnej kategorii informacji, jaką są dane osobowe.

Incydent bezpieczeństwa informacji (danych osobowych)

Wyjaśnienie pojęcia „incydent bezpieczeństwa informacji” rozpocząć należy od etymologicznego i słownikowego znaczenia słowa „incydent”. Słowo to, wywodzące się z języka łacińskiego *incidens, incidensis* oznacza „zdarzający się”. W znaczeniu słownikowym incydent to „nieprzyjemne wydarzenie”¹⁷. Pojęcie to rozszerza Internetowa Poradnia Językowa, nazywając incydent „nieprzyjemnym lub niespodziewanym wydarzeniem, które zakłóca przebieg innych zdarzeń, często bardziej znaczących, towarzyszy mu dezorganizacja”¹⁸. Zapis normy technicznej PN-ISO/IEC27000, wyjaśnia, że incydent bezpieczeństwa informacji to pojedyncze niepożądane lub niespodziewane zdarzenie lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji¹⁹.

Zdarzenie związane z bezpieczeństwem informacji, jest pojęciem węższym od incydentu i oznacza wystąpienie takiego stanu systemu, sieci lub usługi, który wskazuje na naruszenie polityki bezpieczeństwa lub błąd zabezpieczenia, lub nieznaną dotychczas sytuację, która może być związana z bezpieczeństwem informacji²⁰. Skoro incydent bezpieczeństwa informacji tworzy zagrożenie dla ciągłości określonej działalności, to w standardach przywołanej normy ISO podkreślono konieczność właściwego reagowania na zaistniałą sytuację, reagowania, które zminimalizuje ewentualne szkody oraz zapobiegnie podobnym wydarzeniom w przyszłości. Zarządzaniem incydentami związanymi z bezpieczeństwem informacji określono procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków²¹.

O bezpieczeństwie informacji, incydentach, a więc wszelkiego rodzaju zagrożeniach czy wreszcie faktycznych naruszeniach mówi się zwłaszcza w kontekście prawa o ochronie danych osobowych osób fizycznych, gdyż te informacje,

¹⁶ <https://gdpr.pl/iso-27701-miedzynarodowy-standard-dotyczacy-ochrony-danych-osobowych> (dostęp: 06.01.2024 r.).

¹⁷ <https://sjp.pwn.pl/slowniki/incydent.html> (dostęp: 06.01.2024 r.).

¹⁸ <https://polszczyzna.pl/incydent-co-to-jest-definicja-synonimy-przyklady-uzycia-sownik/> (dostęp: 06.01.2024 r.).

¹⁹ PN-ISO/IEC27000:2014-11, pkt 2.36, s. 12.

²⁰ *Ibidem*, pkt 2.35.

²¹ *Ibidem*, pkt 2.37.

należące do sfery życia prywatnego poddawane są ciągłym procesom przetwarzania, implikując tym samym ryzyko naruszenia praw i wolności człowieka.

Istota naruszenia ochrony danych osobowych w świetle rozporządzenia ogólnego 2016/679 (RODO)

Pojęcie bezpieczeństwa danych osobowych

Jednym z wymogów ustanowionych w RODO jest to, że dane osobowe muszą być przetwarzane za pomocą odpowiednich środków technicznych i organizacyjnych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem²².

Przetwarzanie danych osobowych to z kolei pojęcie oznaczające operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych sposób zautomatyzowany lub niezautomatyzowany. Ta definicja opisowa, umieszczona w art. 4 pkt 2 RODO została uszczegółowiona przykładami czynności przetwarzania – począwszy od zbierania, poprzez utrwalanie, ujawnianie po usuwanie niszczenie danych osobowych. Tak więc zakres faktycznych działań wykonywanych na danych osobowych jest bardzo szeroki stąd też, koniecznym stało się skonkretyzowanie przez ustawodawcę europejskiego przepisów zapewniających bezpieczeństwo danych osobowych w procesie ich przetwarzania.

„Bezpieczeństwo danych osobowych” to tytuł sekcji 2 rozporządzenia, którą rozpoczyna art. 32 poświęcony bezpieczeństwu przetwarzania, a w nim to określono obowiązki administratora i podmiotu przetwarzającego dane osobowe w zakresie zapewnienia bezpieczeństwa procesom przetwarzania. Wskazany obowiązek prawny nie precyzuje jakiego rodzaju środki, metody, procedury mają być przez adresatów normy zastosowane, wymaga jednakowoż, aby przy doborze środków organizacyjnych i technicznych uwzględnili oni następujące aspekty: (1) stan wiedzy technicznej, (2) koszty wdrażania, (3) charakter, zakres, kontekst i cele przetwarzania, (4) ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze.

Tak więc „dobór adekwatnych środków opiera się na ocenie ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia oraz na zasadzie proporcjonalności uwzględniającej stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania”²³.

W tym samym artykule, ust. 1, rozporządzenie 2016/679 podaje przykładowe środki do wdrożenia w celu zapewnienia adekwatnego do poziomu ryzyka systemu

²² Zob. art. 5 ust. 1 lit. f) i art. 32 RODO.

²³ D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018, art. 32, <https://sip.lex.pl/#/commentary/587747173/544613/bielak-jomaa-edyta-red-lubasz-dominik-red-rodoo-ogolne-rozporzadzenie-o-ochronie-danych-komentarz?pit=2024-01-29&cm=URELATIONS> (dostęp: 30.01.2024 r.).

bezpieczeństwa i są nimi: (1) pseudonimizacja i szyfrowanie danych osobowych, (2) zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania, (3) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego, (4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Artykuł 32 pozostaje w korelacji z motywem 83 preambuły RODO, w którym dodatkowo określono jakie ryzyko dla podmiotów danych osobowych wiąże się z procesami przetwarzania, pisząc „Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych”.

Naruszenie ochrony danych osobowych – definicja i rodzaje

Zgodnie z treścią art. 4 pkt 12 rozporządzenia 2016/679 przez naruszenie ochrony danych osobowych rozumiemy „naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”.

Z definicji tej można wyprowadzić wniosek o konieczności jednoczesnego, łącznego wystąpienia trzech przesłanek, aby można było zidentyfikować naruszenie ochrony danych osobowych, a to:

- naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie,
- skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,
- naruszenie jest skutkiem złamania zasad bezpieczeństwa danych²⁴.

Klasyfikując rodzaje naruszeń ochrony danych osobowych należy odwołać się do stanowiska Grupy Roboczej art. 29, wyrażonego w „Opinii 03/2014 na temat powiadamiania o przypadkach naruszenia danych osobowych”, która stosując triadę CIA (*confidentiality, integrity i availability*) jako klasyczne kryteria bezpieczeństwa, wyróżniła:

- naruszenie dotyczące poufności danych – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych,

²⁴ *Obowiązki administratorów związane z naruszeniami ochrony danych osobowych*, wersja 1.0, maj 2019, www.uodo.gov.pl, s. 3 (dostęp: 24.01.2024 r.).

- naruszenie dotyczące integralności danych – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych,
- naruszenie dotyczące dostępności danych – naruszenie, w rezultacie którego dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych²⁵.

Z prawnego punktu widzenia, wystarczające jest naruszenie któregośkolwiek z wymienionych kryteriów bezpieczeństwa, aby mówić o naruszeniu ochrony danych osobowych. Oczywiście w praktyce występują również zdarzenia, które ingerują jednocześnie w poufność, integralność i dostępność danych osobowych. Urząd Ochrony Danych Osobowych (UODO) w specjalnym materiale poświęconym naruszeniom ochrony danych osobowych, opierając się na treści zgłoszeń wskazał przykładowe zdarzenia, w których doszło do naruszenia poszczególnych kategorii bezpieczeństwa²⁶.

Naruszeniem dotyczącym poufności danych może być (1) przypadkowe przesłanie danych klienta sklepu internetowego do niewłaściwego działu bądź do osoby postronnej, ale również (2) celowe zainfekowanie systemu informatycznego, w wyniku którego dostęp do danych osobowych uzyskały nieuprawnione, nieupoważnione osoby. Niezamierzone zmodyfikowanie danych, poprzez błędne ich odczytanie i wpisanie do bazy, jak też celowe dopisanie do nazwisk klientów dodatkowej litery (dla żartu) to przykłady naruszenia integralności danych. Czasowa bądź trwała utrata czy zniszczenie danych osobowych, pozbawiające dostępu do nich podmiotów danych może nastąpić w wyniku zgubienia bądź kradzieży nośnika informacji (laptop, pendrive) – przy braku kopii zapasowej, przypadkowego bądź celowego usunięcia danych z bazy klientów (również przy braku kopii zapasowej), celowego bądź wywołanego „siłą wyższą” przerwania zasilania systemu informatycznego, uniemożliwiającego dostęp do danych. Trwała utrata danych osobowych, uniemożliwiająca dostęp do nich dla podmiotu danych jest jednoznacznym naruszeniem ochrony danych osobowych w rozumieniu art. 4 ust. 12 RODO. Wątpliwości interpretacyjne pojawiają się kiedy utrata dostępu do danych osobowych ma charakter tymczasowy, stąd też Urząd Ochrony Danych Osobowych, bazując na wytycznych Grupy Roboczej art. 29 uznał, że naruszeniem ochrony danych osobowych „jest tylko taka niedostępność danych, która może stanowić ryzyko dla praw lub wolności osób fizycznych, np. w przypadku szpitala brak dostępu danych pacjentów może prowadzić do uniemożliwienia

²⁵ *Opinia 3/2014 w sprawie powiadamiania o przypadkach naruszenia danych osobowych z dnia 25 marca 2014 r. (wersja polska)*. Grupa robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE. Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Brussels, Belgia, biuro nr MO-59 02/013, http://ec.europa.eu/justice/data-protection/index_pl.htm, s. 4–5 (dostęp: 24.01.2024 r.).

²⁶ *Obowiązki administratorów związane z naruszeniami...*, *op.cit.*, s. 3–5.

przeprowadzenia operacji medycznej, a zatem narażenia życia, co należy zaklasyfikować jako wysokie ryzyko dla praw lub wolności osób fizycznych²⁷.

Potencjalne skutki naruszenia ochrony danych osobowych

Europejskie ustawodawstwo dedykowane ochronie informacji, a w szczególności danych osobowych (RODO) podkreślając wagę wprowadzanych rozwiązań prawnych koncentruje się na wyeksponowaniu negatywnych konsekwencji naruszenia ochrony danych osobowych. W motywach 75 i 85 preambuły RODO wyliczono potencjalne negatywne konsekwencje dla osób, których dane osobowe w procesie przetwarzania zostały zagrożone bądź pozbawione wymaganej prawem ochrony poprzez naruszenie któregokolwiek z kryterium bezpieczeństwa.

Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze, może „prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą”²⁸.

„Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfalszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorcemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać

²⁷ *Ibidem*, s. 4.

²⁸ Zob. Motyw 75 Preambuły RODO.

zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki”²⁹.

Prawne obowiązki administratora danych osobowych w związku ze stwierdzonym naruszeniem ochrony danych osobowych

Katalog negatywnych konsekwencji wynikających z naruszenia ochrony danych osobowych nie jest katalogiem zamkniętym, pozwala jednak zauważyć jak istotną kwestą dla europejskiego ustawodawcy stało się właściwe i szybkie reagowanie administratorów danych osobowych na incydenty bezpieczeństwa. Do ich prawnych obowiązków w tym zakresie należą: (1) wprowadzenie procedur umożliwiających stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych; (2) zgłaszanie naruszeń organowi nadzorczemu; (3) powiadamianie osoby, której dane dotyczą, o naruszeniu; (4) podejmowanie działań mających na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości³⁰.

Wprowadzenie wewnętrznych procedur, o których mowa powyżej jest niezwykle istotnym elementem polityki bezpieczeństwa danych osobowych. Stwierdzenie i oszacowanie ryzyka naruszenia praw i wolności osób fizycznych jest niezbędne do ukierunkowania dalszego postępowania z incydentami bezpieczeństwa. Badając czy ryzyko naruszenia praw lub wolności osób fizycznych jest mało realne, czy też wysoce prawdopodobne, należy uwzględnić, treść Motywu 76 preambuły RODO – „Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko”.

Nie każde zdarzenie zakłócające ochronę i bezpieczeństwo danych osobowych będzie tożsame z pojęciem naruszenia ochrony danych osobowych. Ustalenie poziomu ryzyka naruszenia praw i wolności osób fizycznych będzie implikowało kolejne obowiązki administratora w zakresie zgłoszenia naruszenia do organu nadzorczego jak też powiadomienia o takim fakcie osoby, której dane dotyczą. Zakres i tryb postępowania w przypadkach naruszenia ochrony danych osobowych ujęto w art. 33 i 34 rozporządzenia. Obowiązkiem (wyłącznie) administratora danych osobowych jest zgłoszenie organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych), bez zbędnej zwłoki, nie później niż 72 godziny po stwierdzeniu naruszenia, a więc o każdym incydencie powodującym ryzyko naruszenia praw lub wolności osób fizycznych. Podmiot przetwarzający zobligowany jest natomiast do zawiadomienia o zdarzeniu właściwego administratora, którego dane przetwarza na podstawie umowy powierzenia przetwarzania danych osobowych. Ponadto podmiot przetwarzający ma obowiązek ustalenia

²⁹ Zob. Motyw 85 Preambuły RODO.

³⁰ Zob. Motywy 85–88 Preambuły RODO.

okoliczności naruszenia i niezwłocznego przekazania tych informacji administratorowi, na którego zlecenie dokonuje przetwarzania³¹. Jeżeli w wyniku oceny zdarzenia okaże się, że nie ma prawdopodobieństwa wystąpienia ryzyka naruszenia praw i wolności osób fizycznych, administrator zwolniony jest z obowiązku powiadamiania organu nadzorczego o naruszeniu³².

W przypadku ustalenia, że naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, niezależnie od obowiązku zgłoszenia tego faktu do organu nadzorczego, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu³³. Niezależnie od poziomu ryzyka naruszenia praw lub wolności osób fizycznych administrator zobligowany jest do dokumentowania wszelkich incydentów bezpieczeństwa precyzując okoliczności, ich skutki oraz podjęte działania zaradcze.

Naruszenie ochrony danych osobowych w praktyce – dane statystyczne

Na podstawie sprawozdania z działalności Prezesa UODO ustalono, że w roku 2022 wpłynęły 12 772 zgłoszenia naruszeń, co jest liczbą porównywalną do roku 2021³⁴. Do najczęściej zgłaszanych przez administratorów danych naruszeń ochrony danych osobowych należały: (1) nieprawidłowe zaadresowanie korespondencji zarówno w formie tradycyjnej, jak i elektronicznej, (2) udostępnienie danych niewłaściwej osobie, (3) nieprawidłowa anonimizacja danych lub niezamierzona ich publikacja, (4) zagubienie korespondencji przez operatora pocztowego lub otwarcie korespondencji przed zwróceniem jej do nadawcy, (5) nieuprawniony dostęp do baz danych, (6) zagubienie, kradzież lub pozostawienie w niezabezpieczonej lokacji dokumentacji papierowej lub nośnika danych, (7) wykorzystanie złośliwego oprogramowania ingerującego w poufność, integralność lub dostępność danych osobowych.

W 2022 roku Prezes UODO wszczął z urzędu 59 postępowań administracyjnych w sprawie naruszenia przepisów o ochronie danych osobowych, a także wydał 25 decyzji administracyjnych w związku ze stwierdzeniem naruszenia ochrony danych osobowych.

Podsumowanie

Rozważania na temat bezpieczeństwa informacji, incydentów bezpieczeństwa oraz bezpieczeństwa i ochrony danych osobowych i związanych z tym naruszeń wykazały niewątpliwie istnienie zależności nie tylko terminologicznych, ale również merytorycznych. Bezpieczeństwo informacji jest pojęciowo najszersze

³¹ M. Smolarska, *Naruszenie ochrony danych osobowych. Obowiązki administratora*, „ZN Politechniki Śląskiej Systemy Wspomagania w Inżynierii Produkcji” 2021, nr 10, s. 15.

³² Zob. art. 33 ust. 1 RODO.

³³ Zob. art. 34 ust. 1 RODO.

³⁴ *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2022*, <https://uodo.gov.pl/pl/487/2279> (dostęp: 30.01.2024 r.).

i bezdyskusyjnie bezpieczeństwo danych osobowych będzie kategorią bezpieczeństwa informacji, które odnosi się również do innych obszarów (bezpieczeństwo sieci, systemów, aplikacji). Jak wykazano powyżej, naruszenie ochrony danych osobowych łączy się z trzema podstawowymi kryteriami bezpieczeństwa informacji (triada CIA), a więc poufnością integralnością i dostępnością.

Naruszenie bezpieczeństwa informacji będzie stanowiło naruszenie ochrony danych osobowych, jeżeli informacjami będą dane osobowe zgodnie z definicją rozporządzenia 2014/679³⁵. Naruszenie ochrony danych osobowych jest rodzajem incydentu bezpieczeństwa informacji, powodując prawdopodobieństwo zakłócenia procesu przetwarzania i zagrażając bezpieczeństwu informacji (danych osobowych). Naruszenie ochrony danych osobowych będzie każdorazowo incydem bezpieczeństwa informacji, bo dane osobowe to określonego rodzaju informacje o osobach fizycznych, ale nie każdy incydent bezpieczeństwa informacji będzie oznaczał naruszenie ochrony danych osobowych, tylko taki, który powoduje negatywne konsekwencje dla osób, których dane przetwarzamy.

Reasumując, terminy, które przybliżono w niniejszym rozdziale mają zarówno cechy wspólne, jak też wyróżniające je odrębności. Bezsporne i łączące wszystkie omówione kategorie jest to, że przy współczesnym rozwoju technologii koniecznością stało się dostosowywanie europejskiego prawa do narastających zagrożeń zarówno dla ochrony i bezpieczeństwa danych osobowych, jak i szeroko rozumianego bezpieczeństwa informacji.

³⁵ Zobacz art. 4 pkt 1 RODO.

IV.
**Wyzwania cyberbezpieczeństwa
a współczesna gospodarka**

CYBERBEZPIECZEŃSTWO W WARUNKACH PRZEMYSŁU 4.0 JAKO WSPÓŁCZESNE WYZWANIE W ZARZĄDZANIU KLASTREM

Wprowadzenie

Współczesne wyzwania rozwojowe dla klastrów jakie generują chociażby przemysł czwartej generacji (4.0) i transformacja cyfrowa są związane w znacznej mierze z zapewnieniem cyberbezpieczeństwa, zapobieganiem różnorodnym formom i przejawom cyberzagrożeń, kształtowaniem świadomości cyfrowej, wdrażaniem odpowiednich rozwiązań technicznych pozwalających na ochronę danych, urządzeń i zasobów cyfrowych. Decydenci w klastrach coraz częściej angażują się w różne projekty z partnerami klastrów, które pomagają im w wykrywaniu różnego rodzaju cyberzagrożeń, ich analizowaniu i reagowaniu na nie w odpowiedni sposób. Niezależnie od profilu działalności klastrów, w każdym z nich, w tym w poszczególnych podmiotach członków klastrów i organizacjach klastrowych, pełniących funkcję instytucjonalnego koordynatora klastra, niemalże codziennie przetwarza się ogromne ilości danych, którym mogą zagrozić zewnątrzni lub wewnętrzni cyberprzestępcy. W wielu klastrach funkcjonują inteligentne fabryki tj. niskoemisyjne, cyberfizyczne systemy o wysokim stopniu cyfryzacji, automatyzacji i autonomizacji, które wykorzystują różne technologie informacyjno-komunikacyjne (ICT), dlatego tym bardziej wzrasta zainteresowanie kompleksową i sprawną ochroną klastrów przed zaawansowanymi cyberzagroženiami. Wzmocnienie odporności klastrów, w tym ich zdolności do reagowania na tego typu zagrożenia może jednocześnie sprzyjać wzrostowi ich konkurencyjności na arenie krajowej i międzynarodowej.

Celem rozdziału monografii jest z jednej strony charakterystyka strategicznego wymiaru cyberbezpieczeństwa w klastrach przyczyniających się do rozwoju Przemysłu 4.0, a z drugiej syntetyczne zarysowanie tła przesłanek inicjatyw klastrowych zorientowanych na cyberbezpieczeństwo. W ramach tak zdefiniowanego celu sformułowano trzy pytania badawcze, odzwierciedlające fragment rzeczywistości klasteringu:

- w czym wyraża się istota inteligentnych fabryk i cyberbezpieczeństwa?
- jakie mogą być efekty i przejawy implementacji koncepcji Przemysłu 4.0?

¹ Politechnika Rzeszowska im. Ignacego Łukasiewicza. ORCID: 0000-0003-1816-1147.

- jakie są doświadczenia i dobre praktyki klastrów w obszarze cyberbezpieczeństwa?

Przyjęte pytania badawcze jako fundament zaplanowanych i oryginalnych badań własnych dotyczyły wybranych aspektów cyberbezpieczeństwa w klastrach. W procesie badawczym zastosowano tradycyjną metodykę przeglądu literatury naukowej, analizę danych zastanych i studium przypadku. Wybór problemu badawczego, niewątpliwie bardzo istotnego zarówno z poznawczego, jak i pragmatycznego punktu widzenia, wynikał z tego, że w polskiej literaturze naukowej brakuje kompleksowych publikacji i szerszej dyskusji z zakresu cyberbezpieczeństwa w warunkach Przemysłu 4.0, traktowanego jako współczesne wyzwanie strategiczne w zarządzaniu klastrem.

Inteligentne fabryki w Przemysle 4.0

We współczesnej literaturze przedmiotu brakuje jednoznacznej definicji Przemysłu 4.0, ponieważ pojęcie to ma charakter złożony, wieloznaczny i interdyscyplinarny. Najczęściej jednak koncepcja tej formy rozwoju przemysłu analizowana jest w kontekście zmian procesu produkcyjnego i transformacji cyfrowej. Powszechnie przyjmuje się, że pojęcie to może być rozumiane jako²:

- nowa generacja produkcji wspomaganej inteligentnymi systemami informatycznymi w obszarze planowania, monitorowania i kontroli procesów technologicznych i wytwórczych oraz podejmowania decyzji na trzech poziomach, tj. strategicznym, taktycznym i operacyjnym,
- wykorzystanie procesów automatyzacji i cyfryzacji przemysłu do przekształcenia istniejących fabryk w wirtualne sieci, samosterujące się i samoadaptujące się systemy socjotechniczne, które pozwalają na tworzenie inteligentnych łańcuchów wartości,
- nowa koncepcja organizacji produkcji, w której kluczowe jest kształtowanie inteligentnych łańcuchów wytwarzania, wspomaganych systemami cyfrowymi,
- zmiana paradygmatu relacji człowiek – maszyna i procesu produkcji w odniesieniu do architektury wytwarzanych wyrobów, sposobu projektowania i organizacji produkcji, modelu biznesowego, wewnętrznego i zewnętrznego łańcucha wartości,

² A. Kamiński, *Inteligentna fabryka – nowe trendy w rozwoju systemów informatycznych dla przemysłu*, „Zarządzanie i Finanse” 2018, nr 3(2), Vol. 16, s. 113–115; Sz. Jarosz, *Zjawisko czwartej rewolucji przemysłowej w sektorze finansów, ekonomii i zarządzania*, „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne” 2022, nr 40, s. 161–164; A. Kemendi, P. Michelberger, A. Mesjasz-Lech, *Industry 4.0 and 5.0 – organizational and competency challenges of enterprises*, „Polish Journal of Management Studies” 2022, Vol. 26, No. 2, s. 209–215; J. Świętoniowska, *Projekty innowacyjne motorem wdrażanych zmian w koncepcji Przemysłu 4.0*, „Przedsiębiorczość i Zarządzanie” 2018, nr 5, Vol. 19, s. 51; J. Bendkowski, *Zmiany w pracy produkcyjnej w perspektywie koncepcji Przemysłu 4.0*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie” 2017, nr 112, s. 22.

- transformacja technologiczna przemysłu przyczyniająca się do znacznego poszerzenia możliwości działalności biznesowej, wzrostu produktywności czynników produkcji, oferowania wyrobów i usług bardziej innowacyjnych i odpowiednio dostosowanych do indywidualnych potrzeb klientów,
- zmiany zachodzące w społeczeństwie, przemyśle i technologii, związane z cyfryzacją przemysłu, automatyzacją, przetwarzaniem i wymianą danych oraz nowoczesnymi technikami wytwórczymi,
- dynamiczna zmiana sposobu pozyskiwania i efektywnego wykorzystania informacji dostępnych w czasie rzeczywistym, z dowolnego miejsca,
- integracja systemów decyzyjnych z siecią powiązań w procesach produkcyjnych, ścisłą współpracą pracowników i sterowanymi cyfrowo maszynami,
- szeroka integracja, koordynacja i współpraca autonomicznych maszyn, robotów i różnych klas i generacji systemów transakcyjnych i analitycznych,
- cyfryzacja, digitalizacja, automatyzacja w procesie produkcji oraz w ramach łańcucha wartości przedsiębiorstw,
- systematyczne wykorzystanie systemów inteligentnych i robotów w różnego rodzaju produkcji i świadczeniu usług,
- przenikanie się świata fizycznego z cyfrowym w procesie produkcji.

Koncepcja Przemysłu 4.0 związana z tzw. czwartą rewolucją przemysłową, będącą kontynuacją upowszechnienia i wykorzystania maszyny parowej, linii produkcyjnej oraz automatyzacji procesu produkcyjnego, zrodziła się w odpowiedzi na takie współczesne zjawiska, jak np.: nasilająca się rywalizacja przedsiębiorstw na zglobalizowanych rynkach, poszukiwanie nowych źródeł względnie trwałej przewagi konkurencyjnej, przesuwanie się preferencji klientów w kierunku wyrobów i usług dostosowanych do ich indywidualnych potrzeb, rozwój przełomowych technologii, stwarzających nowe możliwości reakcji na oczekiwania i potrzeby rynku w zakresie personalizacji i kastomizacji³. W tym miejscu warto podkreślić, że w paradygmacie personalizowanej produkcji klient jest aktywnym uczestnikiem projektowania produktu finalnego, przeważnie z użyciem specjalistycznych narzędzi wspomagających projektowanie, zaś w paradygmacie masowej kastomizacji klient może dokonać wyboru konfigurację adekwatną do swoich potrzeb z katalogu dostępnych w danym czasie opcji⁴.

J. Moczydłowska uważa, że termin „Przemysł 4.0” jest swoistym skrótem myślowym używanym dla określenia efektywnego sposobu wytwarzania wyrobów i świadczenia usług, opartego na nowoczesnych technologiach i sztucznej inteligencji, który integruje sferę informacji i materii⁵. W literaturze przedmiotu pojęcie „Przemysł 4.0” jest współcześnie synonimem inteligentnego przemysłu,

³ P. Wieczorek, *Wizja przemysłu nowej generacji – perspektywa dla Polski. Czwarta rewolucja przemysłowa*, „Kontrola Państwowa” 2018, nr 3, s. 92.

⁴ W. Furmanek, *Najważniejsze idee czwartej rewolucji przemysłowej*, „Dydaktyka Informatyki” 2018, nr 13, s. 62.

⁵ J. Moczydłowska, *Przemysł 4.0: ludzie i technologie*, Difin, Warszawa 2023, s. 9.

który koncentruje się m.in. na spektakularnym postępie technologicznym, integracji kluczowych funkcji przedsiębiorstw z łańcuchami dostaw celem inteligentnej produkcji⁶. Oznacza nowe sposoby pracy i funkcje ludzi w przemyśle, gwałtowny wzrost jakości i efektywności surowcowej, produkcyjnej, logistycznej i transportowej dzięki zachodzącym zmianom technologicznym i transgresji, bezprzewodowym i przewodowym połączeniom komunikacyjnym jednocześnie obsługującym mobilne i stacjonarne urządzenia łącznie realizujące i materializujące określony produkt⁷. Jako nowa koncepcja rozwoju przemysłu nie tylko redefiniuje wyznawane dotychczas wartości i metody pracy, ale także promuje cyfrowy styl życia, w którym automatyzacja oraz technologia informatyczna są wykorzystywane szeroko w różnych aspektach życia codziennego⁸. W rezultacie szybko stała się popularna w duchu idei gospodarki opartej na wiedzy, opierając się na wykorzystaniu złożonych systemów cyberfizycznych i zaawansowanych technologii ICT wraz z potencjałem sztucznej inteligencji i zarządzania wiedzą w technologicznej transformacji produkcji⁹.

Koncepcja Przemysłu 4.0 nie dotyczy tylko modernizacji szeroko ujmowanego procesu produkcyjnego, ale wskazuje także na potrzebę odmiennego podejścia do całej filozofii gospodarowania zasobami oraz kreowania nowych modeli biznesowych, szczególnie w ramach tzw. gospodarki współdzielenia¹⁰. Wprowadza współczesne przedsiębiorstwa w nową erę robotyzacji i digitalizacji poprzez optymalną kontrolę poszczególnych faz procesu produkcyjnego¹¹. Koncentruje się na zrównoważonym rozwoju inteligentnych fabryk (*smart factories*), który uznawany za bezpieczny i przyjazny środowisku naturalnemu wymaga sprawnego wykorzystania sztucznej inteligencji, pełnej autonomiczności operacji sterowania, monitorowania i kontroli produkcji poprzez wymianę danych pomiędzy różnymi maszynami i robotami przemysłowymi, a także integracji technicznych środków produkcji z systemami cyberfizycznymi, które wspomagają procesy operacyjne i zarządcze¹². Aktywność inteligentnych fabryk sprzyjać może szybszej adaptacji systemów do zmian preferencji rynku, minimalizowaniu sytuacji awaryjnych, zwiększeniu efektywności wykorzystania zasobów, w tym energii,

⁶ M. Frankowska, K. Nowicka, *Zarządzanie łańcuchem dostaw w dobie Smart Industry*, „Gospodarka Materiałowa i Logistyka” 2018, nr 3, s. 6.

⁷ R. Janikowski, *Środowiskowe aspekty czwartej rewolucji przemysłowej*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania Uniwersytetu Szczecińskiego” 2017, nr 47(2), s. 68–74.

⁸ A. Rogozińska-Pawelczyk, *Przywództwo 4.0 w przedsiębiorstwach business services sector*, „Zarządzanie Zasobami Ludzkimi” 2022, nr 3–4 (146–147), s. 26.

⁹ A. Białobrodzki, Ł. Nazarko, M. Wilczewska, *Egzogenne czynniki wpływające na rozwój Przemysłu 4.0 w przedsiębiorstwach produkcyjnych Białostockiego Obszaru Funkcjonalnego*, „Akademia Zarządzania” 2020, nr 4(3), s. 9.

¹⁰ P. Wieczorek, *Wizja przemysłu nowej generacji...*, *op.cit.*, s. 90.

¹¹ E. Racek, S. Kosmowska, *Factory technologies of the future – automation and digitalization of production in the aspect of Industry 4.0 concept*, „The Małopolska School of Economics in Tarnów Research Papers Collection” 2018, Vol. 40(4), s. 51–52.

¹² A. Kamiński, *Inteligentna fabryka – nowe trendy w rozwoju systemów informatycznych dla przemysłu*, „Zarządzanie i Finanse” 2018, nr 3 (2), Vol. 16, s. 116.

rozszerzaniu procesu produkcyjnego na dostawców i odbiorców w ramach łańcucha wartości przy jednoczesnym współdzieleniu wiedzy, kompetencji i innowacyjności w zakresie sprawdzonych modeli współpracy z tego typu partnerami biznesowymi¹³.

W modularnej strukturze inteligentnej fabryki to głównie cyberfizyczne systemy monitorują fizyczne procesy, komunikują się ze sobą przez Internet Rzeczy w czasie rzeczywistym, asystują ludziom i maszynom w realizacji ich zadań, tworzą wirtualne kopie fizycznego świata, podejmując zdecentralizowane decyzje w oparciu o mechanizmy samoorganizacji¹⁴. W tak zorganizowanej fabryce w warunkach transformacji cyfrowej musi być zapewniona automatyzacja ciągów technologicznych i pełna integracja wszystkich systemów informatycznych stosowanych w przedsiębiorstwie¹⁵. Z kolei dla zapewnienia należytego poziomu bezpieczeństwa warunków pracy należy mieć na uwadze w szczególności optymalizację produkcji i utrzymania ruchu oraz systemów bezpieczeństwa wykorzystujących inteligentne czujniki i zaawansowane systemy bazodanowe, które mogą w czasie rzeczywistym szczegółowo analizować wybrane dane z linii produkcyjnych¹⁶.

Inteligentne fabryki funkcjonują jak elastyczne sieci, w których dane dotyczące materiałów, projektów, zasobów, interesariuszy itp. są dostępne w czasie rzeczywistym dla każdego systemu nadzoru, planowania i organizowania¹⁷. Jako podmioty innowacyjno-cyfrowe wyposażone w zintegrowaną moc obliczeniową i umiejętności komunikacyjne dbają o jakość komunikacji nie tylko na linii maszyna-maszyna, ale również na linii człowiek-człowiek-maszyna-technologia¹⁸. W całym procesie produkcyjnym zapewniona jest całkowita przejrzystość, co ułatwia optymalizację procesów decyzyjnych¹⁹. Przewiduje się, że integracja nowoczesnych technologii, w tym m.in. automatyzacji, sztucznej inteligencji, cyfrowego bliźniaka, Internetu Rzeczy, przyspieszy transformację cyfrową i doprowadzi do nieodwracalnych zmian w strukturze i formach zatrudnienia, stwarzając liczne wyzwania dla rynku pracy i zarządzania zasobami ludzkimi. Dlatego też świadomość mocnych i słabych stron aktywności inteligentnych fabryk pozwala decydom na podejmowanie właściwych decyzji w zakresie inwestycji

¹³ A. Stasiuk-Piekarska, Ł. Hadaś, M. Wyrwicka, *Wybrane aspekty ryzyka organizacyjnego w koncepcji Przemysłu 4.0*, „Przedsiębiorczość i Zarządzanie” 2018, nr 5, Vol. 19, s. 39.

¹⁴ W. Furmanek, *Najważniejsze idee...*, *op.cit.*, s. 59.

¹⁵ P. Wieczorek, *Wizja przemysłu nowej generacji ...*, *op.cit.*, s. 96.

¹⁶ T. Lis, T. Małysa, *Zarządzanie bezpieczeństwem i higieną pracy w aspekcie wdrażanych rozwiązań Przemysłu 4.0*, „Zeszyty Naukowe WSH” 2021, nr 1, s. 102.

¹⁷ K. Kiraga, *Przemysł 4.0 – rewolucja przemysłowa według FESTO*, „Autobusy” 2016, nr 12, s. 1604.

¹⁸ K. Nowacki, *Rola człowieka w innowacyjnym przedsiębiorstwie z wykorzystaniem koncepcji Przemysłu 4.0 – studium przypadku*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu” 2020, nr 11, Vol. 64, s. 57.

¹⁹ B. Ślusarczyk, *Potencjalne rezultaty wprowadzania koncepcji Przemysłu 4.0 w przedsiębiorstwach*, „Przegląd Organizacji” 2019, nr 1(948), s. 7.

w doskonalenie kompetencji cyfrowych i przekwalifikowania pracowników²⁰. Według M. Cichorzewskiej, B. Hysy i P. Wójcika największą trudnością związaną z wdrożeniem wybranych rozwiązań inteligentnej fabryki może być przede wszystkim konieczność stopniowej lub radykalnej zmiany kultury organizacyjnej i pozyskania nowych kompetencji przez pracowników w nowym środowisku pracy²¹. W tym kontekście K. Nowacki podkreśla, że problematyka zarządzania zasobami ludzkimi w pełni zautomatyzowanych procesach, które są domeną inteligentnych fabryk, jest zagadnieniem słabo rozpoznanym w teorii i praktyce gospodarczej w obliczu wymagań sprawnej realizacji koncepcji Przemysłu 4.0 w gospodarce opartej na wiedzy²².

M. Frankowska i K. Nowicka podkreślają, że inteligentne fabryki mogą współpracować ze sobą w ramach inteligentnych łańcuchów dostaw w oparciu o inteligentne technologie w celu wytworzenia i dostarczenia inteligentnych wyrobów i usług, zgodnie z wymaganiami i oczekiwaniami klientów²³. Jednocześnie są strategicznym elementem klastrów przemysłowych, w tym tych zaawansowanych technologicznie (*high-tech*). W literaturze przedmiotu klastry zaawansowane technologicznie definiowane są jako skupiska firm działających w sektorze zaawansowanych technologii i innych podmiotów z określonych, powiązanych ze sobą branż, charakteryzujących się wysoką intensywnością realizacji projektów badawczo-rozwojowych. Firmy w tych klastrach mają bliskie relacje z podmiotami sektora B+R oraz instytucjami otoczenia biznesu, co ułatwia im transfer wiedzy i technologii, projektowanie i wdrażanie innowacji, przyciąganie i stymulowanie inwestycji. Dlatego też klastry *high-tech* przyczyniają się do zmniejszenia luki w rozwoju sektora zaawansowanych technologii i stanowią istotny komponent regionalnych systemów innowacji i narzędzie kształtowania konkurencyjności gospodarki²⁴. To w nich upatruje się solidną podstawę do wykreowania inteligentnej specjalizacji regionu²⁵. Często w teorii i praktyce określa się ich mianem klastrów wiedzy, innowacyjnych i badawczych, dlatego że postrzegane są jako narzędzie ułatwiające uczelniom komercjalizację wiedzy, pozwalające na korzystne łączenie świata nauki z biznesem i identyfikację wzajemnych potrzeb partnerów, co może prowadzić do tworzenia nowych innowacyjnych firm typu *spin-off*, *spin-out*

²⁰ A.S. Vadie, K. Liptak, *Przemysł 4.0: nowe wyzwania dla rynku pracy i warunków pracy na skutek pojawienia się robotów i automatyzacji*, „Studia Ekonomiczne i Regionalne” 2023, nr 3, Vol. 16, s. 444.

²¹ M. Cichorzewska, B. Hysa, P. Wójcik, *Wybrane aspekty zarządzania różnorodnością pracowników Przemysłu 4.0*, Wydawnictwo Politechniki Lubelskiej, Lublin 2020, s. 30.

²² K. Nowacki, *Rola człowieka w innowacyjnym...*, *op.cit.*, s. 53.

²³ M. Frankowska, K. Nowicka, *Zarządzanie łańcuchem dostaw...*, *op.cit.*, s. 6.

²⁴ A. Baranowska, J. Gąska, M. Lis, D. Pelle, Ł. Skrok, *Klastry zaawansowanych technologii jako instrument wsparcia rozwoju i konkurencyjności regionów – analiza i wnioski dla polityki regionalnej oraz polityki spójności*, Instytut Badań Strukturalnych, Warszawa 2009, s. 9–21.

²⁵ D. Łangowska, *Klastry oparte na wiedzy i ich wpływ na rozwój gospodarczy Polski*, „Roczniki Kolegium Analiz Ekonomicznych Szkoły Głównej Handlowej w Warszawie” 2015, nr 36, s. 135.

i *start-up*²⁶. Według M. Citkowskiego unikatowy zbiór różnorodnych kompetencji występujących w klastrze i wzajemne interakcje między podmiotami klastra generują specyficzny ekosystem predysponujący go do generowania kreatywnych rozwiązań na poziomie wymagań Przemysłu 4.0, co wymusza na organizacji klastrów dbałość o skuteczność zarządzania kompetencjami relacyjnymi²⁷. Dlatego też w 2017 roku w ramach inicjatywy przedsiębiorczej Politechniki Rzeszowskiej, uczelni będącej liderem z zakresu badań nad aplikacją przemysłową wspomaganych komputerowo systemów projektowania, prototypowania, wytwarzania i automatyzacji procesów produkcyjnych, rozpoczęto prace nad utworzeniem struktury sieciowej Krajowego Klastra Przemysłu 4.0. Przyjęto, że cel strategiczny klastra będzie dotyczył integracji przedsiębiorstw przygotowujących się do wdrażania inteligentnych technologii, a także przedsiębiorstw produkujących komponenty i systemy stosowane w procesach digitalizacji i cyfryzacji przemysłowej. Aktywność klastra ma umożliwić realizację zaawansowanych prac badawczo-rozwojowych z zakresu inteligentnych fabryk oraz wdrażania zintegrowanych systemów komputerowych opartych na potencjale przemysłowym²⁸.

Strategiczny wymiar cyberbezpieczeństwa

W literaturze przedmiotu często podkreśla się, że Przemysł 4.0 i związany z nim dynamiczny rozwój cyfryzacji i digitalizacji z jednej strony jest szansą na wzmocnienie konkurencyjności przedsiębiorstw i zaspakajanie indywidualnych potrzeb klientów, zaś z drugiej jest źródłem cyberzagrożeń i nowych wyzwań w obszarze cyberbezpieczeństwa inteligentnych fabryk²⁹.

Dyskusja i pierwsze prace z zakresu zapewnienia cyberbezpieczeństwa rozpoczęły się wraz powstaniem cyberprzestrzeni, gdyż w efekcie tej rewolucji informatycznej, która ukształtowała nową domenę ludzkiej aktywności, zrodziła się naturalna potrzeba, a wręcz konieczność ochrony sieci informatycznych, urządzeń, wykorzystywanych programów przed ich uszkodzeniami, atakami i nieuprawnionym dostępem³⁰. Cyberbezpieczeństwo to szczególny rodzaj bezpieczeństwa, który ujmowany jest przez pryzmat ochrony informacji niejawnych i ustawowo chronionych, porządku i ładu struktur umieszczonych w cyberprzestrzeni, odporności systemów informacyjnych³¹. Polega na ochronie systemów komputerowych

²⁶ J. Machnik-Słomka, *Znaczenie klastrów wiedzy w komercjalizacji wyników badań z uczelni*, „Organizacja i Zarządzanie” 2011, nr 4, s. 96-99.

²⁷ M. Citkowski, *Managing relational competences of industrial cluster and the challenges of Industry 4.0 — theoretical approach*, „Marketing i Rynek” 2021, nr 12(28), s. 3.

²⁸ <https://forumakademickie.pl/sprawy-nauki/politechnika-rzeszowska-czlonkiem-klastra-industry-4-0> (dostęp: 28.10.2023 r.).

²⁹ M. Wodnicka, *Wpływ czwartej rewolucji przemysłowej na innowacyjność usług*, „Optimum. Economic Studies” 2021, nr 3(105), s. 56; B. Ślusarczyk, *Potencjalne rezultaty...*, *op.cit.*, s. 9.

³⁰ S. Woszek, *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2022, nr 27(14), s. 200.

³¹ D. Skoczyła, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterrorizm i incydent sieciowe*, „Prawo w Działaniu. Sprawy Karne” 2023, nr 53, s. 102.

przed złośliwymi atakami lub szpiegostwem, obejmując szeroki wachlarz narzędzi i technik pozwalających chronić infrastrukturę, poufność, integralność i dostępność danych, które są przechowywane lub wymieniane w cyberprzestrzeni w warunkach gospodarki cyfrowej³². Jako bezpieczeństwo informatyczne polega na wdrożeniu i zarządzaniu właściwymi środkami zabezpieczeń technicznych systemu informacyjnego w ramach cyberprzestrzeni tj. przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy informatyczne i systemy powiązań internetowych³³. Cyberprzestrzeń traktowana jako nie w pełni rozpoznany wymiar aktywności człowieka, rzeczywistość wirtualna, przestrzeń komunikacyjna zmieniająca się wraz z postępem technologicznym i cechująca się anonimowością, aterytorialnością, systematycznością i globalnym zasięgiem, pozwala na nawiązywanie relacji w czasie rzeczywistym³⁴. W tym kontekście bezpieczeństwo w cyberprzestrzeni polega na przyjętych zabezpieczeniach i działaniach mających na celu zachowanie dostępności i integralności sieci i infrastruktury, zachowanie poufności zawartych w nich danych i informacji, redukcję obecnych i potencjalnych zagrożeń, zmniejszenie podatności na nie³⁵. Według M. Laszczaka zarządzanie cyberbezpieczeństwem organizacji w erze cyfrowej wymaga podejścia systemowego, sprecyzowania zbioru najważniejszych zasad, koncentracji wysiłków na tych obszarach aktywności organizacji, które uznaje się za kluczowe dla bezpieczeństwa³⁶.

Problem zapewnienia cyberbezpieczeństwa wiąże się bezpośrednio z potrzebą ciągłej identyfikacji i oceny niebezpieczeństwa, a wręcz zagrożenia, związanego z ryzykownymi i niepewnymi działaniami i sytuacjami, które mogą przyczynić się do utraty wartościowych zasobów informacyjnych i informatycznych przez ich właściciela/dysponenta w danym miejscu i czasie³⁷. W świetle współczesnej literatury przedmiotu należy przyjąć, że cyberzagrożenia stają się coraz liczniejsze, bardziej inteligentne i coraz trudniejsze do wykrycia³⁸. Ze względu na ich źródło wyróżnia się wewnętrzne i zewnętrzne tego typu zagrożenia, gdzie³⁹:

³² A. Pieczywok, *Polityczno-prawne strategie i dyrektywy przeciwdziałania cyberzagrożeniom*, „Cybersecurity and Law” 2023, nr 2(10), s. 158.

³³ P. Górny, J. Krawiec, *Cyberbezpieczeństwo – podejście systemowe*, „Obronność. Zeszyty Naukowe” 2016, nr 2(18), s. 2.

³⁴ M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny” 2018, nr 1–2, s. 59–60.

³⁵ Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej” 2016, nr 2(10), s. 108.

³⁶ M. Laszczak, *Zarządzanie bezpieczeństwem w erze cyfrowej*, „Bezpieczeństwo. Teoria i Praktyka” 2019, nr 4, s. 136.

³⁷ P. Sienkiewicz, *Bezpieczeństwo cyberprzestrzeni państwa*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług” 2012, nr 703(88), s. 807.

³⁸ J. Sadowski, *Cybernetyczny wymiar współczesnych zagrożeń*, „Studia nad Bezpieczeństwem” 2017, nr 2, s. 73.

³⁹ M. Marczyk, *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny” 2018, nr 1–2, s. 68.

- wewnętrzne cyberzagrożenia dotyczą wszelkich zamierzonych i niezamierzonych, niebezpiecznych działań odnoszących się bezpośrednio lub pośrednio do elementów cyberprzestrzeni, środowiska sieci i systemów komputerowych, na które oddziałuje wewnętrzny podmiot/interesariusz danego otoczenia (np. nieuprawniony dostęp do zasobów sieci, kradzież informacji i danych, niewłaściwe wykorzystanie aplikacji działających w systemie, nieuprawnione wykorzystywanie luk systemów i oprogramowania, awarie sprzętowe, wadliwe oprogramowanie),
- zewnętrzne cyberzagrożenia o charakterze naturalnym, technicznym i społecznym to głównie te zjawiska, które powstają na skutek działalności zewnętrznych podmiotów (np. cyberataki, kradzieże tożsamości, hacking, phishing, malvertising, cyberprzemoc, cyberszpiegostwo) lub spowodowane są przez „siły natury”, np. silną burzę słoneczną (magnetyczną), która może mieć wpływ na infrastrukturę internetową.

W literaturze przedmiotu dominuje jednomyślne przekonanie, że wraz z dokonującą się transformacją cyfrową problem cyberzagrożeń będzie dynamicznie wzrastał⁴⁰. Wraz ze wzrostem poziomu cyberprzestępczości i pojawianiem się wciąż nowych technologii, m.in. Internetu Rzeczy, jednocześnie powstają nowe i złożone wyzwania w zakresie cyberbezpieczeństwa. Cyberzagrożenia z uwagi na fakt, że zmieniają się niemalże każdego dnia, nie są w pełni zidentyfikowane i poznane, przez co trudno zapewnić optymalną ochronę w tym obszarze aktywności. Dlatego osiągnięcie dojrzałości cyfrowej i mądra polityka cyberbezpieczeństwa może stanowić kluczowy punkt odniesienia dla zasad ochrony cyberprzestrzeni w skali makro, mezo i mikro oraz bezpiecznego jej użytkowania przez osoby fizyczne i prawne⁴¹. Europejskie i krajowe regulacje prawne, które tworzą liczne wymogi dotyczące cyberbezpieczeństwa, czy też regulacje sektorowe i zbiory dobrych praktyk w zakresie cyberbezpieczeństwa pokazują jak ogromne jest zapotrzebowanie na spójne, kompletne i rzetelnie opracowane ramy prawne zarówno dla ochrony przed atakami cybernetycznymi, jak i w zakresie ochrony danych osobowych⁴². Jednakże niezwykle trudno jest ujednoczyć regulacje prawne cyberprzestrzeni dla wszystkich krajów Unii Europejskiej, czy całego świata, chociażby ze względu na różnice w prawie cywilnym i karnym, czy konflikty interesów⁴³.

W procesie projektowania zabezpieczeń organizacyjnych i technicznych sprzyjających sprawnemu zapewnieniu cyberbezpieczeństwa bardzo użyteczny jest System Zarządzania Bezpieczeństwem Informacji. Obejmuje on wszelkie procedury, zasady, regulaminy i instrukcje przenikające newralgiczne obszary

⁴⁰ S. Woszek, *Cyberbezpieczeństwo państw w XXI wieku...*, *op.cit.*, s. 214.

⁴¹ D. Skoczyła, *Cyberzagrożenia w cyberprzestrzeni...*, *op.cit.*, s. 110.

⁴² W. Hydzik, *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Business Law Journal” 2019, nr 3, s. 84–87.

⁴³ K. Wąsik, *Międzynarodowe regulacje prawne dotyczące cyberprzestrzeni*, „Cybersecurity and Law” 2023, nr 2(10), s. 152.

organizacji, w tym obszar bezpieczeństwa informatycznego, osobowego, prawnego i fizycznego, gdzie jego konstrukcja powinna się opierać na wiedzy w zakresie potrzeb organizacji i jej celów biznesowych, jak także wymaganiach w odniesieniu do jej kompleksowego bezpieczeństwa⁴⁴. Pełne i pomyślnie wdrożenie tego systemu zgodnie z normą ISO 27001 jest procesem złożonym i trudnym⁴⁵. Wymaga stosowania się do właściwych przepisów prawa w tym obszarze, organizacyjnego uczenia się i rozwoju wiedzy członków organizacji m.in. o zasadach postępowania w sytuacjach naruszenia cyberbezpieczeństwa, czy sprawdzonych sposobach unikania i przeciwdziałania różnym cyberzagrożeniom. Przyjmuje się, że system zarządzania zgodny z ISO 27001 umożliwia zarządzanie bezpieczeństwem informacji w sposób kompleksowy i usystematyzowany, oparty na podejściu wynikającym z ryzyka biznesowego, przez co jest źródłem wartości dla różnych interesariuszy⁴⁶.

Cyfrizacja w klastrach – doświadczenia i dobre praktyki

Rozwój inteligentnych fabryk w klastrach przemysłowych wymaga sprawnej cyfrizacji i digitalizacji. W literaturze przedmiotu pojęcia cyfrizacji i digitalizacji są powiązane ze sobą znaczeniowo, gdyż digitalizacja polega na przekształceniu analogowej, papierowej formy dokumentacji w elektroniczny, cyfrowy zapis danych, zaś cyfrizacja jako pojęcie szersze sprowadza się do rozpowszechniania technologii cyfrowej w różnych aspektach życia, przetwarzania danych cyfrowych, zwiększania dostępności zasobów internetowych, optymalizacji wykorzystania cyberprzestrzeni⁴⁷. Analizując ten złożony problem cyfrizacji w klastrach celowe jest odniesienie się do wybranych wyników ogólnopolskich badań benchmarkingowych klastrów, które zrealizowano w 2022 roku na zlecenie Polskiej Agencji Rozwoju Przedsiębiorczości na próbie 41 klastrów. W raporcie z badań wykazano, że⁴⁸:

- cyfrizacja klastrów sprzyja urzeczywistnianiu koncepcji Przemysłu 4.0,
- klastry z dominującą liczbą podmiotów branży ICT mogą tworzyć ofertę w zakresie dostaw technologii Przemysłu 4.0, skierowaną do przedsiębiorstw i klastrów,

⁴⁴ M. Wiśniewska, *Kompleksowe podejście do zarządzania bezpieczeństwem informacji – System Zarządzania Bezpieczeństwem Informacji*, „Zeszyty Naukowe Politechniki Łódzkiej. Organizacja i Zarządzanie” 2009, nr 45(1064), s. 80.

⁴⁵ D. Rydz, M. Krakowiak, T. Bajor, *Zapewnienie bezpieczeństwa informacji w przedsiębiorstwie*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa” 2013, t. 1, s. 286.

⁴⁶ M. Pałęga, *System zarządzania bezpieczeństwem informacji ISO/IEC27001 w działalności logistycznej*, „Logistyka” 2014, nr 3, s. 4938.

⁴⁷ M. Warszewicz, *Digitalizacja oraz transformacja cyfrowa. Studium Przypadku PKN Orlen S.A.* [w:] *Logistyka i transport*, red. J. Brach, N. Szozda, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2021, s. 87.

⁴⁸ M. Piotrowski, *Benchmarking klastrów w Polsce – edycja 2022. Raport ogólny*, PARP, Warszawa 2023, s. 91–95.

- najczęściej wykorzystywane systemy informatyczne na poszczególnych etapach łańcuchów wartości klastrów to: systemy zarządzania relacjami z klientami, systemy zarządzania zasobami, systemy zarządzania dokumentami, systemy zarządzania treścią, systemy rejestracji czasu pracy, analityka biznesowa,
- pod względem wykorzystywanych systemów informatycznych na poszczególnych etapach łańcuchów wartości klastrów szczególnie wysokie oceny uzyskały klastry informatyczne, motoryzacyjne, chemiczne, obróbki metali i medyczne,
- w klastrach wykorzystywano różne technologie Przemysłu 4.0, m.in. takie jak: systemy informatyczne, systemy cyberbezpieczeństwa, produkcja 3D, technologie chmurowe, analityka dużych zbiorów danych, platformy cyfrowe, Internet Rzeczy, autonomiczne roboty, sztuczna inteligencja,
- w klastrach wzrasta zainteresowanie wykorzystaniem sztucznej inteligencji, w tym potencjału ChatGPT,
- w 22 klastrach spośród 41 badanych klastrów inwestowano w rozwój infrastruktury informatycznej (mediana: 650 zł, zaś benchmark: 50 mln zł),
- większość badanych członków klastrów (72% z 642) wyraziło swoje zadowolenie z aktywności ich instytucjonalnych koordynatorów w obszarze cyfryzacji klastra i wdrażania technologii Przemysłu 4.0,
- członkowie badanych klastrów zainteresowani byli usługami doradczymi w zakresie transformacji cyfrowej i wdrażania technologii Przemysłu 4.0,
- pod względem oceny poziomu cyfryzacji szczególnie wyróżniają się Krajowe Klastry Kluczowe na tle innych badanych klastrów.

Inteligentne fabryki w klastrach, które badają swą dojrzałość cyfrową, aby optymalnie wykorzystać technologie cyfrowe w procesie rozwoju wyrobów, usług i procesów wytwarzania z reguły ambitnie podejmują wciąż nowe wyzwania gospodarki cyfrowej. Wyzwania te często są efektem transformacji cyfrowej, ujmowanej jako kompleksowa i fundamentalna zmiana, która prowadzi do przekształcenia dotychczasowej logiki funkcjonowania przedsiębiorstw, ich sposobu tworzenia wartości dodanej, rozwoju zasobów i kompetencji cyfrowych, zdolności związanych z elastycznością cyfrową, sieciami cyfrowymi i analizą dużych zbiorów danych⁴⁹. Dlatego też funkcjonowanie inteligentnych fabryk w klastrach przemysłowych stymuluje społeczność klastrową do usprawniania technologii produkcji, integrując ją z inteligentną technologią sieciowych systemów komunikacji i przetwarzania danych. Z badań zrealizowanych przez ekspertów z zakresu klasteringu dla Platformy Przemysłu Przyszłości w październiku 2021 roku wśród 12

⁴⁹ P. Kawalec, *Transformacja cyfrowa: szanse i wyzwania dla przedsiębiorstw*, „Nowe Tendencje w Zarządzaniu 2021”, nr 1, s. 50.

Krajowych Klastrow Kluczowych (KKK), dotyczących poziomu cyfryzacji klastrowych łańcuchów wartości wynika, że⁵⁰:

- w sześciu badanych klastrach zidentyfikowano nakładanie technologii cyfrowych na obecnie realizowane procesy biznesowe w ramach tradycyjnych branż gospodarki, w czterech klastrach – wykorzystywano technologie cyfrowe do zmian modelu działania przedsiębiorstw w ramach klastrowego łańcucha wartości, zaś w jednym klastrze – charakterystyczne było tworzenie treści zdigitalizowanych i ich przetwarzanie, gromadzenie, dostarczanie i udostępnianie w ramach cyfrowych branż gospodarki,
- do najbardziej popularnych technologii informatycznych wykorzystywanych w badanych klastrach zaliczono m.in. platformy komunikacyjne, Internet Rzeczy, technologie cyberbezpieczeństwa, zaś do współczesnych rozwiązań technologicznych wykorzystywanych sporadycznie zaliczono m.in. chmurę obliczeniową, sztuczną inteligencję, Big Data,
- cyfryzacja przyspiesza zmiany w klastrowych łańcuchach wartości, powodując konieczność dynamicznego i elastycznego reagowania klastrowych łańcuchów wartości, które mogą w ten sposób utrzymać lub wzmocnić poziom swojej konkurencyjności,
- dojrzałość cyfrowa klastrowych łańcuchów wartości jest traktowana jako ich czynnik sukcesu, źródło względnie trwałej przewagi konkurencyjnej,
- w ocenie dojrzałości cyfrowej klastrowych łańcuchów wartości można wyróżnić pięć poziomów: wstępny (brak wizji, planów i mierników digitalizacji oraz zastosowania technologii cyfrowych w klastrowym łańcuchu wartości), koncepcyjny (kreowanie koncepcji i planów cyfryzacji w ramach klastrowego łańcucha wartości, pierwsze zastosowania technologii Przemysłu 4.0), zdefiniowany (skoordynowane działania na rzecz opracowania wizji i planów cyfryzacji, postrzeganie cyfryzacji i digitalizacji jako strategicznego kierunku zmian), zarządzany (postępy w urzeczywistnianiu wizji i planów cyfryzacji, wdrażanie nowych technologii Przemysłu 4.0, redefiniowanie i cyfryzacja głównych procesów biznesowych), optymalny (cyfryzacja atrybutem funkcjonowania i rozwoju klastrowego łańcucha wartości lub jego elementu, zwinna, innowacyjna, elastyczna, zorientowana na użytkownika kultura cyfrowa, powszechne stosowanie technologii Przemysłu 4.0),
- transformacja cyfrowa klastrowego łańcucha wartości wymaga czasu i koncentracji zasobów członków klastra wokół wspólnych celów cyfryzacji i digitalizacji,
- zestaw podstawowych działań ukierunkowanych na zwiększanie poziomu dojrzałości cyfrowej klastrowego łańcucha wartości obejmuje: komplek-

⁵⁰ A. Kowalski, A. Moskwa, P. Wojciechowski, J. Parzuchowski, S. Rynkiewicz, *Poradnik dotyczący cyfryzacji łańcuchów wartości w klastrach*, Platforma Przemysłu Przyszłości, Warszawa 2021, s. 28–49.

sową diagnozę stanu jego cyfryzacji, identyfikację zasobów i kompetencji cyfrowych, mapowanie technologii cyfrowych, określenie wizji w ramach strategii cyfryzacji, formułowanie, wdrażanie i kontrolę realizacji planów operacyjnych z uwzględnieniem źródeł finansowania,

- możliwe działania przyspieszające cyfryzację klastrowego łańcucha wartości to m.in. edukacja w zakresie cyfryzacji, badania potencjału cyfryzacji, analiza SWOT w zakresie cyfryzacji, identyfikacja barier cyfryzacji, współpraca z ekspertami i firmami doradczymi, zapewnienie finansowania liderów transformacji cyfrowej, zmiana modeli biznesowych, współdzielenie zasobów, benchmarking,
- zauważalne (spektakularne) zmiany pozytywne w klastrowym łańcuchu wartości wystąpią wówczas, gdy transformacja cyfrowa obejmie cały ekosystem klastra, w tym jego partnerów, dostawców, klientów, inwestorów itp.

Koncepcja klastrowego łańcucha wartości implikuje postrzeganie klastra jako całości wszystkich procesów, funkcji, zadań i działań, jakie przedsiębiorstwa klastrowe realizują w zakresie tworzenia wartości dodanej w wyniku podejmowanej działalności gospodarczej. W klastrze każde przedsiębiorstwo jest ogniwem szerszego łańcucha wartości, ale samo też tworzy swój unikatowy wewnętrzny łańcuch wartości⁵¹. Dlatego też koncepcja klastrowego łańcucha wartości zakłada, że wszystkie procesy, funkcje, zadania i działania realizowane przez przedsiębiorstwa klastrowe powinny prowadzić z jednej strony do tworzenia wartości dodanej dla różnych kluczowych interesariuszy klastra, a z drugiej – przyczyniać się do ciągłego osiągania wartości dodanej na rzecz rozwoju i wzmocnienia konkurencyjności klastra jako całości poprzez sekwencję celowo zorientowanych działań współpracujących ze sobą i konkurujących w danej dziedzinie przedsiębiorstw. Według M. Frankowskiej nawiązuje ona do koncepcji ścieżki ekonomicznej, odnosząc się wprost do zorganizowanej formy relacji przedsiębiorstw osadzonych strukturalnie, geograficznie, instytucjonalnie i relacyjnie w klastrze, wykorzystujących pojawiające się możliwości i szanse wynikające ze stopniowego redukcowania międzyorganizacyjnych kosztów transakcyjnych, a także z synergicznego podwyższania efektywności operacyjnej realizowanych przepływów fizycznych, informacyjnych i finansowych⁵². Klastrowe łańcuchy wartości to odpowiedź na współczesne potrzeby nie tylko jednoczesnego różnicowania, specjalizacji oferty i koncentracji działań na obniżce kosztów, ale także usprawniania procesów logistycznych sprzyjających m.in. dostępności dla podmiotów rynków krajowych i międzynarodowych. Sukces tego typu łańcuchów wartości upatrywany jest w umiejętności stworzenia silnego i zrównoważonego łańcucha dostaw, którego

⁵¹ T. Rojek, *Koncepcja łańcucha wartości w zarządzaniu przedsiębiorstwem*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubezpieczenia” 2014, nr 803(66), s. 821.

⁵² M. Frankowska, *Współdziałanie przedsiębiorstw w klastrowych łańcuchach dostaw*, CeDeWu, Warszawa 2018, s. 237.

fundamentem jest innowacyjny, dynamiczny w każdym ogniwie i międzynarodowo zorientowany łańcuch dostaw⁵³. W tym miejscu nie sposób nie nawiązać do dobrych praktyk Klastra Gospodarki Odpadowej i Recyklingu, w którym jego instytucjonalny koordynator wspiera jego członków w zakresie transformacji cyfrowej, w tym rozwoju kompetencji cyfrowych, tworzenia cyfrowych map drogowych, transformacji innowacyjnej Przemysłu 4.0. W ramach oferowanego wsparcia członek klastra może otrzymać zestaw narzędzi do tworzenia i zarządzania innowacjami oraz aktywne wsparcie na etapie tworzenia rozwiązań innowacyjnych, poszukiwania i pozyskiwania zewnętrznych źródeł finansowania⁵⁴.

Klaster cyberbezpieczeństwa – studium przypadku

Struktura Polskiego Klastra Cyberbezpieczeństwa CyberMadeInPoland jako klastra przemysłowego ukonstytuowała się w 2020 roku w ramach inicjatywy klastrów m.in. Instytutu Kościuszki i ICsec S.A. – doświadczonego producenta na rynku zabezpieczeń infrastruktury przemysłowej, oferującego rozwiązania zmniejszające ryzyko biznesowe związane z cyberatakami na sieci przemysłowe. Partnerem wspierającym rozwój klastra jest Związek Cyfrowa Polska, który jest zaangażowany w projekty związane z transformacją cyfrową polskich firm i kształtowaniem higieny cyfrowej. Dla instytucjonalnej koordynacji działań klastra w sierpniu 2020 roku zarejestrowano spółkę z o.o. funkcjonującą pod nazwą klastra.

Nawiązując do genezy powstania klastra warto podkreślić, że w 2017 roku w ramach III European Cybersecurity Forum – CYBERSEC, gdzie przyjęto, że cyberbezpieczeństwo musi być priorytetem rządów, instytucji i biznesu, przedstawiciele 14 regionalnych centrów cyberbezpieczeństwa z 10 krajów (Cyberspark – Israel, Centre for Secure Information Technologies – U.K., The Hague Security Delta – Netherlands, Global Cybersecurity Resource – Carleton University – Canada, University of New Brunswick – Canada, CyberTech Network – U.S.A., The Kosciuszko Institute – Poland, Politecnico di Torino Italy, La Fundación INCYDE – Spain, Cyber Wales – U.K., bwtech@UMBC – U.S.A., Procomer – Costa Rica, Innovation Boulevard Surrey, BC – Canada, CSA – Singapore), podpisali w Krakowie porozumienie promujące działalność Globalnej Platformy Innowacji dla Cyberbezpieczeństwa (GlobalEPIC – Global Ecosystems Partnered in Innovation and Cybersecurity). Jej członkowie łącząc kompetencje, doświadczenie i wiedzę chcą wspólnie opracowywać i wdrażać innowacyjne rozwiązania w obliczu bieżących i potencjalnych cyberzagrożeń, napędzać dzielenie się wiedzą, przeprowadzać analizy trendów i badania, wpływać i wyznaczać standardy na poziomie

⁵³ M. Frankowska, *Znaczenie koncepcji klastrowych łańcuchów dostaw w zwiększaniu międzynarodowej konkurencyjności regionalnych sieci kooperacyjnych*, „International Journal of Management and Economics” 2011, nr 32, s. 105–114.

⁵⁴ <https://klasterodpadowy.com/portal/oferta-klustra/proinno> (dostęp: 28.10.2023 r.).

globalnym⁵⁵. Poprzez współpracę w sieci strategicznej i rozwijanie międzynarodowych ekosystemów innowacji podejmują próbę „glokalizacji” – lokalizowania tego, co globalne i globalizacji tego, co lokalne⁵⁶.

Z opracowanej w 2021 roku strategii rozwoju klastra CyberMadeInPoland (Polish Cybersecurity Cluster #CyberMadeInPoland) wynika, że⁵⁷:

- klastery powstały w odpowiedzi na najbardziej naglące kwestie bezpieczeństwa cyfrowego oraz potrzebę kształtowania i rozwoju bezpiecznej cyberprzestrzeni,
- organizacja może uzyskać status członka klastra zwyczajnego po zaakceptowaniu treści Regulaminu Klastra, podpisaniu i złożeniu Deklaracji Przyłączenia oraz jej zaakceptowaniu przez instytucjonalnego Koordynatora Klastra,
- w strukturze klastra liczebnie dominują mikro i małe przedsiębiorstwa,
- celem strategicznym klastra jest stworzenie efektywnego systemu współpracy członków klastra przyczyniającego się do bardziej dynamicznego rozwoju, wzrostu konkurencyjności i poprawy sprawności ich działania,
- koordynator klastra jest bezpośrednio odpowiedzialny za realizację strategii rozwoju klastra, dlatego nadzoruje on implementację zaplanowanych działań, monitoruje je oraz dokonuje ewaluacji, a także koordynuje działania operacyjne konieczne do osiągnięcia celu strategicznego,
- system monitoringu realizacji strategii klastra obejmuje procesy zachodzące wewnątrz klastra oraz zjawiska i procesy zachodzące w jego otoczeniu (np. usługi edukacyjne w obszarze cyberbezpieczeństwa, certyfikacja i regulacja rynku cyberbezpieczeństwa, źródła finansowania działalności operacyjnej i rozwojowej).

Klastery stanowią przykład platformy współpracy oraz promocji polskiego przemysłu cyberbezpieczeństwa w kraju i poza granicami kraju. Misją klastra jest kształtowanie i rozwój bezpiecznej cyberprzestrzeni w Polsce poprzez tworzenie ekosystemu, składającego się z wielu przedstawicieli organizacji komercyjnych, społecznych i publicznych, tak aby efekt synergii pozwolił na kompleksowe podejście do rozwoju tego obszaru aktywności w kraju i poza jego granicami. Z kolei wizja klastra zakłada, że będzie on rozpoznawalnym i wiarygodnym Krajowym Klastrem Kluczowym o globalnym potencjalnym oddziaływaniu, wspierającym rozwój polskiego przemysłu cyberbezpieczeństwa, kształtującym nowe kierunki rozwoju cyberbezpieczeństwa w ramach współpracy międzysektorowej. W maju 2021 roku klastery przystąpiły do rządowego Programu Współpracy w Cyberbezpieczeństwie (PWCyber), będącego niekomercyjną inicjatywą o charakterze partnerstwa publiczno-prywatnego, którego zakres i forma zbieżne były z celami Strategii Cyberbezpieczeństwa RP na lata 2019–2024 i spójne są z ustawą o krajowym

⁵⁵ <https://2017.cybersecforum.eu/global-cybersecurity-initiative-launched-strengthen-collaboration-between-regional-ecosystems> (dostęp: 28.10.2023 r.).

⁵⁶ <https://globalepic.org> (dostęp: 28.10.2023 r.).

⁵⁷ <https://cybermadeinpoland.pl> (dostęp: 28.10.2023 r.).

systemie cyberbezpieczeństwa, która implementuje do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady Unii Europejskiej z dnia 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej. Partnerzy zawartego porozumienia mają wymieniać się wiedzą i doświadczeniem dla zwiększenia bezpieczeństwa cyfrowych procesów, wyrobów i usług. Ponadto ich aktywność ma przyczynić się do rozwoju badań nad certyfikacją cyberbezpieczeństwa, budowania sprawnego Krajowego Systemu Cyberbezpieczeństwa, podnoszenia kompetencji w zakresie świadomości cyberzagrożeń, promowania innowacji cyberbezpieczeństwa. Warto podkreślić, że z chwilą przystąpienia klastra do tego programu w jego strukturze funkcjonowało 47 przedsiębiorstw oferujących wyroby i usługi z zakresu m.in. anti-malware, compliance, szyfrowania, informatyki śledczej, bezpieczeństwa przemysłowego, audytu⁵⁸.

W efekcie podpisanego porozumienia w czerwcu 2021 roku zorganizowano w klastrze cykl bezpłatnych szkoleń dla Operatorów Usług Kluczowych, uwzględniających najważniejsze wyzwania w kontekście ustawy o krajowym systemie cyberbezpieczeństwa, czy też innowacyjne rozwiązania opracowane przez polskich dostawców wyrobów i usług szeroko rozumianego przemysłu cyberbezpieczeństwa. We wrześniu 2021 roku w ramach klastra opracowano raport badawczy nt. „Cyberbezpieczeństwo polskich firm – 2021” dotyczący m.in. incydentów cyberbezpieczeństwa, inwestycji i doskonalenia wiedzy o cyberbezpieczeństwie. Kolejny opracowany raport badawczy dotyczył rynku cyberbezpieczeństwa w latach 2023–2028 i miał na celu diagnozę obecnego stanu tego rynku, jego mocnych i słabych stron oraz szans i zagrożeń, które są istotne dla jego uczestników/aktorów, czy też ocenę wpływu strategii i polityk międzynarodowych i perspektyw rozwojowych⁵⁹.

Do sukcesów klastra należy zaliczyć to, że jest jedyną instytucją w Polsce upoważnioną przez Europejską Organizację Cyberbezpieczeństwa (ECISO) do przyznawania znaku jakości Cybersecurity Made in Europe, który wyróżnia europejskie firmy w oparciu o kryterium rozwoju technologii Made in Europe, podnosi świadomość strategicznej wartości firm, które rozwijają swoją działalność w oparciu o europejskie wartości, zwiększa rozpoznawalność firm wśród interesariuszy (np. inwestorów, partnerów biznesowych, klientów, instytucji publicznych). Ponadto znak ten przyznawany w procedurze aplikacyjnej jest ważny przez okres 12 miesięcy i popularny jest w szczególności wśród europejskich start-upów i MŚP. Warto zaznaczyć, że koszt przyznania znaku w tej procedurze wynosił 6,5 tys. zł, zaś dla członków i partnerów klastra możliwa była opłata promocyjna w wysokości 3,5 tys. zł. Wybrane firmy klastra uznano za rekomendowane do realizacji grantu w ramach projektu „Cyberbezpieczny Samorząd” programu „Fundusze Europejskie na Rozwój Cyfrowy 2021–2027”, którego celem jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez

⁵⁸ <https://www.gov.pl/web/baza-wiedzy/wspolnie-dla-cyberbezpieczenstwa> (dostęp: 28.10.2023 r.).

⁵⁹ <https://cybermadeinpoland.pl> (dostęp: 28.10.2023 r.).

wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na współczesne cyberzagrożenia w systemach informatycznych⁶⁰.

Mówiąc o aktywności i rozwoju Polskiego Klastra Cyberbezpieczeństwa nie sposób nie podkreślić, że nie jest to jedyny przykład tego typu klastra w Polsce. Dolnośląski Klaster Cyberbezpieczeństwa powstał w maju 2018 roku w ramach inicjatywy klastrowej Politechniki Wrocławskiej. Za główne obszary współpracy klastrowej uznano m.in.: cyberochronę, informatykę śledczą, bezpieczeństwo elektromagnetyczne, bezpieczeństwo aplikacji, badania penetracyjne mające na celu identyfikację i ocenę potencjalnych ataków i słabych punktów w systemach informatycznych i wdrożonych systemach obronnych. Członkowie klastra byli zaangażowani w realizację projektu „Cyberbezpieczeństwo dla gospodarki przyszłości” realizowanego przez Politechnikę Wrocławską w ramach grantu z NCBiR w kwocie 22 mln zł⁶¹. W czerwcu 2022 roku klaster stał się częścią większej sieci strategicznej, tj. Makroklastra – Technologie w Bezpieczeństwie Publicznym. Była to inicjatywa Politechniki Wrocławskiej, władz samorządowych Dolnego Śląska i Wrocławia oraz Zachodniej Izby Gospodarczej. Celem nowo powstałej struktury sieciowej jest m.in. identyfikowanie newralgicznych obszarów i potrzeb bezpieczeństwa publicznego, kreowanie nowych kierunków rozwoju technologii w bezpieczeństwie publicznym, łączenie twórców i dostawców z odbiorcami innowacyjnych technologii bezpieczeństwa publicznego oraz inicjowanie, aplikowanie i realizacja wspólnych projektów badawczych. W ramach klastra wydzielono grupy robocze z zakresu: bezpieczeństwa energetycznego, bezpieczeństwa środowiska naturalnego, bezpieczeństwa społecznego, bezpieczeństwa techniczno-infrastrukturalnego i cyberbezpieczeństwa⁶².

Podsumowanie

Wraz z zachodzącą dynamicznie transformacją cyfrową, rozwojem gospodarki opartej na wiedzy i społeczeństwa informacyjnego, upowszechnieniem technologii informacyjno-komunikacyjnych, przenoszeniem aktywności gospodarczej i innych obszarów ludzkiej działalności ze świata realnego do wirtualnego (globalnej cyberprzestrzeni) to właśnie cyberbezpieczeństwo staje się jednym z kluczowych czynników sprawnie funkcjonujących organizacji, w tym klastrów i inteligentnych fabryk, a także wyzwaniem strategicznym. Z uwagi na fakt, że w warunkach transformacji cyfrowej znaczenie cyberbezpieczeństwa systematycznie wzrasta, dlatego też współczesne organizacje klastrowe jako instytucjonalni koordynatorzy klastrów stoją przed ważnym wyzwaniem, jakim jest zapewnienie odpowiedniego poziomu cyberbezpieczeństwa, zarówno dla nich samych, jak

⁶⁰ *Ibidem*.

⁶¹ <https://pwr.edu.pl/uczelnia/aktualnosci/dolnoslaski-klaster-cyberbezpieczenstwa-zainaugurowal-dzialalnosc-11079.html> (dostęp: 28.10.2023 r.).

⁶² <https://www.wroclawskiportal.pl/razem-w-kierunku-bezpieczenstwa-w-sieci-cele-makroklastra> (dostęp: 28.10.2023 r.).

i członków społeczności klastrowej. Niemalże codziennie w klastrach i organizacjach klastrowych w trakcie przetwarzania, gromadzenia, przekazywania, przechowywania i wykorzystywania danych i informacji rodzi się naturalna potrzeba minimalizowania zagrożeń ze strony cyberataków. Przestępczość w sieci internetowej może prowadzić do sytuacji kryzysowej.

W dobie rozwijającej się gospodarki cyfrowej w wielu klastrach przemysłowych, w tym klastrach zaawansowanych technologicznie funkcjonują inteligentne fabryki, które nasilając usieciowienie i niematerialny przepływ danych i informacji jednocześnie narażone są na różne cyberzagrożenia. Dlatego organizacje klastrowe oprócz zapewnienia odpowiedniego poziomu cyberbezpieczeństwa w klastrowych łańcuchach wartości dążą do kształtowania świadomości społeczności klastrowej w zakresie eliminowania lub unikania cyberzagrożeń. W obliczu Przemysłu 4.0 i rozwoju gospodarki cyfrowej jednym z celów strategicznych klastrów powinno być względnie trwale wzmocnienie ich odporności na różne cyberzagrożenia oraz pomoc ich członkom w doskonaleniu kompetencji cyfrowych i zapewnieniu dostępu do najlepszych narzędzi cyfrowych. Wymaga to sprawnego zarządzania cyberbezpieczeństwem w klastrze ujmowanego jako forma dialogu między jego członkami i instytucjonalnym koordynatorem, tak aby tego typu cele mogły być osiągnięte. Wspólne działania koordynatorów klastrów i ich członków mogą sprzyjać wzmocnieniu partnerstwa na rzecz zapobieganiu cyberataków, promowaniu dobrych praktyk cyberbezpieczeństwa, budowaniu zdolności cyfrowych oraz ich finansowaniu w ramach różnorodnych projektów inwestycyjnych i badawczo-rozwojowych. W ten sposób zwiększają się realne możliwości społeczności klastrowej do aktywnego podejmowania nowych wyzwań, jakie będzie dostarczać bezgraniczna i ewoluująca cyberprzestrzeń.

Rozdział nie wyczerpuje analizowanej problematyki, pomimo że mocno ją nakreśla. Tym samym stanowi źródło inspiracji dla prowadzenia dalszych, bardziej pogłębionych badań jakościowych i ilościowych. Współczesne i złożone zagadnienia jakimi są cyberzagrożenia i cyberbezpieczeństwo w inteligentnych fabrykach klastrów przemysłowych, mogą być analizowane na wielu płaszczyznach, pod różnymi względami na gruncie dyscypliny nauki o zarządzaniu i jakości w kontekście zarządzania strategicznego i przedsiębiorczości.

V.
**Problemy cyberbezpieczeństwa
w obszarze obronności**

Markus BRESINSKY, prof. dr¹
Francesca Elena STRAT²

CHATGPT SUPPORTING INTELLIGENCE ANALYSIS IN STRATEGIC FORECASTING

Introduction

The purpose of this study is to explore the possibility of utilising artificial intelligence (AI) tools for supporting the strategic forecasting process of intelligence analysts. Specifically, it aims at employing ChatGPT for assisting in the analysis of competing hypotheses (ACH). This paper gives an insight into the generation of hypotheses and indicators for developing scenarios in North-East Nigeria. Consequently, it discusses the results and limitations of this method in the intelligence analysis field.

Intelligence Analysis and Artificial Intelligence

Intelligence analysis plays a crucial role in the decision-making processes of governments, military organisations, law enforcement agencies, and private sector entities. This field is situated at the intersection of data and actionable insights, transforming large volumes of information into knowledge that guides operational plans, policies, and strategy³. Its role is pivotal in a global landscape characterized by multifaced challenges, where the ability to predict and mitigate emerging threats is essential. At its core, intelligence analysis is a systematic process that involves collecting, assessing, and interpreting information about an adversary or the environment⁴. It seeks to deepen comprehension of a given situation, whether it involves geopolitical developments, national security concerns, cyber threats, or criminal activities. The objective is to provide decision-makers with the clarity and foresight needed for well-informed choices⁵.

The linchpin of the intelligence analysis process is the role of intelligence analysts. They are tasked with connecting the dots, identifying patterns, and

¹ OTH-Regensburg.

² OTH-Regensburg.

³ J. Richards, *The art and science of intelligence analysis*, Oxford University Press, 2010.

⁴ S. Marrin, *Improving intelligence analysis: Bridging the gap between scholarship and practice*, Routledge, 2012.

⁵ N. Derbentseva, L. McLellan, D.R. Mandel, *Issues in Intelligence Production: Summary of Interviews with Canadian Managers of Intelligence Analysis*, Defence R & D Canada, 2010.

drawing conclusions from the available data⁶. They provide explanations for current circumstances and formulate predictions for the future⁷. The process of monitoring the long-term development of crisis and conflict zones is referred to as strategic forecasting. It methodically evaluates various possible scenarios⁸, their latent assumptions, and the potential impacts for recommendations and decisions that might promote more desirable futures⁹. When predicting future events, intelligence analysts must develop plausible hypotheses using the information at hand and then compile their findings into reports. Despite the analysts' apparent objectivity, the complex situations they attempt to explain and predict make hypothesis generation challenging. Moreover, due to the fragmentary and unreliable nature of information¹⁰, military strategies, criminal trends, or governors' decisions cannot be predicted.

Analysts try to overcome these challenges by incorporating so-called Structured Analytical Techniques (SATs) into their analysis process. SATs are a collection of methods designed to assess, coordinate, and evaluate analytical thinking. According to the CIA Tradecraft Primer¹¹, twelve SATs are classified into three distinct categories according to their fundamental analytic function: to facilitate diagnostic, contrarian, or imaginative thinking. These mechanisms ensure accountability and aid analysts in making decisions that are more credible and objective through the mitigation of cognitive biases and the management of information overload¹². In theory, using a structured method allows analysts to trace their process in order to ascertain the reasoning behind certain outcomes¹³.

Traditionally, intelligence analysis relies on human analysts who apply their expertise to interpret complex data and make informed judgments. As technology advances and information becomes more accessible, the role of the intelligence analyst is evolving and the need for innovative tools and approaches has become increasingly apparent.

⁶ I. Wing, *The characteristic of successful and unsuccessful intelligence analysts*, "Journal of the Australian Institute of Professional Intelligence Officers" 2000, 9(2), p. 4–11.

⁷ M.K. Dhami, I.K. Belton, D.R. Mandel, *The "analysis of competing hypotheses" in intelligence analysis*, "Applied Cognitive Psychology" 2019, 33(6), p. 1080–1090.

⁸ S. Inayatullah, *Questioning the future: Methods and tools for organizational and societal transformation*, Tamkang University Press, 2005.

⁹ C.N. Cook, S. Inayatullah, M.A. Burgman, W.J. Sutherland, B.A. Wintle, *Strategic foresight: how planning for the unpredictable can improve environmental decision-making*, "Trends in ecology & evolution" 2014, 29(9), p. 531–541.

¹⁰ R.K. Betts, *Analysis, war, and decision: Why intelligence failures are inevitable*, "World politics" 1978, 31(1), p. 61–89.

¹¹ US Government, *A Tradecraft Primer: Structured analytic techniques for improving intelligence analysis*, "CIA Center for the study of intelligence" 2009.

¹² R.J. Heuer Jr., *Improving Intelligence Analysis with ACH*, Washington DC: Center for the Study of Intelligence Analysis, Central Intelligence Agency, 2005.

¹³ H.B. de Melo, *Does Analysis of Competing Hypotheses (ACH) Really Mitigate Cognitive Biases? Practical Implications for Intelligence Analysts and Criminal Investigators*, "International Journal of Criminal Justice" 2021, 3(2), p. 68–82.

Artificial intelligence (AI) refers to the science and engineering of constructing systems that can perform tasks typically associated with intelligent beings, such as learning, judging, and making decisions¹⁴. AI technologies can handle large datasets, perform complex pattern recognition, and offer real-time insights. Indeed, one of the most notable advantages of AI is its ability to handle vast amounts of unstructured data, such as images, texts, and video, at an unparalleled scale and speed¹⁵. It can also comprehend and generate human language¹⁶ and automate tasks¹⁷. For instance, the extraction and categorization of information from various sources can be automated, saving analysts considerable time and effort. Moreover, natural language processing (NLP) enables AI systems to understand and generate human language, facilitating the extraction of insights from text-based sources, including open-source information, reports, and social media¹⁸.

The ‘Chat Generative Pre-trained Transformer’, or ChatGPT, as a neural language processing model, represents a great advancement in the realm of artificial intelligence. This model, developed as an extension of the GPT-3.5 architecture, became available for the first time on November 30, 2022, and acquired over a million subscribers in its first week¹⁹. Its training data spans a wide range of sources, enabling coherent and contextually relevant conversations²⁰. Its adaptability in terms of language style and tone allows it to cater to a wide range of communication needs. Due to its versatility, it can serve a wide range of applications, from answering questions and providing explanations to generating creative content and assisting with language translation²¹. It can be integrated into chatbots, virtual assistants, and various other AI-powered systems to enhance user interactions and provide valuable insights²².

The integration of reinforcement learning from human feedback (RLHF) is a standout feature. This mechanism enables the model to iteratively improve its responses through interactions with human evaluators, enhancing its ability to

¹⁴ L.D. Xu, Y. Lu, L. Li, *Embedding blockchain technology into IoT for security: A survey*, IEEE Internet of Things Journal” 2021, 8(13), p. 10452–10473.

¹⁵ F. Qayyum, D.H. Kim, S.J. Bong, S.Y. Chi, Y.H. Choi, *A Survey of Datasets, Preprocessing, Modeling Mechanisms, and Simulation Tools Based on AI for Material Analysis and Discovery*, “Materials” 2022, 15(4).

¹⁶ M. Jakesch, J.T. Hancock, M. Naaman, *Human heuristics for AI-generated language are flawed*, “Proceedings of the National Academy of Sciences” 2023, 120(11).

¹⁷ D. Acemoglu, P. Restrepo, *Artificial intelligence, automation, and work* [In:] *The economics of artificial intelligence: An agenda*. University of Chicago Press, 2018.

¹⁸ E. Brill, R.J. Mooney, *An overview of empirical natural language processing*, “AI magazine” 1997, 18(4).

¹⁹ N. Kurian, J.M. Cherian, N.A. Sudharson, K.G. Varghese, S. Wadhwa, *AI is now everywhere*, “British Dental Journal” 2023, 234(2), p. 72.

²⁰ H. Hassani, E.S. Silva, *The role of ChatGPT in data science: how ai-assisted conversational interfaces are revolutionizing the field*, “Big data and cognitive computing” 2023, 7(2).

²¹ P.P. Ray, *ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope*, “Internet of Things and Cyber-Physical Systems” 2023.

²² L. Kohnke, B.L. Moorhouse, D. Zou, *ChatGPT for language teaching and learning*, “RELC Journal” 2023, 00336882231162868.

provide contextually accurate and valuable replies²³. This dynamic approach highlights ChatGPT's ability of continuous refinement and addressing its limitations. Additionally, the availability of ChatGPT Plus opens up new avenues for users. With this option, businesses and private individuals can access enhanced features, ensuring reliable and specialized responses for users seeking a higher level of engagement and accuracy in their interactions²⁴. The use of RLHF and the introduction of ChatGPT Plus are proactive responses to the incorrect or biased responses that the model sometimes gives due to the biases present in its training data²⁵.

Since ChatGPT has been gaining worldwide attention due to its various capabilities and existing/possible fields of application²⁶, this research focuses on investigating its implementation in the intelligence analysis field. Specifically, it aims to explore how ChatGPT can be used to support the analysis of competing hypothesis (ACH), an SAT for minimising cognitive bias. Instead of beginning with the most probable hypothesis, this method requires analysts to generate an exhaustive list of plausible alternatives. Analysts subsequently evaluate the consistency or inconsistency of each pertinent piece of information with each hypothesis. The goal is to disprove hypotheses by indicators rather than confirming them²⁷. Thus, the significance of this research lies in its potential to enhance and streamline intelligence analysis practices. Traditional intelligence analysis often relies on limited human cognitive capacities, which might hinder the ability to consider a wide range of hypotheses or process vast amounts of information efficiently and in a short period of time. ChatGPT could enable analysts to explore diverse scenarios and formulate hypotheses that might otherwise have been overlooked in a traditional analysis.

Method – ChatGPT and ACH

In this section, the methodology employed to assess how ChatGPT can support ACH is described. The experiment for this study was designed to investigate ChatGPT's ability to generate alternative hypotheses, refine them, and provide

²³ H. Chen, K. Yuan, Y. Huang, L. Guo, Y. Wang, J. Chen, *Feedback is all you need: from ChatGPT to autonomous driving*, "Science China Information Sciences" 2023, 66(6), p. 1–3.

²⁴ S. Vaughan-Nichols, *GPT-3.5 vs GPT-4: Is chatgpt plus worth its subscription fee?*, "ZDNET" 2023, <https://www.zdnet.com/article/gpt-3-5-vs-gpt-4-is-chatgpt-plus-worth-its-subscription-fee/> (Access: 10 October 2023).

²⁵ E.A. Van Dis, J. Bollen, W. Zuidema, R. van Rooij, R., C.L. Bockting, *ChatGPT: five priorities for research*, "Nature" 2023, 614(7947), p. 224–226.

²⁶ See: S.S. Biswas, *Role of chat gpt in public health*, "Annals of Biomedical Engineering" 2023, p. 1–2; M. Firat, *How chat GPT can transform autodidactic experiences and open education*, Department of Distance Education, Open Education Faculty, Anadolu Unive, 2023; M. Sallam, *ChatGPT utility in healthcare education, research, and practice: Systematic review on the promising perspectives and valid concerns*, "Healthcare" 2023, 11(6).

²⁷ R.H. Pherson, R.J. Heuer Jr., *Structured analytic techniques for intelligence analysis*, Cq Press, 2000.

relevant indicators for each hypothesis. The study was conducted using three different ChatGPT accounts with a functioning internet connection, aiming to verify the consistency – if the hypothesis was logically constructed per se – and plausibility – if the hypothesis was valid from an empirical point of view – of the results across platforms. Two test runs – *Test 1* and *Test 2* – used the free version of ChatGPT, and the third one – *Test 3* – used the ChatGPT Plus version. This choice was made for enabling a comparison not only between accounts but also between the two ChatGPT models. The experiment was structured into three sequential phases – *hypotheses generation*, *hypotheses specification*, and *indicators generation*.

The first stage aimed at assessing ChatGPT's ability to provide diverse and relevant hypotheses. To do so, it was necessary to provide the model with a so-called prompt or task. With the case study chosen for the analysis being North-East Nigeria, with a focus on internally displaced persons (IDPs), the prompt for the first phase was:

Hello! I have the following research question: "What is the leading cause of IDPs in North-East Nigeria?". My hypothesis is the following: "Boko Haram is the major cause for IDPs in North-East Nigeria". Could you please generate three competing hypotheses that could answer our research question?

Following the generation of alternative hypotheses, the second prompt asked ChatGPT to refine the hypotheses in order to evaluate its capacity to enhance their specificity. Thus, the second prompt was:

Could you please formulate the hypotheses more precisely?

In the final stage, the prompt aimed to assess ChatGPT's ability to identify pertinent indicators that could aid intelligence analysts in evaluating the viability of each hypothesis. Thus, the following prompt was formulated for each hypothesis:

Could you please give me a list of indicators to monitor in order to try and disprove the hypothesis 1?

Data collection involved collecting the responses provided by ChatGPT for each question of the experiment. It was essential to acknowledge that the quality of the responses was contingent on the training data it had received up until its last update – June 2021 for the free version and September 2021 for the plus version²⁸ – and therefore, it lacked the most recent information or developments related to North-East Nigeria.

²⁸ L. Frady, *Chat GPT-4 vs Chat GPT-3: What's the Difference, and Which Is Better?*, 2023, <https://history-computer.com/chat-gpt-4-vs-chat-gpt-3/> (Access: 10 October 2023).

Findings and Discussion

Hypotheses generation

The hypotheses provided by ChatGPT in response to the first prompt are reported in Table 1 (see also Annex 1).

Table 1. Hypotheses generated by ChatGPT after the first input for all subjects

Test 1	Test 2	Test 3
<p>Economic Factors: Socio-economic conditions and poverty levels are the leading cause of IDPs in North-East Nigeria. This hypothesis suggests that factors such as lack of employment opportunities, limited access to education and healthcare, and economic instability contribute significantly to the displacement of people in the region. It argues that the root cause of displacement is primarily tied to economic struggles rather than solely the activities of Boko Haram.</p>	<p>Environmental factors hypothesis: Environmental factors, such as natural disasters or climate change-related issues, are the primary cause of IDPs in North-East Nigeria. This hypothesis suggests that events like floods, droughts, or desertification have displaced people from both their homes and communities, leading to the formation of IDP camps.</p>	<p>Environmental Factors Hypothesis: This hypothesis would suggest that environmental factors such as climate change, desertification, drought are the leading causes of IDP situations in North-East Nigeria. These environmental challenges could be forcing people to leave their homes in search of more hospitable areas, impacting agriculture, and leading to food insecurity.</p>
<p>Conflict Dynamics: This hypothesis proposes that while Boko Haram plays a significant role in causing displacement in North-East Nigeria, it is not the sole or major cause. It suggests that a combination of various conflict dynamics, including inter-communal clashes, resource disputes, and other armed groups' activities, contribute to the high number of IDPs in the region. It argues that a comprehensive understanding of the conflict landscape is necessary to address the root causes of displacement effectively.</p>	<p>Government response hypothesis: Inadequate government response and governance issues are the major cause of IDPs in North-East Nigeria. This hypothesis posits that the government's failure to address socio-economic disparities, provide security, and implement effective policies has resulted in widespread conflict and forces displacement.</p>	<p>Ethnic and Religious Conflicts Hypothesis: This hypothesis posits that ethnic and religious tensions and conflicts in North-East Nigeria, independent of Boko Haram's activities, are a major cause of internal displacement. These conflicts might arise from historical, cultural, or resource-related disputes between different ethnic or religious groups.</p>

Table 1 (cont.). Hypotheses generated by ChatGPT after the first input for all subjects

Test 1	Test 2	Test 3
Government Response and Policies: This hypothesis argues that the inadequate response of the Nigerian government and ineffective policies aimed at preventing displacement are the primary cause of IDPs in North-East Nigeria. It suggests that insufficient security measures, inadequate provision of basic services, and a lack of sustainable development initiatives contribute to the displacement of people. This hypothesis highlights the importance of examining governance and policy failures in addressing the issue of internal displacement.	Ethno-religious conflicts hypothesis: Intercommunal and ethno-religious conflicts, rather than solely Boko Haram activities, are the main cause of IDPs in North-East Nigeria. This hypothesis suggests that tensions between different ethnic and religious groups, fueled by competition over resources or historical grievances, have contributed significantly to the displacement of people in the region.	Economic Hardship and Lack of Infrastructure Hypothesis: Under this hypothesis, the primary cause of internal displacement is attributed to economic hardship and lack of basic infrastructure. Factors like poverty, unemployment, lack of access to education and health services, and poor infrastructure could be compelling people to leave their homes in search of better opportunities and living conditions elsewhere.

The analysis revealed that ChatGPT's hypotheses are of limited use due to their demonstrated flaws, such as disjunction and incoherence, which are illustrated with examples in the following section. At first glance, it is visible that ChatGPT's responses always included a brief explanation of the hypotheses as well. Despite the same prompts in all three test runs, the length of the responses differed in some cases.

For example, the lack of adequate security is mentioned in the explanation of the third hypothesis of Test 1 – “Government response and policies” – and the second hypothesis of Test 2 – “Government response hypothesis”; however, none of these hypotheses furnish a sufficient delineation of the nature of these security breaches. The hypotheses fail to account for the North-East Nigerian context of internally displaced persons, and the results appear to lack nuance; thus, it is not possible to test any of these hypotheses. It is noteworthy that both hypotheses present a tautological issue: both of them provide a problem-solving justification, suggesting what should be taken into account in addressing the problem. Nonetheless, this is not what it is required during the stage of hypotheses generation. In addition, the “Government response and policies” hypothesis is not valid since it claims the “policies aimed at preventing displacement” are a major cause of the current situation when in reality they are the government's response to it.

Similarly, the second hypothesis of Test 1 – “Conflict Dynamics” – states that “a comprehensive understanding of the conflict landscape is necessary to address the root causes of displacement”. This provides a procedural and redundant assessment to the analyst instead of an actual hypothesis. The presence of conflicts as the

leading cause of IDPs has been provided also during the second test run – “Ethno-religious conflicts hypothesis” – and the third one – “Ethnic and Religious Conflicts Hypothesis”. However, these two hypotheses are not consistent because they are not disjunct, which is an essential criterion for sound hypotheses. Disjunction means that each hypothesis should present a distinct and exclusive explanation for the observed phenomenon or problem²⁹. This ensures that the hypotheses are independent of each other, preventing overlap and ambiguity in their interpretations. By including both ethnic and religious conflicts these hypotheses are not disjunct, therefore they are not consistent. Furthermore, the “Ethnic and Religious Conflicts Hypothesis” states that these disputes are “independent of Boko Haram’s activities”, presenting a tautological problem. Since Boko Haram is a religious group it cannot be taken out of the explanation, hence this hypothesis lacks plausibility.

ChatGPT also provided economic hypotheses, which it referred to as “Economic Factors” during Test 1 and “Economic Hardship and Lack of Infrastructure Hypothesis” during Test 3. However, from an analyst’s point of view, none of these hypotheses would be of any use to a sound analysis. The hypothesis provided during Test 1 is not consistent. By stating that “factors such as lack of employment opportunities, limited access to education and healthcare, and economic instability” contribute to IDPs it confuses the causes and effects, since “economic instability” is an effect of the previously mentioned factors. On the other hand, the hypothesis provided during Test 3 is also not disjunct since it includes both economic struggles and infrastructure deficiencies.

Lastly, ChatGPT identified environmental hypotheses during Test 2 and Test 3. Both, however, showed similar issues to the previously discussed hypotheses. Regarding the second test run, the last sentence of the provided hypothesis gives an assessment of the situation while including both causes – “floods, droughts, or desertification” – and consequences – “formation of IDP camps” in the explanation. Therefore, it is not consistent. Comparatively, the hypothesis generated during the third test run presents the same issues because the last sentence adds an extra layer of detail, highlighting the broader implications of environmental factors on the livelihoods and well-being of the affected population. It not only gives an assessment but also includes causes – “forcing people to leave their homes” – as well effects – “impacting agriculture, and leading to food insecurity”, which is problematic for an analyst to work with.

All factors mentioned in the hypotheses can be valid within the North-Eastern Nigerian setting. Nonetheless, the AI model neglects to provide further details regarding the complexities of the situation, as it solely mentions Boko Haram, which was the group name provided in the first input. Moreover, there is a lack of consistency, plausibility, or both, in the structure of the outputs and their corresponding explanations. As a result, the analyst may employ the recommended factors;

²⁹ R.J. Heuer Jr., R.H. Pherson, *Structured analytic...*, *op.cit.*

however, to ensure plausibility and consistency, the hypotheses should be re-phrased.

Hypotheses specification

Regarding the second phase, the results are reported in Table 2 (see also Annex 2).

It can be noticed that the outcomes maintained a similar word count and response structure compared to the outputs of the previous stage. Nevertheless, the results obtained during this stage fall short of surmounting the constraints of the initial stage for both the free and Plus version.

Table 2. Hypotheses specified by ChatGPT after the second input for all subjects

Test 1	Test 2	Test 3
Economic Factors Hypothesis: Socio-economic conditions and poverty levels are the primary drivers of internal displacement in North-East Nigeria. This hypothesis contends that factors such as high unemployment rates, limited access to education and healthcare, and economic instability significantly contribute to the displacement of individuals in the region, overshadowing the impact of Boko Haram activities.	Environmental factors hypothesis: Environmental factors, such as recurring floods, droughts, or desertification, are the primary drivers of internal displacement in North-East Nigeria. This hypothesis suggests that the frequency and severity of natural disasters in the region have forced people to flee their homes and seek refuge in IDP camps.	Environmental Degradation Hypothesis: "The primary cause of internal displacement in North-East Nigeria is environmental degradation, including factors such as climate change-induced desertification, soil erosion, and recurrent droughts, which significantly impact agricultural productivity and livelihoods, leading to mass displacement of populations in search of more living conditions."
Conflict Dynamics Hypothesis: Boko Haram, along with other armed groups and inter-communal clashes, collectively account for the majority of internal displacement in North-East Nigeria. This hypothesis argues that a combination of conflict dynamics, including activities of Boko Haram, inter-group conflicts, and resource disputes, plays a crucial role in causing displacement, suggesting that a comprehensive understanding of the broader conflict landscape is necessary.	Government response hypothesis: Inadequate government response and governance issues contribute significantly to the formation of IDPs in North-East Nigeria. This hypothesis posits that the government's failure to address socio-economic disparities, provide effective security measures, and implement policies for conflict resolution has resulted in widespread displacement of the population.	Ethnic and Religious Conflict Hypothesis: "Internal displacement in North-East Nigeria is predominantly caused by ongoing ethnic and religious conflicts, independent of Boko Haram's insurgency. These conflicts are rooted in historical, cultural, or socio-economic disparities and competition for resources, leading to frequent clashes and the displacement of communities caught in these conflicts."

Table 2 (cont.). Hypotheses specified by ChatGPT after the second input for all subjects

Test 1	Test 2	Test 3
Government Response and Policies Hypothesis: Inadequate government response and ineffective policies aimed at preventing displacement are the primary factors contributing to the high number of IDPs in North-East Nigeria. This hypothesis posts that insufficient security measures, inadequate provision of basic services, and a lack of sustainable development initiatives by the Nigerian government contribute significantly to internal displacement, suggesting that governance and policy failures must be addressed to tackle the root causes of the issue.	Ethno-religious conflicts hypothesis: Intercommunal and ethno-religious conflicts, alongside the activities of Boko Haram, are the major causes of internal displacement in North-East Nigeria. This hypothesis suggests that tensions and violence between different ethnic and religious groups, fueled by competition over resources, political power, or historical grievances, have played a significant role in the displacement of people and the formation of IDP camps.	Economic and Infrastructure Deficiency Hypothesis: "The leading cause of internal displacement in North-East Nigeria is the region's severe economic hardship and lack of essential infrastructure. Factors such as pervasive poverty, high unemployment rates, inadequate access to education and healthcare, and poor transportation and communication infrastructure are compelling residents to migrate internally in search of better socio-economic opportunities."

The outputs provided by ChatGPT contained the same flaws – e.g., disjunction, tautological issues – that were present during the previous hypotheses generation phase. Therefore, this section concentrates only on one additional example to highlight the existing problems, since the specification merely modified the structure of the sentences, while leaving the contents of the six hypotheses unchanged from the preceding section.

For instance, the third hypothesis of the third test run changed from "Economic Hardship and Lack of Infrastructure Hypothesis" to "Economic and Infrastructure Deficiency Hypothesis". The phrasing in both hypotheses varies in capturing the essence of why people are compelled to migrate. The first hypothesis suggests that economic hardship and poor infrastructure are "compelling people to leave their homes", focusing on individual agency. On the other hand, the second hypothesis phrases economic hardship as "compelling residents to migrate internally", which implies a more collective or community-driven aspect to the internal migration phenomenon. In terms of structural presentation, the second hypothesis adopts a more formal style by enclosing the hypothesis in quotation marks. This formatting choice lends an air of authority, resembling a direct quote or a formal proposition. Nevertheless, while the expression of the same hypothesis differs between the two results, the specified hypothesis is still not consistent due to the fact that it is not disjunct.

In essence, in the specification stage, the nuances in phrasing, emphasis, and structural presentation contribute to distinctions in tone, formality, and the conveyed perception of the internal displacement phenomenon. Nonetheless, an

analyst could not use these hypotheses per se due to a lack of consistency, plausibility, or both.

Indicators generation

As regards the indicators generated for each hypothesis, they can be seen in Annex 3.

The outputs pertaining to identical inquiries provided during the three test runs varied in the quantity of indicators. During the first test run, ChatGPT provided six potential indicators for each hypothesis, while in the second test run, it generated five. It is noteworthy that an intelligence analyst might require looking into several types of potential indicators, which, ideally, should differ for each hypothesis. However, ChatGPT places a lower priority on the number of outputs than on the number of indicators required to prove or disprove a hypothesis. This is apparent from the fact that it consistently generates the same number of outputs for all inputs on one computer, but it is not consistent over devices. Regarding the third test run, the Plus version gave 10 indicators for each hypothesis, therefore suggesting a more comprehensive analysis compared to the other subjects. This discrepancy in the number of indicators highlights the adaptability of ChatGPT in tailoring its responses based on different input conditions. The variation in output prioritization across devices underscores the complexity of the model's decision-making process.

The three hypotheses generated by ChatGPT during each test run were supposed to compete with the initial input hypothesis "Boko Haram is the major cause of IDPs in North-East Nigeria". Nonetheless, within the indicators of these conflicting hypotheses, there is limited reference to other actors, such as the United Nations, INTERSOS, and Solidarités International; instead, a broad spectrum of actors is mentioned, which could be considered implicated not only in this particular situational context but in various conflict contexts which lead to IDPs, such as in Sudan, Syria, and Democratic Republic of Congo³⁰. ChatGPT uses terminologies such as civil society, NGOs, other armed groups, and local authorities. In addition, the output makes numerous references to Boko Haram while neglecting to mention any other non-state actors involved in the conflict. It also contradicts itself by suggesting that analysts contact the local government to inquire about the government's failings to provide adequate governance for the people in their region.

Some indicators have been repeated for different hypotheses during the same test run. For instance, during Test 1, the indicator "security measures" was proposed for both hypothesis 1 and hypothesis 3, generally suggesting monitoring the effectiveness of the adopted security practices. While this indicator might be appropriate for the "Government Response and Policies Hypothesis", it does not fit for monitoring economic factors. Additionally, other outputs provided a method rather than an indicator, hindering the plausibility of the result. This can be noticed

³⁰ UNHCR (2022), *GLOBAL TRENDS – FORCED DISPLACEMENT IN 2022*, <https://www.unhcr.org/sites/default/files/2023-06/global-trends-report-2022.pdf> (Access: 10 October 2023).

in the list generated for the second hypothesis during the Test 3, in which the last two indicators are named “Comparative Analysis with Non-conflict Areas” and “Analysis of Historical Conflict Pattern”.

Other indicators suggest the presence of correlation as causality. For example, “If there is significant humanitarian aid and support available, yet internal displacement rates remain high, it suggests that systemic issues beyond immediate humanitarian response are contributing to the problem” (Test 1, hypothesis 3); or in indicator “conflict hotspots”. The presence of significant humanitarian aid correlated with high IDPs numbers, merely “suggests” systemic issues but it is not sufficient to disprove a certain hypothesis. In order to disprove a hypothesis, smoking gun evidence must be presented in opposition to it; in its absence, the hypothesis could always remain valid. Trends that could be utilised to disprove the hypothesis are identified by ChatGPT’s recommendations; when utilised in conjunction, they invariably bolster the argument. The situational context and specifics are omitted from the indicators, which instead present broad possibilities.

Nonetheless, the indicators generated by the Plus version tend to be more detailed. This can be noticed in the environmental factors hypothesis, generated during the second and third test runs. In examining the hypothesis that environmental factors are the primary drivers of internal displacement in North-East Nigeria, a comprehensive set of indicators is proposed in Test 2. By including factors beyond environmental issues, such as conflict dynamics and socio-economic disparities, the given indicators seek to provide a nuanced understanding of the causes of internal displacement. Challenging the hypothesis of environmental degradation as the primary cause of internal displacement, the output for Test 3 recommends a focused examination of specific indicators, e.g., rates of desertification, changes in agricultural productivity, water availability. It adopts a targeted approach, homing in on environmental metrics to assess their impact on displacement and highlighting the need to scrutinize these factors.

However, ChatGPT Plus sometimes emulates the shortcomings of the free version. While it is specific in some of the indicators it presents, for Hypothesis 2, for example, it resorts back to broad indicators such as “Socio-economic indicators in conflict areas”. This shows that the software has limited ability to reflect critically after a certain point in both of its versions. Furthermore, it does not mention region-specific indicators, but rather focuses on broad data that would be applicable to a conflict-ridden region, which could potentially lead to biased assumptions. Therefore, while the Plus version has some advantages, it still does not help an analyst to make informed decisions, while it might provide directions for research. For informed quality strategic forecasting, an analyst would still need to rely on traditional methods.

The AI model has been specifically engineered to utilise its information database in order to provide the requested information in a concise yet correct manner. This is reflected in the responses provided. Nevertheless, by eliminating the situational contexts, it might lead to misinformation of users.

Limitations

The study highlights concerns regarding ChatGPT's suitability for supporting intelligence analysis, emphasizing potential inaccuracies due to its reliance on a pre-existing dataset, resulting in outdated or contextually inadequate information. Issues such as inconsistency, lack of uniformity in outputs, and the implication of correlation as causality raise important considerations, requiring additional scrutiny and verification processes by analysts to ensure the quality of hypotheses and indicators.

Firstly, while the study explores the potential of ChatGPT as a tool for supporting intelligence analysis, it's essential to acknowledge that ChatGPT's responses are based on a vast but pre-existing dataset. This dataset does not always encompass the most recent or context-specific information. Consequently, there is a risk that the hypotheses and indicators generated by ChatGPT may not accurately reflect the dynamic and evolving nature of real-world situations. Analysts relying on ChatGPT might be presented with information that is either outdated or fails to account for rapidly changing circumstances, which can compromise the reliability of their assessments.

One significant concern is the quality and depth of the hypotheses and indicators provided by ChatGPT. Even when provided with the same input, the outputs for different subjects exhibit disparities in content and length. This lack of uniformity could impede the comparability of results between subjects. The study reveals that ChatGPT's responses frequently lack consistency and plausibility, indicating that the tool might not always deliver adequate or useful results. Analysts using ChatGPT may need to adopt additional scrutiny and verification processes to ensure the quality of the hypotheses and indicators it produces, specifically considering the vagueness of the outputs. Despite the confinement of the research to a single case study – North-East Nigeria – it is possible to generalise the provided responses for most conflict cases, showing a lack of specificity.

Another noteworthy limitation is that ChatGPT sometimes implies correlation as causality in its recommendations. The study demonstrates instances where the tool suggests that specific indicators correlate with certain outcomes, but it does not provide conclusive evidence of causation. This can lead to erroneous assumptions and the misinterpretation of data, potentially affecting the quality of intelligence analysis. Consequently, further investigation is often required to establish causal relationships.

Conclusions

In conclusion, the intersection of artificial intelligence and intelligence analysis marks a significant evolution in the way we perceive, interpret, and respond to complex global challenges. This study delved into the potential of leveraging ChatGPT, an advanced AI tool, to enhance the strategic forecasting

process for intelligence analysts, specifically focusing on the analysis of competing hypotheses in the context of North-East Nigeria. The exploration of AI applications in the realm of intelligence analysis is pivotal, given the ever-expanding landscape of threats and the critical need for accurate, timely, and actionable insights. The advent of AI technologies, particularly ChatGPT, offers promising avenues to augment the capabilities of human analysts. ChatGPT's ability to handle vast volumes of unstructured data, generate hypotheses, and suggest relevant indicators represents a paradigm shift in the analytical process.

However, the study also shed light on the limitations inherent in AI-driven intelligence analysis. Despite ChatGPT's abilities, it is crucial to acknowledge the constraints of its training data, which might lack the most recent or context-specific information. Consequently, the hypotheses and indicators generated by ChatGPT may not always align with the dynamic and evolving nature of real-world situations. This limitation emphasises the need for analysts to exercise discernment, cross-verify results, and contextualize AI-generated insights within the broader socio-political landscape.

The findings of this study revealed notable shortcomings in ChatGPT's responses. While the AI model provided diverse hypotheses, it lacked the contextual depth necessary for a more precise analysis. Linguistic variations and inconsistencies in generated responses highlighted the challenge of ensuring uniformity and accuracy, a critical aspect in the field of intelligence where standardized methodologies are paramount.

Furthermore, the lack of consistency and plausibility of the hypotheses as well as ChatGPT's tendency to imply correlation as causality in its recommendations pose a major pitfall. Analysts must be vigilant in analysing the outputs and distinguishing between correlation and causation to prevent misinterpretation of data and erroneous assumptions. The study underscored the importance of critically evaluating ChatGPT-generated indicators, emphasizing the need for thorough investigation to verify causal relationships.

A notable aspect of the study was the comparison between the free and Plus versions of ChatGPT. Despite some expectations of significant differences, the outputs of the Plus version did not markedly surpass those of the free version in terms of content or length. While there were minor variations in language and structure, the Plus version did not consistently outperform the free version. This suggests that, at least in the context of this study, the additional features of the Plus version might not significantly enhance the tool's performance in generating more context-specific, detailed, consistent and plausible hypotheses.

Despite these limitations, the integration of AI, exemplified by ChatGPT, in intelligence analysis offers a transformative potential. Enhancing the timeliness of the data that ChatGPT uses is likely to contribute to a substantial improvement in its results. Furthermore, a crucial enhancement involves augmenting the model's comprehension of cause and effect, which would result in improved outputs. Anticipating future breakthroughs in both aspects is a reasonable expectation, which

underscores the importance for analysts to remain informed about ChatGPT innovations. This will ensure ongoing enhancements in efficiency and reliability. The iterative refinement process, enabled by ChatGPT's reinforcement learning from human feedback (RLHF) mechanism, showcases a proactive method for tackling biases and improving accuracy, suggesting a trajectory towards ongoing enhancement and reliability.

In the broader context, this study serves as a foundation for future research endeavours, emphasising the imperative of refining AI models, enhancing training datasets, and developing standardized protocols for integrating AI tools effectively into intelligence analysis processes. As the field of AI continues to advance, collaboration between human analysts and AI systems will play a pivotal role in shaping a more secure, informed, and resilient global landscape.

Annex 1 – Hypotheses Generation

Test 1

1. **Economic Factors:** Socio-economic conditions and poverty levels are the leading cause of IDPs in North-East Nigeria. This hypothesis suggests that factors such as lack of employment opportunities, limited access to education and healthcare, and economic instability contribute significantly to the displacement of people in the region. It argues that the root cause of displacement is primarily tied to economic struggles rather than solely the activities of Boko Haram.
2. **Conflict Dynamics:** This hypothesis proposes that while Boko Haram plays a significant role in causing displacement in North-East Nigeria, it is not the sole or major cause. It suggests that a combination of various conflict dynamics, including inter-communal clashes, resource disputes, and other armed groups' activities, contributes to the high number of IDPs in the region. It argues that a comprehensive understanding of the conflict landscape is necessary to address the root causes of displacement effectively.
3. **Government Response and Policies:** This hypothesis argues that the inadequate response of the Nigerian government and ineffective policies aimed at preventing displacement are the primary cause of IDPs in North-East Nigeria. It suggests that insufficient security measures, inadequate provision of basic services, and lack of sustainable development initiatives contribute to the displacement of people. This hypothesis highlights the importance of examining governance and policy failures in addressing the issue of internal displacement.

These three competing hypotheses provide alternative explanations for the leading cause of IDPs in North-East Nigeria, beyond the focus on Boko Haram as the primary factor. Exploring these different perspectives can help provide a comprehensive understanding of the complex dynamics at play and guide future research and interventions.

Test 2



Certainly! Here are three competing hypotheses that could provide alternative explanations for the leading cause of internally displaced persons (IDPs) in North-East Nigeria.

1. **Environmental factors hypothesis:** Environmental factors, such as natural disasters or climate change-related issues, are the primary cause of IDPs in North-East Nigeria. This hypothesis suggests that events like floods, droughts, or desertification have displaced people from their homes and communities, leading to the formation of IDP camps.
2. **Government response hypothesis:** Inadequate government response and governance issues are the major cause of IDPs in North-East Nigeria. This hypothesis posits that the government's failure to address socio-economic disparities, provide security, and implement effective policies has resulted in widespread conflict and forced displacement.
3. **Ethno-religious conflicts hypothesis:** Intercommunal and ethno-religious conflicts, rather than solely Boko Haram activities, are the main cause of IDPs in North-East Nigeria. This hypothesis suggests that tensions between different ethnic and religious groups, fueled by competition over resources or historical grievances, have contributed significantly to the displacement of people in the region.

It is important to explore these competing hypotheses to gain a comprehensive understanding of the complex factors contributing to the high number of IDPs in North-East Nigeria. Conducting further research and analysis can help evaluate the validity and relative significance of each hypothesis.

Test 3



Certainly! To generate alternative hypotheses for the leading causes of internally displaced persons (IDPs) in North-East Nigeria, apart from the influence of Boko Haram, you could consider the following:

1. **Environmental Factors Hypothesis:** This hypothesis would suggest that environmental factors such as climate change, desertification, and drought are the leading causes of IDP situations in North-East Nigeria. These environmental challenges could be forcing people to leave their homes in search of more hospitable areas, impacting agriculture, and leading to food insecurity.
2. **Ethnic and Religious Conflicts Hypothesis:** This hypothesis posits that ethnic and religious tensions and conflicts in North-East Nigeria, independent of Boko Haram's activities, are a major cause of internal displacement. These conflicts might arise from historical, cultural, or resource-related disputes between different ethnic or religious groups.
3. **Economic Hardship and Lack of Infrastructure Hypothesis:** Under this hypothesis, the primary cause of internal displacement is attributed to economic hardship and lack of basic infrastructure. Factors like poverty, unemployment, lack of access to education and health services, and poor infrastructure could be compelling people to leave their homes in search of better opportunities and living conditions elsewhere.

Each of these hypotheses offers a different perspective on the complex and multifaceted issue of internal displacement in North-East Nigeria, and investigating them could provide a more comprehensive understanding of the situation.

Annex 2 – Hypotheses specification

Test 1

1. **Economic Factors Hypothesis:** Socio-economic conditions and poverty levels are the primary drivers of internal displacement in North-East Nigeria. This hypothesis contends that factors such as high unemployment rates, limited access to education and healthcare, and economic instability significantly contribute to the displacement of individuals in the region, overshadowing the impact of Boko Haram activities.
2. **Conflict Dynamics Hypothesis:** Boko Haram, along with other armed groups and inter-communal clashes, collectively account for the majority of internal displacement in North-East Nigeria. This hypothesis argues that a combination of conflict dynamics, including the activities of Boko Haram, inter-group conflicts, and resource disputes, plays a crucial role in causing displacement, suggesting that a comprehensive understanding of the broader conflict landscape is necessary to address the issue effectively.
3. **Government Response and Policies Hypothesis:** Inadequate government response and ineffective policies aimed at preventing displacement are the primary factors contributing to the high number of IDPs in North-East Nigeria. This hypothesis posits that insufficient security measures, inadequate provision of basic services, and a lack of sustainable development initiatives by the Nigerian government contribute significantly to internal displacement, suggesting that governance and policy failures must be addressed to tackle the root causes of the issue.

These refined hypotheses provide more precise statements for each perspective, allowing for clearer investigation and analysis of the leading cause of IDPs in North-East Nigeria.

Test 2

1. **Environmental factors hypothesis:** Environmental factors, such as recurring floods, droughts, or desertification, are the primary drivers of internal displacement in North-East Nigeria. This hypothesis suggests that the frequency and severity of natural disasters in the region have forced people to flee their homes and seek refuge in IDP camps.
2. **Government response hypothesis:** Inadequate government response and governance issues contribute significantly to the formation of IDPs in North-East Nigeria. This hypothesis posits that the government's failure to address socio-economic disparities, provide effective security measures, and implement policies for conflict resolution has resulted in widespread displacement of the population.
3. **Ethno-religious conflicts hypothesis:** Intercommunal and ethno-religious conflicts, alongside the activities of Boko Haram, are the major causes of internal displacement in North-East Nigeria. This hypothesis suggests that tensions and violence between different ethnic and religious groups, fueled by competition over resources, political power, or historical grievances, have played a significant role in the displacement of people and the formation of IDP camps.

Test 3



Certainly! To formulate the hypotheses more precisely, let's refine them:

1. **Environmental Degradation Hypothesis:** "The primary cause of internal displacement in North-East Nigeria is environmental degradation, including factors such as climate change-induced desertification, soil erosion, and recurrent droughts, which significantly impact agricultural productivity and livelihoods, leading to mass displacement of populations in search of more sustainable living conditions."
2. **Ethnic and Religious Conflict Hypothesis:** "Internal displacement in North-East Nigeria is predominantly caused by ongoing ethnic and religious conflicts, independent of Boko Haram's insurgency. These conflicts are rooted in historical, cultural, or socio-economic disparities and competition for resources, leading to frequent clashes and the displacement of communities caught in these conflicts."
3. **Economic and Infrastructure Deficiency Hypothesis:** "The leading cause of internal displacement in North-East Nigeria is the region's severe economic hardship and lack of essential infrastructure. Factors such as pervasive poverty, high unemployment rates, inadequate access to education and healthcare, and poor transportation and communication infrastructure are compelling residents to migrate internally in search of better socio-economic opportunities."

These refined hypotheses provide a clearer and more specific understanding of potential causes behind the internal displacement crisis in North-East Nigeria, apart from the impact of Boko Haram.

Annex 3 – Indicators generation

Test 1, Hypothesis 1



Certainly! To monitor and potentially disprove the hypothesis that socio-economic conditions and poverty levels are the primary drivers of internal displacement in North-East Nigeria (Hypothesis 1), you can consider the following indicators:

1. **Education Access:** Monitor the availability and accessibility of educational facilities, including schools, teachers, and resources in the affected areas. If education infrastructure and opportunities improve while internal displacement persists or increases, it suggests that other factors beyond economic conditions may be contributing significantly to displacement.
2. **Employment Opportunities:** Track employment rates, job availability, and economic opportunities in the region. If employment opportunities increase or economic conditions improve, but internal displacement remains high, it indicates that socio-economic factors may not be the sole cause.
3. **Poverty Levels:** Analyze poverty rates, income inequality, and access to basic necessities such as food, water, and shelter. If poverty rates decrease or poverty alleviation efforts show positive results, but internal displacement continues or even rises, it suggests that other factors might be more influential.
4. **Security Measures:** Monitor the effectiveness of security measures and counter-terrorism efforts against Boko Haram. If significant progress is made in curbing the activities of Boko Haram, resulting in a decline in violence and attacks, yet internal displacement persists, it indicates that factors beyond Boko Haram's actions are contributing to the displacement.
5. **Socio-economic Development:** Assess the implementation and impact of development programs and initiatives aimed at addressing socio-economic challenges in the region. If substantial efforts are made to improve socio-economic conditions, but internal displacement rates do not significantly decrease, it suggests that other factors are playing a significant role.
6. **Local Perspectives:** Gather qualitative data through surveys, interviews, or focus group discussions with IDPs and local communities. Explore their experiences, perceptions, and reasons for displacement, paying attention to the factors they identify beyond economic conditions.

Test 1, Hypothesis 2

1. **Boko Haram Activities:** Monitor the intensity, frequency, and geographical spread of Boko Haram attacks and insurgent activities. If Boko Haram experiences a significant decline or is successfully neutralized, yet internal displacement rates remain high, it suggests that other factors beyond Boko Haram's actions may be contributing significantly to displacement.
2. **Inter-communal Clashes:** Track instances of inter-communal conflicts and their impact on displacement. If inter-communal clashes decrease or cease, but internal displacement persists or increases, it indicates that factors beyond inter-communal clashes are playing a more significant role.
3. **Other Armed Groups:** Assess the presence and activities of other armed groups operating in the region. Monitor their engagement in violent activities and their impact on displacement. If other armed groups emerge or become more active, contributing to displacement, it suggests that Boko Haram alone may not be the primary driver of internal displacement.
4. **Resource Disputes:** Monitor conflicts related to access and control of resources such as land, water, and minerals. Analyze their impact on displacement, particularly if resource disputes persist or escalate even if Boko Haram activities decrease.
5. **Collaboration and Coordination:** Assess the level of collaboration and coordination among armed groups and their alliances. If there is evidence of alliances or collaborations that go beyond Boko Haram and contribute to displacement, it challenges the notion that Boko Haram is the sole major cause.
6. **Conflict Hotspots:** Identify geographical areas with a high incidence of displacement and analyze the specific conflict dynamics present in those areas. If certain areas experience displacement even in the absence of significant Boko Haram presence, it indicates the influence of other conflict dynamics.

Test 1, Hypothesis 3

1. **Security Measures:** Monitor the effectiveness of government security measures in countering the activities of Boko Haram and other armed groups. If the government demonstrates significant progress in maintaining security and reducing violence, yet internal displacement rates remain high, it suggests that factors beyond security measures are contributing to displacement.
2. **Provision of Basic Services:** Assess the government's ability to provide essential services such as healthcare, education, clean water, and infrastructure in the affected areas. If there are improvements in service delivery, but internal displacement persists or increases, it indicates that other factors may have a stronger influence.
3. **Humanitarian Assistance:** Monitor the presence and effectiveness of humanitarian organizations and their efforts in addressing the needs of IDPs. If there is significant humanitarian aid and support available, yet internal displacement rates remain high, it suggests that systemic issues beyond immediate humanitarian response are contributing to the problem.
4. **Policy Implementation:** Assess the implementation and impact of government policies and programs aimed at addressing displacement and promoting sustainable development. If policies are well-designed and adequately resourced, but internal displacement rates do not significantly decrease, it indicates that other factors may be more influential.
5. **Governance and Accountability:** Monitor the level of transparency, accountability, and governance effectiveness in the affected regions. Assess the government's ability to address corruption, provide equitable resource allocation, and engage with local communities. If governance failures persist or worsen despite government efforts, it suggests that governance issues may play a larger role in displacement.
6. **Stakeholder Perceptions:** Gather qualitative data through interviews, surveys, or focus group discussions with IDPs, local communities, and civil society organizations. Explore their perspectives on government response, policies, and governance, paying attention to the factors they identify as contributing to displacement beyond government failures.

Test 2, Hypothesis 1

1. **Conflict incidents:** Monitor the occurrence and frequency of conflict incidents, including Boko Haram attacks, communal clashes, and violence between different ethnic or religious groups. If conflict-related factors consistently overshadow environmental factors in triggering displacement, it would challenge the hypothesis.
2. **Humanitarian reports:** Analyze reports from humanitarian organizations and agencies working in the region. Look for evidence of the causes of displacement cited in their assessments, such as interviews with IDPs, community leaders, or local authorities. If conflict-related factors consistently emerge as the main cause, it would contradict the environmental factors hypothesis.
3. **Climate and disaster data:** Examine historical climate and disaster data, such as rainfall patterns, temperature records, flood reports, and drought indices. Evaluate if there is a strong correlation between environmental events and subsequent displacements. If the data shows inconsistencies or weak correlation, it would cast doubt on the hypothesis.
4. **IDP narratives:** Conduct interviews or surveys with IDPs to understand their experiences and reasons for displacement. Explore their perspectives on whether environmental factors, like floods or droughts, played a primary role in their displacement. If conflict-related factors consistently emerge as the dominant cause in their narratives, it would challenge the environmental factors hypothesis.
5. **Socio-economic indicators:** Assess socio-economic indicators such as poverty rates, unemployment rates, access to education and healthcare, and basic infrastructure. Examine if socio-economic disparities are prevalent in areas with high IDP populations, which could suggest that underlying social and economic factors are contributing more significantly to displacement than environmental factors alone.

Test 2, Hypothesis 2

1. **Security incidents:** Monitor the frequency and intensity of security incidents, including Boko Haram attacks, clashes between security forces and armed groups, and intercommunal violence. If security incidents consistently outweigh governance-related factors as the primary cause of displacement, it would challenge the hypothesis.
2. **Government policies and programs:** Analyze the effectiveness and implementation of government policies and programs aimed at addressing socio-economic disparities, conflict resolution, and provision of basic services in the region. Evaluate if there is evidence of meaningful efforts and their impact on reducing displacement. If government actions appear inadequate or ineffective in addressing the root causes of displacement, it would support the hypothesis.
3. **Human rights reports:** Examine reports from human rights organizations that document cases of human rights abuses, violence, and forced displacement in North-East Nigeria. Assess if these reports highlight systemic governance issues, corruption, or lack of accountability as key contributors to the displacement crisis. If governance-related factors are consistently emphasized in the reports, it would support the hypothesis.
4. **Socio-economic indicators:** Evaluate socio-economic indicators such as poverty rates, unemployment rates, access to basic services, and infrastructure development. Assess whether there is evidence of systemic socio-economic disparities that are perpetuated by governance issues, leading to displacement. If socio-economic indicators strongly correlate with displacement patterns, it would support the hypothesis.
5. **Stakeholder perspectives:** Engage with local communities, NGOs, civil society organizations, and local authorities to gather their perspectives on the role of government response and governance issues in the displacement crisis. Explore their experiences, opinions, and critiques regarding government efforts. If there is a widespread perception of inadequate government response or governance issues as the primary cause, it would support the hypothesis.

🔄 Regenerate response

Test 2, Hypothesis 3

1. Boko Haram activities: Monitor the scale and impact of Boko Haram attacks, including the number of incidents, casualties, and areas affected. Evaluate whether Boko Haram activities are the primary driver of displacement or if other factors, such as intercommunal conflicts, play a more significant role.
2. Intercommunal conflict incidents: Track the occurrence and severity of intercommunal conflicts, clashes between different ethnic or religious groups, and communal violence. Assess whether these conflicts independently contribute to significant displacement or if they are overshadowed by Boko Haram activities.
3. IDP narratives: Conduct interviews or surveys with IDPs to understand their experiences and reasons for displacement. Explore their perspectives on the main drivers of displacement, including Boko Haram activities and intercommunal conflicts. If IDPs consistently highlight intercommunal conflicts as the primary cause, it would challenge the hypothesis.
4. Conflict dynamics: Analyze the dynamics and triggers of conflicts in the region. Assess whether intercommunal conflicts have distinct patterns, causes, or escalation factors that are independent of Boko Haram activities. This analysis can help determine the relative importance of intercommunal conflicts compared to Boko Haram in driving displacement.
5. Stakeholder perspectives: Engage with local communities, NGOs, civil society organizations, and local authorities to gather their perspectives on the main causes of displacement. Explore their experiences, opinions, and observations regarding the role of Boko Haram activities versus intercommunal conflicts. If there is a consensus among stakeholders that intercommunal conflicts are the primary cause, it would challenge the hypothesis.

Test 3, Hypothesis 1



To try and disprove the hypothesis that environmental degradation (including climate change-induced desertification, soil erosion, and recurrent droughts) is the primary cause of internal displacement in North-East Nigeria, you would need to monitor a set of indicators that could demonstrate a lack of significant impact of environmental factors on displacement. Here's a list of such indicators:

1. **Rate of Desertification:** Monitor the progression or regression of desertification in North-East Nigeria. If desertification is not worsening or is being effectively managed, it could challenge the hypothesis.
2. **Agricultural Productivity:** Track changes in agricultural productivity, especially in areas prone to soil erosion and drought. Stable or improving agricultural yields would counter the idea that environmental degradation is driving displacement.
3. **Rainfall Patterns:** Analyze rainfall data over time. Consistent or improving rainfall patterns, contradicting the expectation of droughts due to climate change, would weaken the hypothesis.
4. **Water Availability:** Assess the availability and quality of water for consumption and agriculture. Improved water resources management and availability could undermine the hypothesis.
5. **Migration Patterns vs. Environmental Conditions:** Compare internal migration patterns with areas experiencing the most severe environmental degradation. A lack of correlation would suggest other factors are more influential.
6. **Livelihood Opportunities:** Evaluate the availability of alternative livelihood opportunities that are not dependent on the environment. The existence of diverse and stable economic opportunities could negate the environmental degradation hypothesis.
7. **Local Perceptions and Responses:** Conduct surveys or interviews with local communities and IDPs to understand their perceptions of the causes of displacement. If environmental factors are not predominantly cited, this would challenge the hypothesis.
8. **Health Indicators:** Monitor health indicators that could be affected by environmental conditions, such as rates of malnutrition or waterborne diseases. Improving or stable health conditions might indicate that environmental degradation is not a primary driver.
9. **Government and NGO Interventions:** Review the effectiveness of government and NGO interventions aimed at combating environmental degradation. Successful mitigation efforts could diminish the impact of environmental factors on displacement.
10. **Geographic Distribution of IDPs:** Analyze the geographic distribution of IDPs. If the majority are not from areas hardest hit by environmental issues, this would weaken the environmental degradation hypothesis.

Monitoring these indicators can provide a comprehensive understanding of the role of environmental degradation in internal displacement and help in assessing the validity of the hypothesis.

Test 3, Hypothesis 2



To attempt to disprove the hypothesis that ongoing ethnic and religious conflicts, independent of Boko Haram's insurgency, are the predominant cause of internal displacement in North-East Nigeria, you would focus on indicators that could suggest either a minimal role of these conflicts in displacement or highlight other more significant factors. Here's a list of such indicators:

1. **Frequency and Intensity of Ethnic and Religious Conflicts:** Monitor the occurrence and severity of ethnic and religious conflicts in the region. A decrease in the frequency or intensity of these conflicts, or their confinement to specific, limited areas, would challenge the hypothesis.
2. **Correlation between Conflict Areas and IDP Origins:** Examine the geographic correlation between areas experiencing ethnic and religious conflicts and the origins of IDPs. A lack of strong correlation would suggest other factors are more significant.
3. **IDP Surveys on Reasons for Displacement:** Conduct surveys or interviews with IDPs to ascertain their stated reasons for displacement. If ethnic and religious conflicts are not frequently mentioned, this would counter the hypothesis.
4. **Government and NGO Reports:** Analyze reports from governmental bodies and non-governmental organizations regarding the causes of displacement. Discrepancies in these reports could indicate other prevailing causes.
5. **Peacebuilding and Reconciliation Efforts:** Evaluate the effectiveness of peacebuilding and reconciliation efforts in the region. Successful reduction in ethnic and religious tensions without a corresponding decrease in IDP numbers could negate the hypothesis.
6. **Socio-economic Indicators in Conflict Areas:** Assess socio-economic conditions in areas affected by ethnic and religious conflicts. If these areas show signs of stability or improvement, it might suggest that conflicts are not the primary drivers of displacement.
7. **Media Reports and Independent Observations:** Monitor media reports and independent observations for evidence of ethnic and religious tensions leading to displacement. A lack of consistent reporting on such linkages would weaken the hypothesis.
8. **Security Forces Deployment and Effectiveness:** Review the deployment and effectiveness of security forces in conflict areas. Effective control and reduction of conflict without a decrease in IDP numbers would contradict the hypothesis.
9. **Comparative Analysis with Non-conflict Areas:** Compare displacement rates in areas with ethnic and religious conflicts to those without such conflicts. Similar or higher displacement rates in non-conflict areas would challenge the hypothesis.
10. **Analysis of Historical Conflict Patterns:** Examine historical patterns of ethnic and religious conflicts in the region. If these conflicts have been persistent over a long period but the displacement phenomenon is relatively new or escalated recently, it might suggest other causes.

Monitoring these indicators would provide insights into the actual impact of ethnic and religious conflicts on displacement in North-East Nigeria, helping to assess the validity of the hypothesis.

Test 3, Hypothesis 3



To attempt to disprove the hypothesis that severe economic hardship and lack of essential infrastructure are the leading causes of internal displacement in North-East Nigeria, you should focus on indicators that would suggest these factors are not as influential as proposed or that other factors play a more significant role. Here's a list of such indicators:

1. **Economic Stability and Growth:** Monitor indicators of economic stability and growth in the region, such as GDP, employment rates, and income levels. Improvement or stability in these areas could challenge the hypothesis.
2. **Infrastructure Development:** Assess the development and availability of essential infrastructure, including transportation, healthcare, education, and communication facilities. Significant improvements or adequacy in infrastructure could counter the hypothesis.
3. **IDP Surveys on Displacement Reasons:** Conduct surveys or interviews with internally displaced persons to understand their primary reasons for displacement. If economic hardship and infrastructure issues are not predominantly cited, this would weaken the hypothesis.
4. **Poverty and Unemployment Rates:** Track the poverty and unemployment rates in the region. A decrease or stability in these rates, especially in areas with high IDP numbers, could negate the economic hardship argument.
5. **Access to Basic Services:** Evaluate access to basic services like healthcare, education, and clean water. Improvements in these areas could suggest that lack of infrastructure is not a primary driver of displacement.
6. **Government and NGO Reports:** Analyze reports from government and non-governmental organizations on the causes of displacement. Discrepancies or lack of emphasis on economic and infrastructure factors could indicate other causes.
7. **Migration Patterns vs. Economic Conditions:** Compare internal migration patterns with economic conditions across different regions. If people are not predominantly moving away from the most economically deprived areas, this would challenge the hypothesis.
8. **Investment and Development Projects:** Monitor the extent and impact of investment and development projects in the region. Successful and impactful projects might indicate that economic and infrastructure issues are being addressed.
9. **Socio-Economic Indicators in IDP Origin and Destination Areas:** Compare socio-economic conditions in areas where IDPs originate and where they relocate. If destination areas do not significantly differ in economic and infrastructure terms, it could suggest other reasons for displacement.
10. **Local and Regional Market Dynamics:** Observe local and regional market dynamics, including the availability of goods, market prices, and trade patterns. Stability or improvement in these areas could indicate that economic hardship is not the primary cause of displacement.

By monitoring these indicators, you can gain insights into the actual impact of economic hardship and lack of infrastructure on internal displacement in North-East Nigeria, helping to assess the validity of the hypothesis.

BIBLIOGRAFIA

- Acemoglu D., Restrepo P., *Artificial intelligence, automation, and work* [In:] *The economics of artificial intelligence: An agenda*. University of Chicago Press, 2018.
- Andersson J. et. al., *Envisioning European Defence: Five Futures*, „Chaillot Paper” 2017, nr 137.
- Appelbaum J. et al., *Documents Reveal Top NSA Hacking Unit*, <https://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html>.
- Baczwarow M., Napierała T., *Wpływ wydarzeń 11 września 2001 r. na turystykę światową*, Wyższa Szkoła Turystyki i Hotelarstwa w Łodzi, „Turystyka i Hotelarstwo” 2002, nr 1.
- Bańczyk Ł. et al., *Analiza zdarzeń lotniczych z udziałem laserów na świecie i w Polsce*, „Biuletyn Bezpieczeństwa w Lotnictwie Cywilnym” 2023, nr 2(23).
- Baranowska A. et al., *Klasy zaawansowanych technologii jako instrument wsparcia rozwoju i konkurencyjności regionów – analiza i wnioski dla polityki regionalnej oraz polityki spójności*, Instytut Badań Strukturalnych, Warszawa 2009.
- Barfield W., *Cyber-Humans. Our Future with Machines*, New York 2015.
- Baseley Walker B., *Current international space security initiatives* [w:] *The fair and responsible use of space*, W. Rathgeber, K-U. Schrogl, R.A. Williamson, Springer, 2010.
- Becla A., *Spółeczeństwo informacyjne i społeczeństwo pseudoinformacyjne – problemy pojęciowe i metodyczne identyfikacji*, „Handel Wewnętrzny” 2012, t. 3.
- Bendkowski J., *Zmiany w pracy produkcyjnej w perspektywie koncepcji Przemysłu 4.0*, „Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie” 2017, nr 112.
- Berlin A., Brotherson L., *Bezpieczeństwo defensywne. Podstawy i najlepsze praktyki*, Gliwice 2018.
- Betts R.K., *Analysis, war, and decision: Why intelligence failures are inevitable*, “World politics” 1978, 31(1).
- Białobrodzki A., Nazarko Ł., Wilczewska M., *Egzogenne czynniki wpływające na rozwój Przemysłu 4.0 w przedsiębiorstwach produkcyjnych Białostockiego Obszaru Funkcjonalnego*, „Akademia Zarządzania” 2020, nr 4(3).
- Bierca M., Wysocka-Światała A., *Sharenting po polsku, czyli ile dzieci wpadło do sieci? Pierwszy raport w Polsce na temat wizerunku dzieci w Internecie na zlecenie Clue PR*, 2019.
- Biometria w bankowości – kluczowe aspekty*, red. T. Woszczyński, Warszawa 2015.
- Biscop S., *The EU Global Strategy 2020*, „Security Policy Brief” 2019, nr 108.
- Biswas S.S., *Role of chat gpt in public health*, “Annals of Biomedical Engineering” 2023.
- Błażewski M., *Wartości e-administracji i ich wyważenie* [w:] *Aksjologia prawa administracyjnego*, red. J. Zimmermann, t. 1, Warszawa 2017.
- Błażewski M., *Zasada zapewnienia bezpieczeństwa w e-administracji*, „Folia Iuridica Universitatis Wratislaviensis” 2017/6(1).
- Bochyńska N., #CyberMagazyn: *Ukraińska armia IT. Nieoczywisty obraz hakowania wroga*, CyberDefence24.

- Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003.
- Boguszewski Ł., *Komunikacja, informacja i retoryka – wpływ na środowisko bezpieczeństwa*, „Kwartalnik Bellona” 2017, nr 3.
- Bonnal Ch., *Pollution spatiale, l'etat d'urgence*, Belin 2016.
- Borkowska A., Witkowska M., *Sharenting i wizerunek dziecka w sieci. Poradnik dla rodziców*, Warszawa 2020.
- Brill E., Mooney R.J., *An overview of empirical natural language processing*, “AI magazine” 1997, 18(4).
- Britchenko I., Chochowski K., *Artificial intelligence, its application and development prospects in the context of state security*, “Politics & Security” 2022, Vol. 6, No. 3.
- Buchała K., *Glosa do wyroku Sądu Najwyższego z dnia 9.10.1996 r.*, sygn. akt VKKN 79/96, „Państwo i Prawo” 1999 r., nr 9.
- Burek E., Wroński M., *Quantum Annealing and Algebraic Attack on Speck Cipher*, “Computational Science – ICCS” 2022.
- Burger E., Bordaccini G., *Yearbook on Space Policy 2017. Security in Outer Space: Rising Stakes for Civilian Space Programmes*. Edited by the European Space Policy Institute, Cham, Switzerland 2019.
- California Code of Regulations, Title 8, Chapter 6. Division of Labor Standards Enforcement, Subchapter 2. Employment of Minors in the Entertainment Industry New Query, § 11760. Working Hours of Minors.
- Cantillo J., Martín J.C., Román J.C., *Hybrid Fuzzy TOPSIS Method to Analyze the Coverage of a Hypothetical EU Ecolabel for Fishery and Aquaculture Products (FAPs)*, “Applied Sciences” 2020, 11(1).
- Centralne Biuro Antykorupcyjne, *Korupcja na przestrzeni wieków*, Warszawa 2012.
- Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law” 2019, 2(2).
- Chanock B., *The problems and potential solutions related to the emergence of Space Weapons in the 21st Century*, “Journal of Air Law and Commerce (JALC)” 2013, t. 78.
- Cheah W.K.A., Aigbogun O., *Exploring attitude-behaviour inconsistencies in organic food consumption during the COVID-19 pandemic in the Klang Valley, Malaysia*, “Cleaner and Responsible Consumption” 2022.
- Chen H. et al., *Feedback is all you need: from ChatGPT to autonomous driving*, “Science China Information Sciences” 2023, 66(6).
- Ching J., *Cyberterrorism*, New York 2010.
- Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej” 2016, nr 2(10).
- Chochowska A., Chochowski K., *Bezpieczeństwo lotnictwa cywilnego wobec zagrożenia terroryzmem [w:] Prawne aspekty bezpieczeństwa transportu lotniczego*, red. N. Jasiuk, K. Sikora, Warszawa 2021.
- Chochowski K., *Basic determinants of special services efficiency*, “Košická Bezpečnostná Revue” 2023, Vol. 13, No. 1(2023).
- Chochowski K., *Śłużby specjalne w Polsce*, Sofia 2021.
- Christoph K., *Digital innovation and entrepreneurship: a review of challenges in competitive markets*, “Journal of Innovation and Entrepreneurship” 2023, Vol. 12(49).

- Chrostowska B., *Sharenting – skala i wielowymiarowość zjawiska (nierozważnego) ujawniania przez rodziców informacji o dzieciach w mediach społecznościowych*, „Problemy Wczesnej Edukacji” 2018/4, s. 59.
- Chudy W., *Kłamy profesjonalni? Praca dyplomaty i szpiega w ujęciu etyki*, Tychy 2004.
- Ciborowski L., *Walka informacyjna*, Europejskie Centrum Edukacyjne, Toruń 1999.
- Cichorzewska M., Hysa B., Wójcik P., *Wybrane aspekty zarządzania różnorodnością pracowników Przemysłu 4.0*, Wydawnictwo Politechniki Lubelskiej, Lublin 2020.
- Citkowski M., *Managing relational competences of industrial cluster and the challenges of Industry 4.0 – theoretical approach*, „Marketing i Rynek” 2021, nr 12(28).
- Compa T., *Bezpieczeństwo w lotnictwie. Prawne i proceduralne aspekty badania wypadków lotniczych*, „Facta Simonidis” 2019, nr 1(12).
- Compa T., *Współczesne zagrożenia bezpieczeństwa transportu lotniczego*, „Facta Simonidis” 2018, nr 1(11).
- Cook C.N. et al., *Strategic foresight: how planning for the unpredictable can improve environmental decision-making*, “Trends in ecology & evolution” 2014, 29(9).
- Cruickshank I.J., *On Data Science and Intelligence Analysis*, Military Intelligence 2019 (PDF) On Data Science and Intelligence Analysis (researchgate.net).
- Cywoniuk J., *Współczesne zagrożenia cyberprzestrzeni Rzeczypospolitej Polskiej [w:] E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni*, M. Lakomy, M.K. Zwierzdzyński, K. Oświecimski, Akademia Ignatianum w Krakowie, Kraków 2015.
- Czajkowska K., *Rynek e-commerce – jego specyfika i perspektywy rozwoju w Polsce*, „Journal of Modern Management Process” 2016, Vol. 1(1).
- Czaputowicz J., *Kryteria bezpieczeństwa międzynarodowego – aspekty teoretyczne [w:] Kryteria bezpieczeństwa międzynarodowego państwa*, red. S. Dębski, B. Górską-Winter, PISM, Warszawa 2003.
- Czas na Cyfrową Gospodarkę*, Fundacja DigitalPoland, Warszawa 2022.
- Czepielewski S., *E-administracja – kolejny krok ku e-integracji Europy*, „Zeszyty Naukowe Wyższej Szkoły Informatyki, Zarządzania i Administracji” 2012/3.
- Czub-Kielczewska S., *Okiem IOD-a: dane biometryczne – granice wykorzystania*, LEX/el. 2020.
- Czupryński A., *Bezpieczeństwo w ujęciu teoretycznym [w:] Bezpieczeństwo. Teoria – Badania – Praktyka*, Józefów 2015.
- Daniluk P., *Kultura strategiczna Unii Europejskiej. Podejście normatywne*, „Rocznik Bezpieczeństwa Międzynarodowego” 2015, t. 9(2).
- Davis P.K., *Deterrence, Influence, Cyberattack and cyberwar*, „New York University Journal of International Law and Politics” 2014.
- de Melo H.B., *Does Analysis of Competing Hypotheses (ACH) Really Mitigate Cognitive Biases? Practical Implications for Intelligence Analysts and Criminal Investigators*, “International Journal of Criminal Justice” 2021, 3(2).
- Dela P., *Teoria walki w cyberprzestrzeni*, Warszawa 2020.
- Dela P., *Zasady sztuki wojennej w cyberprzestrzeni [w:] Wojny i konflikty zbrojne XXI wieku – podejście polemologiczne*, red. A. Polak, J. Lasota, M. Palczewska, Warszawa 2016.
- Denning D.E., *Cyberterrorism*, Global Dialogue, Autumn 2000.
- Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002.
- Dependence of the European Economy on Space Infrastructures Potential Impacts of Space Assets Loss, PwC, 2017.

- Derbentseva N., McLellan L., Mandel D.R., *Issues in Intelligence Production: Summary of Interviews with Canadian Managers of Intelligence Analysis*, Defence R & D Canada, 2010.
- Dhami M.K., Belton I.K., Mandel D.R., *The "analysis of competing hypotheses" in intelligence analysis*, "Applied Cognitive Psychology" 2019, 33(6).
- Dmitruk T., *Budżet obronny Polski na 2023 rok*, „Nowa Technika Wojskowa” 2023, nr 3.
- Dołzbłasz S., Raczyk A., *Stabilność współpracy transgranicznej w Polsce w wymiarze tematycznym i przestrzennym*, „Studia Regionalne i Lokalne” 2020, 4(90).
- Domeny internetowe. Teoria i praktyka*, red. I. Matusiak, WKP 2020, el.
- Driven by global threats, shaped by civil high-tech*, European Defence Matters, European
- Ducaru S., *Security from Space and Security in Space- an operational perspective* [w:] SMI's Military Space Situational Awareness 2020 Conference (virtual), 3–4 September 2020.
- E-commerce w czasach kryzysu*, IAB Polska, Warszawa 2020.
- ESPI report June 2018 Security in Outer Space: Rising Stakes for Europe*, report 64.
- Fajgielski P., *Ochrona danych osobowych w administracji publicznej*, Warszawa 2021.
- Fajgielski P., *Przetwarzanie szczególnych kategorii danych w świetle ogólnego rozporządzenia o ochronie danych* [w:] *Przetwarzanie danych osobowych*, red. G. Szpinador, K. Czaplicki, Warszawa 2019.
- Ferdousi B., *Data Security Concerns and Customers' Trust in Online Business*, Proceedings of the 5th NA International Conference on Industrial Engineering and Operations Management Detroit, Michigan, USA 2020.
- Ferrer-Estevez M., Chalmeta R., *Sustainable customer relationship management*, „Marketing Intelligence & Planning” 2022, Vol. 41, No. 2.
- Filipowicz T., *Zasada równego traktowania wykonawców w zamówieniach publicznych dotyczących technologii informatycznych*, Lex 2015.
- Firat M., *How chat GPT can transform autodidactic experiences and open education*, Department of Distance Education, Open Education Faculty, Anadolu Unive, 2023.
- Fleszer D., *Wokół problematyki e-administracji*, „Roczniki Administracji i Prawa” 2014/14.
- Formicki T., *Wywiad i kontrwywiad jako kluczowe komponenty walki informacyjnej*, Warszawa 2020.
- Frankowska M., Nowicka K., *Zarządzanie łańcuchem dostaw w dobie Smart Industry*, „Gospodarka Materiałowa i Logistyka” 2018, nr 3.
- Frankowska M., *Współdziałanie przedsiębiorstw w klastrach łańcuchach dostaw*, CeDeWu, Warszawa 2018.
- Frankowska M., *Znaczenie koncepcji klastrów łańcuchów dostaw w zwiększaniu międzynarodowej konkurencyjności regionalnych sieci kooperacyjnych*, „International Journal of Management and Economics” 2011, nr 32.
- Furmanek W., *Najważniejsze idee czwartej rewolucji przemysłowej*, „Dydaktyka Informatyki” 2018, nr 13.
- Future Directions in Human Machine Teaming Workshop*, Arlington 2019. Future Directions in Human Machine Teaming Workshop report (for public release).pdf (defense.gov).
- Gałka J., Mąsior M., Salasa M., *System kontroli dostępu oparty na biometrycznej weryfikacji głosu*, „Przegląd Elektroniczny” 2014, nr 11.
- Ganczar M., *Elektroniczna administracja publiczna* [w:] *Encyklopedia prawa administracyjnego*, red. M. Domagała, A. Haładaj, S. Wrzosek, Warszawa 2010.
- Ganczar M., Sytek A., *Informatyzacja administracji publicznej. Skuteczność regulacji*, CeDeWu, Warszawa 2021.

- Gawliczek P., Pawłowski J., *Zagrożenia asymetryczne*, Warszawa 2003.
- Gawroński M., Sztąberek M., *Artykuł 9 i 10 RODO – dane szczególnych kategorii i dane karne* [w:] *Ochrona danych osobowych, przewodnik po ustawie i RODO ze wzorami*, red. M. Gawroński, Warszawa 2018.
- Gleeson P.K., *Perspectives on Space Operations, Astropolitics*, "The International Journal of Space Politics and Policy" 2007, Vol. 5, No. 09.
- Goodman M., *Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko Tobie*, Gliwice 2015.
- Górka M., *Współczesne zagrożenia cybernetyczne na przykładzie zjawiska cyberwojny. Analiza teoretyczna*, „Acta Politica Polonica” 2021, nr 1.
- Górniewicz M., Obczyński R., Pstruś M., *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną*, Warszawa 2014.
- Górny P., Krawiec J., *Cyberbezpieczeństwo – podejście systemowe*, „Obronność. Zeszyty Naukowe” 2016, nr 2(18).
- Grabalska W., Wielki R., „Czy dzieci powinny trafiać do sieci?”. *Prawne i kryminologiczne aspekty zjawiska sharentingu*, „Prawo w Działaniu” 2022, nr 49.
- Grabowski T., *Wykorzystywanie Internetu przez ugrupowania terrorystyczne* [w:] *E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni*, M. Lakomy, M.K. Zwierzdzyński, K. Oświecimski, Akademia Ignatianum w Krakowie, Kraków 2015.
- Grego-Planer D., Liczmańska K., Petrykowska J., *Korzyści wynikające z budowania trwałych relacji z klientami w firmach usługowych*, Zeszyty Naukowe SGGW, „Polityki Europejskie, Finanse i Marketing” 2013, nr 10(59).
- Grodzka D., *E-administracja w Polsce*, „Infos”, Studia BAS Kancelarii Sejmu, Warszawa 2007, nr 18.
- Grześkowiak A., Wiak K., *Kodeks karny. Komentarz*, wyd. 6, Warszawa 2019.
- Hahne P., *Sila manipulacji*, Warszawa 1997.
- Hajduk-Stelmachowicz M., Belch P., Siwiec D., Bednárová L., Pacana A., *Instruments used to improve the betterment of products quality*. Scientific Papers of Silesian University of Technology, “Organization and Management Series” 2022.
- Haręza A., *Wprowadzenie do problematyki elektronicznej administracji publicznej*, PME 2011/1.
- Harrel Y., *Rosyjska cyberstrategia*, Warszawa 2015.
- Hassani H., Silva E.S., *The role of ChatGPT in data science: how ai-assisted conversational interfaces are revolutionizing the field*, “Big data and cognitive computing” 2023, 7(2).
- Herman M., *Potęga wywiadu*, Warszawa 2002.
- Heuer R.J. Jr., *Improving Intelligence Analysis with ACH*, Washington DC: Center for the Study of Intelligence Analysis, Central Intelligence Agency, 2005.
- Hoc S., *Ustawa o ochronie informacji niejawnych. Komentarz*, Warszawa 2010.
- Hoffmann R., *Stochastyczny model ogólnego cyklu życia ataku cybernetycznego* [w:] A.Z. Sosnowiecki, *Symulacje komputerowe w badaniach i rozwoju*, Oficyna Wydawnicza Politechniki Białostockiej, Białystok 2020.
- Hong J., *The state of phishing attacks*, „Communications of the ACM” 2012, No. 55(1).
- Huovinen P., *Hybrid Warfare – Just a twist of compound Warfare? Views on warfare from the US Armed Force perspective*, National Defence University, 2011.

- Husak Z., *Ochrona bezpieczeństwa państwa przed zagrożeniami cybernetycznymi w Unii Europejskiej* [w:] *Bezpieczeństwo państwa. Zagadnienia podstawowe*, red. W. Lis, Lublin 2014.
- Hydzik W., *Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych*, „Business Law Journal” 2019, nr 3.
- Ilieska K., Alavantija M., *Customer Relationship Marketing as an E-Marketing Strategic Imperative for The Companies*, „Entrepreneurship, Faculty of Economics, South-West University „Neofit Rilski” 2016, Blagoevgrad, Vol. 4(1).
- Inayatullah S., *Questioning the future: Methods and tools for organizational and societal transformation*, Tamkang University Press, 2005.
- ISO 14020:2000, Environmental labels and declarations – General principles (2000).
- Jakesch M., Hancock J.T., Naaman M., *Human heuristics for AI-generated language are flawed*, “Proceedings of the National Academy of Sciences” 2023, 120(11).
- Jakubowski A., Bronisz U., Miszczuk A., *Polityka Spójności oraz Europejski Instrument Sądztwa i Partnerstwa jako narzędzia wsparcia współpracy transgranicznej na wewnętrznych i zewnętrznych granicach Unii Europejskiej*, „Roczniki Nauk Społecznych” 2020, nr 45(3).
- Jancelewicz J., *Phishing i pokrewne ataki socjotechniczne jako zagrożenie dla organizacji pozarządowych*, „Kwartalnik Trzeci Sektor” 2022, nr 59–60 (3–4/2022).
- Janikowski R., *Środowiskowe aspekty czwartej rewolucji przemysłowej*, „Studia i Prace Wydziału Nauk Ekonomicznych i Zarządzania Uniwersytetu Szczecińskiego” 2017, nr 47(2).
- Jankowska-Mihułowicz M., *Environmental Choice* [w:] *Innovations in circular economy – Environmental labels and declarations*, red. B. Ziółkowski, B. Agarski, J. Šebo, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2021.
- Janowski J., *Administracja elektroniczna*, Warszawa 2009.
- Janowski J., *Administracja elektroniczna. Kształtowanie się informatycznego prawa administracyjnego i elektronicznego postępowania administracyjnego w Polsce*, Municipium S.A., Lublin 2009.
- Janowski J., *Cybernetyzacja prawa* [w:] *X-lecie CBKE. Księga pamiątkowa z okazji 10-lecia Centrum Badań Problemów Prawnych i Ekonomicznych Komunikacji Elektronicznej i Studenckiego Koła Naukowego*, red. E. Galewska, S. Kotecka, Warszawa 2012.
- Jarosz Sz., *Zjawisko czwartej rewolucji przemysłowej w sektorze finansów, ekonomii i zarządzania*, „Studenckie Prace Prawnicze, Administratywistyczne i Ekonomiczne” 2022, nr 40.
- Johanesova V., Vanova J., *What is Relationship Marketing and How to Use it to Connect with Your Customers*, “Research Papers, Faculty of Materials Science and Technology in Trnava” 2020, Vol. 28, No. 46.
- Joshi A.B., *Eco-labels: Concerns and Experiences*. Icfai University Press 2008.
- Jurgilewicz M., Kosior E., *Ochrona danych osobowych a bezpieczeństwo wewnętrzne państwa* [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Wydawnictwo UPH w Siedlcach, Siedlce 2019.
- Juszczak S., *Internet – współczesne medium komunikacji społeczne*, <http://www.ktime.up.krakow.pl/symp2011/referaty/juszczak.pdf> [za:] A. Warchoń, *(Nie) bezpieczeństwo w cyberprze-strzeni* [w:] *Współczesne zagrożenia bezpieczeństwa państwa*, A. Żebrowski, E. Sadowska, I. Szkułat, A. Warchoń, Kraków–Stalowa Wola 2018.
- Kaczorowska A., *E-usługi administracji publicznej w warunkach zarządzania projektami*, Łódź 2013.
- Kaiser S.A., *Legal and policy aspects of space situational awareness*, “Space Policy” 2014, 31(2015).

- Kamiński A., *Inteligentna fabryka – nowe trendy w rozwoju systemów informatycznych dla przemysłu*, „Zarządzanie i Finanse” 2018, nr 3(2), Vol. 16.
- Kamiński M.A., *Ewolucja wywiadu jako instytucji państwa*, Warszawa 2021.
- Kapera K., *Wpływ technologii informacyjnej na rozwój systemów informacji marketingowej*, „Acta Universitatis Lodzianensis, Folia Oeconomica” 2004, 179.
- Kardas P., *Oszustwo komputerowe w kodeksie karnym*, „Przegląd Sądowy” 2000, nr 11–12.
- Karpik M., Chałubińska-Jentkiewicz K., *Informacja i informatyzacja w administracji publicznej*, Warszawa 2015.
- Karwowska K., Folga A., *Phishing: modus operandi sprawców oraz środki zapobiegawcze*, „Kortowski Przegląd Prawniczy” 2013, nr 4.
- Kawalec P., *Transformacja cyfrowa: szanse i wyzwania dla przedsiębiorstw*, „Nowe Tendencje w Zarządzaniu 2021”, nr 1.
- Kemendi A. et al., *Industry 4.0 and 5.0 – organizational and competency challenges of enterprises*, „Polish Journal of Management Studies” 2022, Vol. 26, No. 2.
- Kieltyka A., *Zatrzymanie rzeczy [w:] Prawo karne procesowe dla sędziów, prokuratorów, obrońców i pełnomocników. Praxis*, red. M. Oleżałek, Warszawa 2024.
- Kieźel M., Wieczorek J., *Narzędzia e-marketingu w procesie kreowania wartości dla klienta*, Zeszyty Naukowe Politechniki Śląskiej, Seria „Organizacja i Zarządzanie” 2017, z. 114.
- Kim E., McDonald S., *Food Safety Labelling Management in the Green Supply Chain Management: A Direct Observational Study in the Vietnamese Retail Food Sector*, “Journal of International Logistics and Trade” 2018, 16(3).
- Kiraga K., *Przemysł 4.0 – rewolucja przemysłowa według FESTO*, „Autobusy” 2016, nr 12.
- Klamut R., *Bezpieczeństwo jako pojęcie psychologiczne*, „Zeszyty Naukowe Politechniki Rzeszowskiej” 2012.
- Kłosińska J., *Nowe formy budowania relacji z klientem w Internecie za pomocą takich narzędzi jak content marketing, real-time marketing, aplikacje mobilne, portale społecznościowe, komunikacja video*, „Nowoczesne Systemy Zarządzania” 2018, t. 13, nr 3.
- Kodeks postępowania karnego*, t. II: *Komentarz do art. 167–296*, red. R.A. Stefański, S. Zabłocki, Warszawa 2019.
- Kohnke L., Moorhouse B.L., Zou D., *ChatGPT for language teaching and learning*, “RELC Journal” 2023.
- Konopelko A., *Wdrażanie Programu Współpracy Transgranicznej Polska-Białoruś-Ukraina w ramach Europejskiej Polityki Sąsiedztwa*, „Przedsiębiorczość i Zarządzanie” 2018, nr 19(3.1).
- Korga M., *Ochrona danych osobowych – od czego zacząć, jak opracować i utrzymać system oraz na czym polega ochrona danych w praktyce [w:] Przygotowanie organizacji do stosowania RODO*, red. M. Korga, Warszawa 2016.
- Korzeniowski L., *Potrzeby i wartości a poczucie bezpieczeństwa menedżerów*, „Acta Univ. Wratisl. Socjol.” 2006, 38.
- Kos J., *Nowoczesne narzędzia w komunikacji marketingowej – potencjał społeczności internetowych [w:] Marketing przyszłości. Trendy. Strategie. Instrumenty. Współczesne wyzwania komunikacji marketingowej*, red. G. Rosa, A. Smalec, Zeszyty Naukowe Uniwersytetu Szczecińskiego, Nr 559, „Ekonomiczne Problemy Usług” 2009, nr 42.
- Kotler P. et al., *Marketing. Podręcznik Europejski*, Warszawa 2002.
- Kowalski A. et al., *Poradnik dotyczący cyfryzacji łańcuchów wartości w klastrach*, Platforma Przemysłu Przyszłości, Warszawa 2021.

- Koziej S., *Transsektorowy charakter cyberbezpieczeństwa. Strategiczne wyzwania dla Polski i NATO*, Warszawa 2016.
- Krajewski R., *Przestępstwo publicznego propagowania lub pochwalania zachowań o charakterze pedofilskim*, „Przebieg Sądowy” 2011, nr 6.
- Kralikova R., Rusko M., Wessely E., *Ekolabeling as Development Facilitator of the Environmentally Oriented Product Policy* [In:] *DAAAM Proceedings* (1st ed., Vol. 1), ed. B. Katalinic, DAAAM International Vienna 2017.
- Krzywka K., *Bezpieczeństwo osobowe i ochrona fizyczna informacji niejawnych w Unii Europejskiej*, „OBRONNOŚĆ. Zeszyty Naukowe” 2018, nr 4(28).
- Kuba M., *Administrator danych osobowych biometrycznych – wybrane zagadania* [w:] *Administrator i inspektor ochrony danych osobowych*, red. T. Wyka, M.A. Mielczarek, Warszawa 2019.
- Kulik T., *Uwarunkowania bezpieczeństwa powietrznego państwa w aspekcie militarnych zagrożeń powietrznych*, „Kwartalnik Bellona” 2020, 701(2).
- Kurian N. et al., *AI is now everywhere*, „British Dental Journal” 2023, 234(2).
- Kwećka R., *Strategia bezpieczeństwa informacyjnego państwa*, Warszawa 2014.
- Kwiatkiewicz B., *Dokument elektroniczny w ogólnym postępowaniu administracyjnym*, WKP, Warszawa 2020, Lex el.
- Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wyd. Uniwersytetu Śląskiego, Katowice 2015.
- Lakomy M., Zwierżdżyński M.K., Oświecimski K., *Paradoks sieci: szanse i zagrożenia cyfrowej demokracji* [w:] *E-administracja publiczna i (nie)bezpieczeństwo cyberprzestrzeni*, M. Lakomy, M.K. Zwierżdżyński, K. Oświecimski, Akademia Ignatianum w Krakowie, Kraków 2015.
- Łangowska D., *Klasy oparte na wiedzy i ich wpływ na rozwój gospodarczy Polski*, „Roczniki Kolegium Analiz Ekonomicznych Szkoły Głównej Handlowej w Warszawie” 2015, nr 36.
- Lasota-Kapczuk A., *Sztuczna inteligencja w kształtowaniu bezpieczeństwa państwa w II dekadzie XXI wieku*, rozprawa doktorska, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach, Siedlce 2021.
- Laszczak M., *Zarządzanie bezpieczeństwem w erze cyfrowej*, „Bezpieczeństwo. Teoria i Praktyka” 2019, nr 4.
- Latiff R.H., *Wojna przyszłości w obliczu nowego globalnego pola bitwy*, Warszawa 2018.
- Libera B., *Zagrożenia ze strony służb specjalnych* [w:] *Urzędnik i biznesmen w środowisku międzynarodowym. Wybrane aspekty pragmatyki zawodowej*, red. J. Barcz, B. Libera, Kraków 2007.
- Lis T., Małysa T., *Zarządzanie bezpieczeństwem i higieną pracy w aspekcie wdrażanych rozwiązań Przemysłu 4.0*, „Zeszyty Naukowe WSH” 2021, nr 1.
- Littlejohn Shinder D., Tittel E., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w Sieci*, Gliwice 2004.
- Litwiński P., Barta P., Kawecki M., *Zasady RODO* [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, P. Barta, M. Kawecki, Warszawa 2018.
- Liu C.-C. et al., *Measuring Consumer Preferences and Willingness to Pay for Coffee Certification Labels in Taiwan*, „Sustainability” 2019, 11(5).
- Liu Q. et al., *Consumer Choices and Motives for Eco-Labeled Products in China: An Empirical Analysis Based on the Choice Experiment*, „Sustainability” 2017, 9.

- Lubasz D., *Dopuszczalność przetwarzania szczególnych kategorii danych osobowych* [w:] *RODO dla małych i średnich przedsiębiorstw*, red. D. Lubasz, Warszawa 2018.
- Łuczak J., Tyburski M., *Systemowe zarządzanie bezpieczeństwem informacji ISO/IEC 27001*, Poznań 2009.
- Machnik-Słomka J., *Znaczenie klastrów wiedzy w komercjalizacji wyników badań z uczelni*, „Organizacja i Zarządzanie” 2011, nr 4.
- Maciejewski M., *Prawo informacji – zagadnienia podstawowe* [w:] *Prawo informacji. Prawo do informacji*, red. W. Góralczyk jun., Warszawa 2006.
- Madej M., *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007.
- Maintaining the Intelligence EDGE. Reimagining and Reinventing Intelligence through Innovation*, 2021. Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation (csis.org).
- Malešević S., *Terrorism. In The Rise of Organised Brutality: A Historical Sociology of Violence*, Cambridge 2017.
- Maliszewski W., *Akcje psychologiczne w działaniach nieregularnych*, „Myśl Wojskowa” 1996, nr 6.
- Marczyk M., *Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru*, „Przegląd Teleinformatyczny” 2018, nr 1–2.
- Marrin S., *Improving intelligence analysis: Bridging the gap between scholarship and practice*, Routledge, 2012.
- Martin A., Greenberg C., *The NIST 2010 Speaker Recognition Evaluation*, Interspeech 2010.
- Martysz Cz., Wojsyk K., *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, wyd. II, LEX 2015.
- Matela K., *Wybrane aspekty systemów wywiadu, obserwacji i rozpoznania*, „Wiedza Obronna” 2021, Vol. 276, No. 3.
- Matusiak B.E., Matejun M., Różańska-Bińczuk I., *Koncepcja zrównoważonego rozwoju jako środowisko implementacji praktyk green HR we współczesnych przedsiębiorstwach* [w:] *Wyzwania społeczne i technologiczne a nowe trendy w zarządzaniu współczesnymi organizacjami*, red. M. Urbaniak, A. Tomaszewski, Oficyna Wydawnicza SGH, Warszawa 2020.
- Matusiak J., *Publicznoprawna regulacja administracji elektronicznej*, WSB Poznań, Poznań 2016.
- Mazepa D., *Narodowa Strategia Bezpieczeństwa Cybernetycznego Republiki Macedonii Północnej i Plan Działania 2018–2022*, „Wschodnioznawstwo” 2019, t. 13.
- Meng C., *Competitive Advantages and Challenges of E-Commerce*, Proceedings of the 2nd International Conference on Financial Technology and Business Analysis, EWA Publishing, California 2023.
- MI6 Chief Alex Younger spoke on how the Secret Intelligence Service is evolving in response to hybrid threats and pioneering new approaches to keep the UK safe*. MI6 'C' speech on fourth generation espionage – GOV.UK (www.gov.uk).
- Migała-Warchoł A., Ziółkowski B., Babiarz P., *The circular economy vs the sustainable development approach to production and consumption: The case of the European Union countries*, “Humanities and Social Sciences” 2024, 30(2).
- Minkina M., Gałek B., *Kłamstwo i podstęp we współczesnym świecie*, Warszawa 2015.
- Minkina M., *Sztuka wywiadu w państwie współczesnym*, Warszawa 2022.
- Moczydłowska J., *Przemysł 4.0: ludzie i technologie*, Difin, Warszawa 2023.

- Monham A., *Securing EUMETSAT's Mission from an Evolving Space Environment*, SMI's Military Space Situational Awareness 2020 Conference (virtual).
- Monitoring space weather as a key enabler for holistic SSA* [w:] SMI's Military Space Situational Awareness 2020 Conference (virtual), 3–4 September 2020.
- Moran Ch.R., Burton J., Christou G., *The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying*, "Journal of Global Security Studies" 2023, 8(2).
- Moranta S., *Security in Outer Space: Perspectives on Transatlantic Relations*, 12th ESPI Autumn Conference Vienna, September 27, 2018.
- Mostowik M., *Ochrona danych osobowych w Internecie rzeczy w prawie UE*, Warszawa 2022, Legalis.
- Moszczyński J., *Informatyka kryminalistyczna* [w:] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa 2011.
- Muliński T., *Zagrożenia bezpieczeństwa dla systemów informatycznych e-administracji*, CeDeWu, Warszawa 2015.
- Muncaster P., *Ukrainian "Blackjack" Hackers Take Out Russian ISP*, "Info-Security Magazine" z 10.01.2024 r.
- Nowacki K., *Rola człowieka w innowacyjnym przedsiębiorstwie z wykorzystaniem koncepcji Przemysłu 4.0 – studium przypadku*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu” 2020, nr 11, Vol. 64.
- Nowak A., *Działania psychologiczne w konfliktach zbrojnych*, Warszawa 2007.
- Nowicki M., *Ukraińscy hakerzy sieją chaos. „Rosja jest naszym placem zabaw”*, „Newsweek Polska” 21.08.2023 r.
- Nwakanma H., Sigleton Jackson A., Burkhalter J.N., *Relationship marketing: An Important Tool for Success in The Marketplace*, „Journal of Business & Economics Research” 2007, Vol. 5, No. 25–66.
- Ochrona danych osobowych w prawie publicznym*, red. M. Jędrzejczak, WKP 2021, lex el.
- Okada N., *Cleaning up space*, "Roomb. The Space Journal" 2019, nr 1(19).
- Okonek P., *Relacje z klientami w e-biznesie*, Wydawnictwo PARP, Warszawa 2010.
- Oleksiewicz I., Civelek M.E., *Where are the changes in EU cybersecurity legislation leading?* "Humanities and Social Sciences Quarterly" 2023, 30(4-part I).
- Oleksiewicz I., *Ochrona cyberprzestrzeni Unii Europejskiej. Polityka. Strategia. Prawo*, Warszawa 2021.
- Olewiński B., *Zadania organów ścigania w zwalczaniu przestępstw przeciwko bezpieczeństwu publicznemu* [w:] *Aktualne zagrożenia i wyzwania w obszarze bezpieczeństwa społecznego i gospodarczego*, red. M. Pomykała, I. Oleksiewicz, Rzeszów 2022.
- Opitek P., *Kwalifikacja prawna i opis znamion przestępstw teleinformatycznych. Studium prawnokryminalistyczne*, Kraków 2023.
- Ostrowski S., *Model zaangażowania w relacji usługodawca – klient*, Oficyna Wydawnicza Politechniki Gdańskiej, Gdańsk 2020.
- Pałęga M., *System zarządzania bezpieczeństwem informacji ISO/IEC 27001 w działalności logistycznej*, „Logistyka” 2014, nr 3.
- Parental trolling – wybrane zagadnienia prawne*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy” 2019, nr 32(3).
- Pherson R.H., Heuer R.J. Jr., *Structured analytic techniques for intelligence analysis*, Cq Press, 2000.
- Pieczywok A., *Polityczno-prawne strategie i dyrektywy przeciwdziałania cyberzagrożeniom*, „Cybersecurity and Law” 2023, nr 2(10).

- Piotrowski M., *Benchmarking klastrów w Polsce – edycja 2022. Raport ogólny*, PARP, Warszawa 2023.
- Pirch K., *Socjotechnika jako cyberzagrożenie* [w:] *Cyberbezpieczeństwo teoretycznie i empirycznie w naukach o bezpieczeństwie*, red. R.A. Janczewski, Wydawnictwo BP, Gdynia 2021.
- Pitts V., *Cyber Crimes: History of World's Worst Cyber Attacks*, Marousi 2017.
- Podręcznik Programu Interreg Polska-Słowacja 2021–2027.
- Pokrzyk D., Tarsa J., *Analiza poziomu wiedzy i zainteresowania tematyką e-biznesu wśród studentów Państwowej Wyższej Szkoły Zawodowej w Tarnowie*, „Progress in Economic Sciences” 2014, nr 1.
- Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, dokument przyjęty przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego, Warszawa 2013.
- Polkowska M., *Prawo bezpieczeństwa w Kosmosie*, Warszawa 2018.
- Polkowska M., *Regulacje prawne zasady „kultury bezpieczeństwa” w systemie raportowania zdarzeń w lotnictwie cywilnym*, „Palestra” 2013, nr 1–2.
- Pomykała M., *Bezpieczeństwo – W poszukiwaniu definicji*, „Zeszyty Naukowe Politechniki Rzeszowskiej. Zarządzanie i Marketing” 2010, 17.
- Prawo nowych technologii. Informatyzacja usług publicznych – założenia konstrukcyjne*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, WKP, Warszawa 2021, Lex el.
- Qayyum F. et al., *A Survey of Datasets, Preprocessing, Modeling Mechanisms, and Simulation Tools Based on AI for Material Analysis and Discovery*, “Materials” 2022, 15(4).
- Qiu J. et al., *A survey of machine learning for big data processing*, “EURASIP Journal of Advances in Signals Processing” 2016.
- Quantum Computing Cybersecurity Preparedness Act, Public Law No. 117–260 (12/21/2022).
- Quantum Technologies Flagship, Komisja Europejska, <https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship>.
- Racek E., Kosmowska S., *Factory technologies of the future – automation and digitalization of production in the aspect of Industry 4.0 concept*, „The Małopolska School of Economics in Tarnów Research Papers Collection” 2018, Vol. 40(4).
- Raczyk A., Dołzbłasz S., *Organizacje realizujące projekty współpracy transgranicznej na pograniczu polski-zmiany w latach 2007–2013 oraz 2014–2020*, „Research Papers of the Wrocław University of Economics/Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu” 2022, nr 66(3).
- Radoniewicz F., *Przeszukanie systemów informatycznych oraz informatycznych nośników danych w kodeksie postępowania karnego*, „Cybersecurity and Law” 2022, nr 2.
- Raport Antyfraudowy BIK, 2023 z badania na zlecenie BIK, „Cyberbezpieczeństwo Polaków 2023”*, N 1057, 18+, CAWI, Quality Watch.
- Raport ENISA 2023, Bruksela 2023.
- Raport roczny z działalności CERT Polska 2022. Krajobraz bezpieczeństwa polskiego Internetu, NASK-PIB/CERT Polska, Warszawa 2022.
- Ray P.P., *ChatGPT: A comprehensive review on background, applications, key challenges, bias, ethics, limitations and future scope*, “Internet of Things and Cyber-Physical Systems” 2023.
- Reginia-Zacharski J., *Wojna w świecie współczesnym*, Wydawnictwo Uniwersytetu Łódzkiego, Łódź 2014.
- Richards J., *The art and science of intelligence analysis*, Oxford University Press, 2010.

- Rogozińska-Pawelczyk A., *Przywództwo 4.0 w przedsiębiorstwach business services sector*, „Zarządzanie Zasobami Ludzkimi” 2022, nr 3–4 (146–147).
- Rojek T., *Koncepcja łańcucha wartości w zarządzaniu przedsiębiorstwem*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubezpieczenia” 2014, nr 803(66).
- Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, P. Barta, M. Kawecki, Warszawa 2018.
- Rybka A., Kozłowska K., *Interdyscyplinarne wymiary bezpieczeństwa w kształtowaniu przestrzeni zurbanizowanej*, „Zeszyty Naukowe Politechniki Częstochowskiej. Budownictwo” 2017, 23(173).
- Rychły-Lipińska A., *Model bezpieczeństwa jednostki we współczesnym zmieniającym się otoczeniu – wstępne rozważania*, „Studia nad Bezpieczeństwem” 2017, nr 2.
- Rydz D., Krakowiak M., Bajor T., *Zapewnienie bezpieczeństwa informacji w przedsiębiorstwie*, „Prace Naukowe Akademii im. Jana Długosza w Częstochowie. Technika, Informatyka, Inżynieria Bezpieczeństwa” 2013, t. 1.
- Sadowski J., *Cybernetyczny wymiar współczesnych zagrożeń*, „Studia nad Bezpieczeństwem” 2017, nr 2.
- Sanger D.E., *Cyberbroń – broń doskonała*, Wydawnictwo Helion, Gliwice 2021.
- Shinder D.L., *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004.
- Sienkiewicz P., *Bezpieczeństwo cyberprzestrzeni państwa*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Ekonomiczne Problemy Usług” 2012, nr 703(88).
- Sienkiewicz P., *Ewaluacja informacji w społeczeństwie informacyjnym*, „Ekonomiczne Problemy Usług” 2011, nr 67.
- Sienkiewicz P., *Wizje i modele wojny informacyjnej* [w:] L.S. Haber, *Spoleczeństwo informacyjne – wizja czy rzeczywistość*, Kraków 2004.
- Siergiejczyk M., Dudek E., *Ocena bezpieczeństwa i jakości informacji w systemach telematiki transportu*, „Autobusy” 2016, nr 12.
- Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo” 2012, nr 7–8.
- Skoczylas D., *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydent sieciowe*, „Prawo w Działaniu. Sprawy Karne” 2023, nr 53.
- Skowera D., *Akademia Cyberpolicyjna – Policja i organizacje międzynarodowe wobec wyzwań przestępczości internetowej*, „Zarządzanie Publiczne” Zeszyty Naukowe ISP UJ 2006, nr 2.
- Skowrońska M., *Zasady funkcjonowania, narzędzia oraz wyzwania dla marketingu XXI wieku*, „Prace Naukowe UE we Wrocławiu” 2017.
- Słownik języka polskiego PWN*, red. L. Drabik, Warszawa 2022.
- Ślusarczyk B., *Potencjalne rezultaty wprowadzania koncepcji Przemysłu 4.0 w przedsiębiorstwach*, „Przegląd Organizacji” 2019, nr 1(948).
- Smolarska M., *Naruszenie ochrony danych osobowych. Obowiązki administratora*, „ZN Politechniki Śląskiej Systemy Wspomagania w Inżynierii Produkcji” 2021, nr 10.
- Snarska S., *Marketing relacji w obrębie sieci dilerkiej – studium przypadku przedsiębiorstwa SaMASZ Sp. z o. o.*, „Marketing i Rynek” 2021, nr 11.
- Snoch J., *Irlandzka służba zdrowia padła ofiarą ataku ransomware*, „Komputer Świat” z 14.05.2021 r.
- Soesanto S., *The IT Army of Ukraine Structure, Tasking, and Eco-System*, “CSS Cyberdefense Reports”, Zurich 2022.
- Sprawozdanie o stanie bezpieczeństwa w lotnictwie cywilnym za 2022 rok*, Urząd Lotnictwa Cywilnego, Warszawa 2023.

- Stasiuk-Piekarska A., Hadaś Ł., M. Wyrwicka M., *Wybrane aspekty ryzyka organizacyjnego w koncepcji Przemysłu 4.0*, „Przedsiębiorczość i Zarządzanie” 2018, nr 5, Vol. 19.
- Steinhoff L. et al., *Online relationship marketing*, „Journal of the Academy of Marketing Science” 2019, Vol. 47(3).
- Su J., *Use of Outer Space for peaceful purposes: non-militarisation, non-aggression and prevention of weaponisation*, “Journal of Space Law” 2010, t. 36.
- Summary of NATO's Quantum Technologies Strategy*, NATO, 16.01.2024, https://www.nato.int/cps/en/natohq/news_221601.htm.
- Sun Tzu, *Sztuka wojny*, Warszawa 1994.
- Świętoniowska J., *Projekty innowacyjne motorem wdrażanych zmian w koncepcji Przemysłu 4.0*, „Przedsiębiorczość i Zarządzanie” 2018, nr 5, Vol. 19.
- Symon E., Rzepka P., *Wypadki drogowe w Polsce w 2022 roku*, Komenda Główna Policji, Warszawa 2023.
- Szczepaniuk E., *Bezpieczeństwo struktur administracyjnych w warunkach zagrożeń cyberprze-strzeni państwa*, Warszawa 2016.
- Szczygieł E., *Circular economy – a new concept or a necessity*, “Sprawy Międzynarodowe” 2021, 74(3).
- Szczygieł E., Kowalska K., *Meeting halfway – Understanding circular behaviours among households as a starting point for business practices*, “European Research Studies Journal” 2021, XXIV(3B).
- Szczygieł M., *Polityka cyberbezpieczeństwa Unii Europejskiej – początek drogi do strategicznej autonomii*, „Sprawy Międzynarodowe” 2018, nr 71(2).
- Szenc T., *Ochrona informacji niejawnych. Komentarz*, Warszawa 2007.
- Szpor G., *Art. 3 – Objasnienia określeń użytych w ustawie [w:] Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, wyd. II, Cz. Martysz, G. Szpor, K. Wojsyk, 2015 Lex el.
- Szpyra R., *Cyberbezpieczeństwo militarne w amerykańskiej praktyce*, Akademia Sztuki Wojennej, Warszawa 2016.
- Zubrycht T., *Współczesne aspekty bezpieczeństwa państwa*, „ZN AMW” 2006, 167(4).
- Taczowska-Olszewska J., *Dostęp do informacji publicznej w polskim systemie prawnym*, Wydawnictwo CH-Beck, 2013.
- Taufique K.M.R. et al., *Integrating General Environmental Knowledge and Eco-Label Knowledge in Understanding Ecologically Conscious Consumer Behavior* [w:] Fifth International Conference on Marketing and Retailing (5th Incomar) 2015, ed. Rashid, WEW, M. Muda, Vol. 37.
- Terlikowski M., *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Hacking, hakytywizm i cyberterroryzm* [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, Warszawa 2009.
- The Aim Initiative. A Strategy for Augmenting Intelligence Using Machines*, 2019. “The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines” (dni.gov).
- Tomaszewska A., *E-administracja jako nowy model funkcjonowania administracji publicznej*, Uniwersytet Szczeciński, Szczecin 2021.
- Tomaszewska-Michalak M., *Prawne i kryminalistyczne aspekty wykorzystania technologii biometrycznej w Polsce*, Warszawa 2015.
- Toumi M., *Regulacje prawa polskiego a zagrożenia w sieci Internet wobec małoletnich* [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Difin, Warszawa 2017.

- Trejderowski T., *Kradzież tożsamości. Terroryzm informatyczny*, Warszawa 2013.
- Tryboń M., Grabowska-Lepczak I., Kwiatkowski M., *Bezpieczeństwo człowieka w obliczu zagrożeń w XXI wieku*, „Zeszyty Naukowe SGSP. Szkoła Główna Służby Pożarniczej” 2011, nr 41.
- Turing A.M., *Computing Machinery and Intelligence*, „Mind” 1950, No. 49.
- Tyburcy T., *Mienie jako przedmiot ochrony w prawie karnym (na wybranych przykładach)*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2018, R. XXII, z. 3.
- UNICEF, *The State of The World’s Children 2017 Children in a Digital World*.
- Urbanek A., *Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa*, „Studia nad Bezpieczeństwem” 2016, nr 1.
- US Government, *A Tradecraft Primer: Structured analytic techniques for improving intelligence analysis*, “CIA Center for the study of intelligence” 2009.
- US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying, “Journal of Global Security Studies”, Oxford Academic (oup.com).
- Uwe Schrögl K., *Security in Outer Space: Rising Stakes for Civilian Space Programmes*, ESPI Conference September 27th 2018.
- Vadie A.S., Liptak K., *Przemysł 4.0: nowe wyzwania dla rynku pracy i warunków pracy na skutek pojawienia się robotów i automatyzacji*, „Studia Ekonomiczne i Regionalne” 2023, nr 3, Vol. 16.
- van Dis E.A. et al., *ChatGPT: five priorities for research*, “Nature” 2023, 614(7947).
- Vernile A., *The rise of private actors in the Space Sector*, ESPI, Springer 2018.
- Vinci A., *The Coming Revolution in Intelligence Affairs. How Artificial Intelligence and Autonomous Systems Will Transform Espionage*, “Foreign Affairs” August 31 2020, The Coming Revolution in Intelligence Affairs (foreignaffairs.com).
- von Clausewitz C., *O naturze wojny*, wyd. Jirafa Roja, Warszawa 2010.
- Wagłowski P., *Prawo w sieci. Zarys regulacji Internetu*, Helion, Gliwice 2005.
- Wang Y. et al., *The interaction relationships among agricultural certification labels or brands: Evidence from Chinese consumer preference for fresh produce*, “International Food and Agribusiness Management Review” 2022, 25(2).
- Warchoła A., *Zagrożenia dla bezpieczeństwa informacyjnego państwa u progu XXI wieku*, Stalowa Wola 2016.
- Warszewicz M., *Digitalizacja oraz transformacja cyfrowa. Studium Przypadku PKN Orlen S.A.* [w:] *Logistyka i transport*, red. J. Brach, N. Szozda, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2021.
- Washabaugh E., *The Robot, the Targeter and the Future of U.S. National Security*, The Robot, the Targeter and the Future of U.S. National Security (thecipherbrief.com).
- Wąsik K., *Międzynarodowe regulacje prawne dotyczące cyberprzestrzeni*, „Cybersecurity and Law” 2023, nr 2(10).
- Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Białystok 2017.
- Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego” 2013, nr 9(5).
- Wen Shien B.L., Yazdanifard R., *Relationship Marketing Vs Internet Marketing; which one Contribute to Gain Higher Level of Consumer Loyalty*, „Global Journal of Management and Business Research: E-Marketing” 2014, Vol. 14, Issue 7.
- Wieczorek P., *Wizja przemysłu nowej generacji – perspektywa dla Polski. Czwarta rewolucja przemysłowa*, „Kontrola Państwowa” 2018, nr 3.

- Wiewiórowski W.R., Wierczyński G., *Informatyka prawnicza*, Wolters Kluwer, Warszawa 2016.
- Wilk L., *Komentarz do art. 286 k.k. [w:] Kodeks karny. Część szczególna, t. 2: Art. 222–316*, red. M. Królikowski, R. Zawłocki, C.H. Beck, Warszawa 2017.
- Wing I., *The characteristic of successful and unsuccessful intelligence analysts*, "Journal of the Australian Institute of Professional Intelligence Officers" 2000, 9(2).
- Wiśniewska M., *Kompleksowe podejście do zarządzania bezpieczeństwem informacji – System Zarządzania Bezpieczeństwem Informacji*, „Zeszyty Naukowe Politechniki Łódzkiej. Organizacja i Zarządzanie” 2009, nr 45(1064).
- Wiszniewska J., *Influencer marketing – wybrane zagadnienia prawne*, ZNUJ. PPWI 2023, nr 3.
- Witecka M.S., *Zagrożenia asymetryczne a technologie informacyjne*, „Towarzystwo Wiedzy Obronnej” 2011, nr 4.
- Włodarczyk M., *Przyszłość komunikacji: e-mail marketing, hiperpersonalizacja i predictive marketing [w:] Biznes w sieci. Cyfrowe narzędzia przedsiębiorczości. Raport*, red. P. Kolenda, Warszawa: Wydaw. ICAN Institute, Warszawa 2016.
- Wodnicka M., *Wpływ czwartej rewolucji przemysłowej na innowacyjność usług*, „Optimum. Economic Studies” 2021, nr 3(105).
- Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, WKP 2020, LEX el.
- Woszek S., *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego” 2022, nr 27(14).
- Wróbel M., *Cyberprzestępczość w polskim systemie prawnym*, Warszawa 2014.
- Wrona J., *Przestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Białystok 2017.
- Współczesne pojmowanie bezpieczeństwa* red. J. Stańczyk, ISP PAN 1996.
- Wyrwisz J., *Wykorzystywanie narzędzi marketingu online do budowania interakcji z klientami [w:] Innowacyjne metody w inżynierii produkcji*, red. J. Lipski, A. Świć, A. Bojanowska, Wydawnictwo Politechniki Lubelskiej, Lublin 2014.
- Wzorce i zasady działania współczesnej administracji publicznej*, red. B. Jaworska-Dębska, P. Kledzik, J. Sługocki, WKP 2020, lex el.
- Xiang L. et al., *Cyber security threats: A never-ending challenge for e-commerce*, "Vietnam. Frontiers in Psychology" 2022, Vol. 13.
- Xu L.D. et al., *Embedding blockchain technology into IoT for security: A survey*, IEEE Internet of Things Journal" 2021, 8(13).
- Zabielska I., *Transgraniczna współpraca regionów [w:] Wybrane aspekty rozwoju regionalnego*, red. R. Kisiel, M. Wojarska, Fundacja Wspieranie i Promocja Przedsiębiorczości na Warmii i Mazurach, Olsztyn 2013.
- Zajac E., *14 sposobów na budowanie relacji z klientem (2016)*, <https://edytazajac.pl/budowanie-relacji-z-klientem/>.
- Zajac G., *Prawne i organizacyjne rozwiązania w zakresie bezpieczeństwa w lotnictwie cywilnym [w:] J. Sztucki, M. Gąsior, G. Zajac, M. Szczelina, Zarządzanie bezpieczeństwem lotnictwa cywilnego. Skrypt dydaktyczny*, Wrocław 2011.
- Żebrowski A., *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej. (Wywiad i kontrwywiad w latach 1989–2003)*, Kraków 2005.
- Zięba R., *Instytucjonalizacja bezpieczeństwa europejskiego*, Wydawnictwo Naukowe Scholar, Warszawa 2007.

- Ziółkowski B., *Challenges for Circular Economy Strategies in Polish Enterprises during the Pandemic Crisis*, "European Research Studies Journal" 2021, XXIV(4B).
- Ziółkowski B., Jankowska-Mihułowicz M., Moravec M., Wyrwa D., *Wstęp [w:] Etykiety i deklaracje środowiskowe – aspekty normatywne*, red. B. Ziółkowski, M. Jankowska-Mihułowicz, M. Moravec, D. Wyrwa, Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2021.
- Żołnierze z Rosji myśleli, że wysyłają zdjęcia atrakcyjnym kobietom. Szybko pożałowali*, „Komputer Świat”.
- Żywucka-Kozłowska E., Dziembowski R., *Wokół definicji cyberbezpieczeństwa*, „Cybersecurity and Law” 2023, nr 2(10).
- Nguyen A.T. et al., *Understanding the Importance of Eco-Labeling for Organic Foods at UNESCO Biosphere Reserves: A Case Study of the Cocoa Powder at the Dong Nai, Vietnam*, "Sustainability" 2023, 15(12).
- Maesano G. et al., *The Role of Credence Attributes in Consumer Choices of Sustainable Fish Products: A Review*, "Sustainability" 2020, 12(23).
- Tan D.N., *Evaluating WTA (Willingness to Accept) a Subsidy for Getting a VietGAP Certificate in Shrimp Farming: A Case Study in Tra Vinh Province, Vietnam*, "Egyptian Journal of Aquatic Biology and Fisheries" 2021, 25.
- Salmiah N.H.B., Ayu S.F., *Analysis of willingness to pay organic vegetables in Medan*, "IOP Conference Series: Earth and Environmental Science" 2021, 782(2), 022028.
- Wang E., Gao Z., *Chinese Consumer Quality Perception and Preference of Traditional Sustainable Rice Produced by the Integrated Rice – Fish System*, "Sustainability" 2017, 9(12).
- Barker M.E. et al., *Food Purchasing Decisions and Environmental Ideology: An Exploratory Survey of UK Shoppers*, "Sustainability" 2019, 11(22).
- Folkvord F. et al., *The effects of ecolabels on environmentally- and health-friendly cars: An online survey and two experimental studies*, "The International Journal of Life Cycle Assessment" 2020, 25(5).
- X. Ma X. et al., *Impact of Food Sustainability Labels on the Price of Rice in Online Sales*, "Foods" 2022, 11(23).

Akty prawne

- Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r. (Dz.U. nr 3, poz. 25).
- Konwencja o prawach dziecka przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r. (Dz.U. z 1991 r., nr 120, poz. 526).
- Konwencja o utworzeniu Europejskiej Agencji Kosmicznej, sporządzona w Paryżu dnia 30 maja 1975 roku (Dz.U. z 2013 r., poz. 61).
- Konwencja Rady Europy o cyberprzestępczości sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).
- Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 2016, nr 119).
- Rozporządzenie Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz.U. poz. 2039 oraz Dz.U. z 2004 r. poz. 597).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE(RODO) (Dz. Urz. UE. L z 4 maja 2016 r., nr 119).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/517 z dnia 19 marca 2019 r. w sprawie wdrażania i funkcjonowania Domeny Najwyższego Poziomu .eu, zmiany i uchylenia rozporządzenia (WE) nr 733/2002 oraz uchylenia rozporządzenia Komisji (WE) nr 874/2004 (Tekst mający znaczenie dla EOG.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 roku w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. Urz. UE L 151 z 07.06. 2019 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/947 z dnia 9 czerwca 2021 r. ustanawiające Instrument Sąsiedztwa oraz Współpracy Międzynarodowej i Rozwojowej – Globalny Wymiar Europy, zmieniające i uchylające decyzję Parlamentu Europejskiego i Rady nr 466/2014/UE oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/1601 i rozporządzenie Rady (WE, Euratom) nr 480/2009 (L 209/1), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32021R0947>.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L z 2016 r., nr 194).

Decyzja Parlamentu Europejskiego i Rady Nr 541/2014/UE z dnia 16 kwietnia 2014 r. ustanawiająca ramy wsparcia obserwacji i śledzenia obiektów kosmicznych (Dz.U. UE z 27.05. 2014 r.), L 158/227.

Decyzja Rady Europejskiej z dnia 25 marca 2011 roku w sprawie zmiany art. 136 Traktatu o funkcjonowaniu Unii Europejskiej w odniesieniu do mechanizmu stabilności dla państw członkowskich, których walutą jest euro (Dz.U. L 91 z dnia 6.04.2011 r.).

Europejska polityka kosmiczna – Rezolucja Parlamentu Europejskiego z dnia 20 listopada 2008 r. w sprawie europejskiej polityki kosmicznej: w jaki sposób przybliżyć przestrzeń kosmiczną do Ziemi (2010/C 16 E/11).

Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Sztuczna inteligencja dla Europy – Publications Office of the EU” (europa.eu).

Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Cyfrowy kompas na 2030 r.: europejska droga w cyfrowej dekadzie, Bruksela, dnia 9.03.2021 r., COM(2021) 118 final.

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., nr 78, poz. 483 ze zm.).

Ustawa z dnia 25 lutego 1964 r. Kodeks rodzinny i opiekuńczy (Dz.U. z 1964 r., nr 9, poz. 59 ze zm.).

Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (t.j. Dz.U. z 2023 r., poz. 2119).

Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz.U. z 2023 r., poz. 1465).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. z 2023 r., poz. 171).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz.U. z 2022 r., poz. 2509).

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2024 r., poz. 17).

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz.U. z 2024 r., poz. 37).

- Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r., poz. 902).
- Ustawa z dnia 21 grudnia 2001 r. o zmianie ustawy o organizacji i trybie pracy Rady Ministrów oraz o zakresie działania ministrów, ustawy o działaniach administracji rządowej oraz o zmianie niektórych ustaw (Dz.U. z 2001 r., nr 154, poz. 1800).
- Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. z 2023 r., poz. 1136).
- Ustawa z dnia 3 lipca 2002 r. Prawo lotnicze (t.j. Dz.U. z 2023 r., poz. 2110).
- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r., poz. 355).
- Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023 r. poz. 57 ze zm.).
- Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2023 r. poz. 122).
- Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz.U. z 2010 r. nr 40, poz. 230 – akt jednorazowy).
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz.U. z 2023 r. poz. 756 ze zm.).
- Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j. Dz.U. z 2024 r., poz. 30 ze zm.).
- Ustawa z dnia 23 listopada 2012 r. Prawo pocztowe (t.j. Dz.U. z 2023 r., poz. 1640).
- Ustawa z dnia 28 stycznia 2016 r. Prawo o prokuraturze (t.j. Dz.U. z 2023 r., poz. 1360).
- Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j. Dz.U. z 2022 r., poz. 2632).
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2019 r., poz. 1781).
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2023 r., poz. 913 ze zm.).
- Ustawa z dnia 16 listopada 2023 r. Prawo bankowe (t.j. Dz.U. z 2023 r., poz. 2488 ze zm.).
- Ustawa z dnia 6 kwietnia 2023 r. o odpowiedzialności podmiotów zbiorowych za czyny zabronione pod groźbą kary (t.j. Dz.U. z 2023 r., poz. 659 ze zm.).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r., poz. 526 ze zm.).
- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (t.j. Dz.U. z 2017 r., poz. 2247 ze zm.).
- Rozporządzenie Rady Ministrów z dnia 28 marca 2007 roku ustanawiające Plan Informatyzacji Państwa na lata 2007–2010 (Dz.U. z 2007 r., nr 61, poz. 415 ze zm.).
- Rozporządzenie Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczenia informacji niejawnych (Dz.U. z 2012 r., poz. 683).
- Uchwała nr 17 Rady Ministrów z dnia 12 lutego 2013 roku w sprawie przyjęcia strategii „Sprawne Państwo 2020” (M.P. poz. 136).
- Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 (MP. z 2019 r., poz. 1037).

Orzecznictwo

- Wyrok Sądu Najwyższego z dnia 14 kwietnia 2004 r., I CKN 308/01, LEX nr 80243.
- Wyrok Sądu Najwyższego z dnia 16 stycznia 2008 r., IV CSK 380/07, OSNC-ZD 2008/D/102.
- Wyrok Sądu Najwyższego z dnia 18 stycznia 2018 r., wydany w sprawie o sygn. akt V CSK 141/17.
- Wyrok Sądu Apelacyjnego w Krakowie z dnia 5 czerwca 2002 r., sygn. akt II AKa 128/02, KZS 2002, nr 6, poz. 16, LEX nr 56953.
- Wyrok Sądu Apelacyjnego w Warszawie z dnia 8 października 2021 r., sygn. VII AGa 228/20.
- Wyrok Sądu Okręgowego w Warszawie z dnia 12 maja 2018 r., wydany w sprawie o sygn. akt: I C 566/17.
- Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 7 sierpnia 2020 r., sygn. akt II SA/Wa 809/20, Legalis nr 2551068.
- Orzeczenie Sądu Okręgowego w Paryżu z dnia 20 października 2000 roku w sprawie Anit-Semitism LICRA v. Yahoo Inc., sygn. akt RG 00/05308.

Netografia

- A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security, Rada UE, 21.03.2022, <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>.
- Banach A., Phishing zagrożeniem dla e-biznesu, “E-mentor” 2005, nr 5(12), <https://www.e-mentor.edu.pl/artykul/index/numer/12/id/227>.
- Banach A., Voice over Internet Protocol – telefonowanie przez internet, <https://www.e-mentor.edu.pl/artykul/index/numer/10/id/173>.
- Biderman B., *Phishing*, <https://cebrf.knf.gov.pl/encyklopedia/hasla/385-definicje/818-phishing>.
- Big Room (2024). *Ecolabel Index*, <https://www.ecolabelindex.com/>.
- Bińkowska B., *Budowanie relacji on-line z klientami (2021)*, <https://zdalni.pl/budowanie-relacji-online-z-klientem/>.
- Cambridge Dictionary “*Cyberattack*”, <https://dictionary.cambridge.org/pl/dictionary/english/cyberattack>.
- Co to jest wskaźnik laserowy?*, <https://pl.theastrologypage.com/laser-pointer>.
- Defence Agency, 2021 Issue 22, <https://eda.europa.eu/docs/default-source/eda-magazine/edm22singleweb.pdf>.
- Defense Budget Overview*, Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2023/FY2023_Budget_Request_Overview_Book.pdf.
- Definicje i rodzaje przemocy* – <https://www.oik.jaworzno.pl/art,6,definicja-i-rodzaje-przemocy>.
- Druk 2505 z dnia 30 kwietnia 2018 roku. Uzasadnienie do Rządowego projektu ustawy o krajowym systemie cyberbezpieczeństwa, <https://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2505>.
- EU Policy on Cyber Defence, Komisja Europejska, 10.11.2022, https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf.
- Fraday L., *Chat GPT-4 vs Chat GPT-3: What’s the Difference, and Which Is Better?*, 2023, <https://history-computer.com/chat-gpt-4-vs-chat-gpt-3/>.
- Fung B., *5.1 million Americans have security clearances. That’s more than the entire population of Norway*, The Washington Post, <https://www.washingtonpost.com/news/the-switch/wp/>

2014/03/24/5-1-million-americans-have-security-clearances-thats-more-than-the-entire-population-of-norway/.

Gierasimow W., *Doktryna Wojenna Federacji Rosyjskiej*, [https://www.bbn.gov.pl/ftp/dok/01/Doktryna Federacji Rosyjskiej.pdf](https://www.bbn.gov.pl/ftp/dok/01/Doktryna%20Federacji%20Rosyjskiej.pdf).

Gorecki B., *Minister obrony Rosji: Główny cel na Ukrainie został „udany osiągnięty”*, <https://furora.tv/minister-obrony-rosji-glowny-cel-na-ukrainie-zostal-udany-osiagniety/>.

<http://www.vpk-news.ru/articles/14632>.

<https://2017.cybersecforum.eu/global-cybersecurity-initiative-launched-strengthen-collaboration-between-regional-ecosystems>.

[https://apwg.org/ Raport](https://apwg.org/Raport)

<https://biometriq.pl/prywatnosc-w-biometrii-glosowej>.

<https://bip.brpo.gov.pl/pl/content/rzecznik-w-sprawie-rozpoznawania-glosu-osob-dzwonia-cych-na-krajowa-informacje-podatkowa>.

https://blog.businessweb.pl/system-crm-przyklady?utm_campaign=%5BDSA%5D+-+Wpisy&utm_medium=ppc&utm_source=adwords&utm_term=&hsa_src=g&hsa_ad=666590684856&hsa_cam=20387279505&hsa_grp=151596349157&hsa_kw=&hsa_acc=2108719825&hsa_tgt=dsa-2171658798608&hsa_net=adwords&hsa_mt=&hsa_ver=3&gad=1&gclid=Cj0KCQjwpompBhDZARIsAFD_Fp8Aw1knaJGm8AbM4WXV4B_p4Q64YDX99kaCa8vz6TKGVhejd4aqmTsaArGHEALw_wcB.

https://cba.gov.pl/ftp/publikacje/Korupcja_na_przestrzeni_wiekow.pdf.

<https://ccit.pl/jaka-jest-roznica-miedzy-ochrona-danych-a-bezpieczenstwem-informacji>.

<https://cert.pl/o-nas/>.

<https://cybermadeinpoland.pl>.

<https://dais.pl/social-media-marketing-wszystko-co-musisz-o-nim-wiedziec/>.

<https://digital-strategy.ec.europa.eu/pl/policies/digital-public-services>.

<https://dynamics.microsoft.com/pl-pl/crm/how-to-build-crm-strategy/>.

https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4619.

<https://ec.europa.eu/docsroom/documents/28325/attachments/1/translations/en/renditions/native>.

[https://epodrecznik.mc.gov.pl/mediawiki/index.php?title=Elektroniczna_platforma_us%C5%82ug_administracji_publicznej_\(ePUAP\)](https://epodrecznik.mc.gov.pl/mediawiki/index.php?title=Elektroniczna_platforma_us%C5%82ug_administracji_publicznej_(ePUAP)).

<https://e-prawnik.pl/informacje/ustawa-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej.html>.

<https://eur-lex.europa.eu/EN/legal-content/summary/eeurope-an-information-society-for-all.html#>.

<https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32002R0733>.

<https://forumakademickie.pl/sprawy-nauki/politechnika-rzeszowska-czlonkiem-klastra-industry-4-0>.

<https://freshmail.pl/wysylka-sms/>.

<https://fundacijapoint.pl/2017/02/w-internecie-nic-nie-ginie/>.

<https://gdpr.pl/iso-27701-miedzynarodowy-standard-dotyczacy-ochrony-danych-osobowych>.

<https://globalepic.org>.

<https://home.pl/reklama-internetowa/pozycjonowanie/>.

<https://itarmy.com.ua/?lang=en> (oficjalna strona AITU).

<https://klasterodpadowy.com/portal/oferta-klastra/proinno>.

<https://komunikatywnie.pl/2021/05/26/sharenting-co-czwarty-rodzic-publikuje-informacje-o-swoich-dzieciach-w-mediach-spolesnosciovych/>.

<https://ks.pl/sloownik/co-to-jest-dns>.

<https://polszczyzna.pl/incyident-co-to-jest-definicja-synonimy-przyklady-uzycia-sloownik/>.

<https://pushsec.pl/bezpieczenstwo-informacji-co-to/>.

<https://pwr.edu.pl/uczelnia/aktualnosci/dolnoslaski-klaster-cyberbezpieczenstwa-zainaugurowal-dzialalnosc-11079.html>.

<https://reasonsmysoniscrying.tumblr.com/page/3>.

<https://rf.gov.pl/nieautoryzowane-transakcje-platnicze-analiza-2020/>.

<https://rozwiwania-antyfraudowe.bik.pl/raporty/2023#scrollform>.

<https://sjp.pl/e-administracja>.

<https://sjp.pwn.pl/sloowniki/incyident.html>.

<https://sjp.pwn.pl/sloowniki/informatyzacja.html>.

https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-4/48035,Utrwalanie-wizerunku-nagiej-osoby-bez-jej-zgody-art-191a.html?fbclid=IwAR2OK04tfRaK0_jzxwKf31Ckrq_atjAr6DZid7IIgMHgDfQ43gkSFzz0FE.

<https://tvn24.pl/ciekawostki/pozwala-rodzicow-za-opublikowanie-jej-zdjec-z-dziecinstwa-ra678737>.

https://twitter.com/UCA_ruhate (oficjalny profil grupy).

https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.

<https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html>

<https://www.egress.com/>.

https://www.europarl.europa.eu/factsheets/pl/sheet/134/bezpieczenstwo-lotnicze#_ftn3.

<https://www.europarl.europa.eu/highlights/pl/1001.html>.

<https://www.gov.pl/web/baza-wiedzy/wspolnie-dla-cyberbezpieczenstwa>.

<https://www.gov.pl/web/cyfryzacja/program-zintegrowanej-informatyzacji-panstwa>.

<https://www.gov.pl/web/cyfryzacja/ustawa-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej-juz-niedlugo-wejdzie-w-zycie--sprawdz-korzysci-jakie-niesie-to-dla-ciebie-i-twoich-bliskich>.

<https://www.gov.pl/web/cyfryzacja/ustawa-o-zwalczaniu-naduzyc-w-komunikacji-elektronicznej-juz-niedlugo-wejdzie-w-zycie--sprawdz-korzysci-jakie-niesie-to-dla-ciebie-i-twoich-bliskich>.

<https://www.gov.pl/web/ia/budowa-interoperacyjnego-systemu-teleinformatycznego>.

<https://www.gov.pl/web/ia/kluczowe-publiczne-systemy-it-lista>.

<https://www.ifirma.pl/blog/zwalczanie-naduzyc-w-komunikacji-elektronicznej-zmiany-2023.html>.

<https://www.money.pl/gospodarka/wojna-w-ukrainie-ukraincy-wykorzystali-profile-pieknych-kobiet-dla-rosjan-skonczylo-sie-tragicznie-6809431044450944a.html>.

<https://www.orange.pl/omnibook/moj-glos-weryfikacja-glosem#dla-klienta#brak#jak-wyrazic-lub-odwolac-zgode-na-weryfikacje-glosem-proste-kroki>.

<https://www.polsatnews.pl/wiadomosc/2019-11-20/historyczna-decyzja-nato-kosmos-uznany-za-obszar-dzialan-operacyjnych/>

<https://www.saos.org.pl/judgments/370187>.

https://www.slaskie.pl/images/STRATEGIA/strat_L.pdf.

- <https://www.telekom.com/en/company/data-privacy-and-security/digitally-secure/details/be-careful-when-sharing-children-s-photos-1041684>.
- <https://www.ulc.gov.pl/pl/kampanie-edukacyjne/5317-laser-to-nie-zabawka>.
- <https://www.wroclawskiportal.pl/razem-w-kierunku-bezpieczenstwa-w-sieci-cele-makroklastra>.
- <https://www.verizon-com>.
- Interreg A NEXT Poland-Ukraine, <https://pl-ua.eu/pl/pages/579>.
- Karlik P., Bergmann M., *Phising – znane zagrożenia w realiach epidemii*, <https://www.filipiak-babicz.com/assets/files/ALERT%20Phishing%20znane%20zagro%C5%BCenie%20w%20realiach%20epidemii.pdf>.
- Kasprzak A., *System zarządzania bezpieczeństwem informacji*, <https://lexdigital.pl/system-zarzadzania-bezpieczenstwem-informacji>.
- Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. II, Warszawa 2022*, <https://sip.lex.pl/#/commentary/587773148/670976/fajgielski-pawel-komentarz-do-rozporzadzenia-nr-2016-679-w-sprawie-ochrony-osob-fizycznych-w...?cm=URELATIONS>.
- Komisja Europejska, *Komisja zawiesza współpracę transgraniczną i transnarodową z Rosją i Białorusią*, https://ec.europa.eu/regional_policy/whats-new/newsroom/03-04-2022-commission-suspends-cross-border-cooperation-and-transnational-cooperation-with-russia-and-belarus_pl.
- Komisja Nadzoru Finansowego, https://www.knf.gov.pl/knf/pl/komponenty/img/Bezp_finansowe_39005.pdf.
- Komisja Nadzoru Finansowego, *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*, Warszawa 2013, https://www.knf.gov.pl/knf/pl/komponenty/img/Rekomendacja_D_8_01_13_uchwala_7_33016.pdf.
- Komunikacja w Internecie – jednostronna i interaktywna*, <http://www.systemycms.com/artykuly/slownik/148.html> [za:] A. Warchoń, *(Nie) bezpieczeństwo w cyberprzestrzeni* [w:] *Współczesne zagrożenia bezpieczeństwa państwa*, A. Żebrowski, E. Sadowska, I. Szkurląt, A. Warchoń, Kraków–Stalowa Wola 2018.
- Kruglashov A., Shvydiuk S., *Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory*, Wschód Europy, <http://journals.umcs.pl/we>.
- Kwanty w PIONIERZE*, Poznańskie Centrum Superkomputerowo-Sieciowe, <https://www.news.pionier.net.pl/kwanty-w-pionierze/>.
- Lukianski M., *Why every business needs a great website*, 2019, <https://www.droptica.com/blog/why-every-business-needs-great-website/>.
- Lynn W.J. III, *Defending a New Domain. The Pentagons Cyberstrategy*, <https://www.jstor.org/stable/20788647>.
- Łużak T., *Whaling oraz Business Email Compromise – na czym polegają te ataki?*, <https://www.netia.pl/pl/srednie-i-duze-firmy/youtra-strefa-wiedzy/na-czym-polega-whaling-oraz-bec>.
- Łysak S., *Marketing relacji – jak budować skuteczną relację z klientem*, https://blog.skyshop.pl/budowanie-relacji-z-klientem-marketing-relacji-w-sklepie-internetowym/?gad=1&gclid=EAIAIqobChMI4LiM96HagAMVQUCRBR2aUw70EAMYAyAAEgIsaPD_BwE.

Mileszko T., *Stan permanentnej cyberwojny. Jak wygląda to od środka i po jakie metody sięgają państwo hakerzy?* <https://www.komputerswiat.pl/artykuly/redakcyjne/stan-permanentnej-cyberwojny-jak-wyglada-to-od-srodka-i-po-jakie-metody-siegaja/yb7n35r>.

Minister Cyfryzacji: będę dążył do powołania specjalnego funduszu dotyczącego AI, PAP, 21.01.2024, <https://www.pap.pl/aktualnosci/minister-cyfryzacji-bede-dazyl-do-powolania-specjalnego-funduszu-dotyczacego-ai>.

Moszczyńska A., *Opinia prawna dotycząca phishingu*, <https://adwokatmoszczynska.pl/aktualnosci/opinia-prawna-dot-phishingu-czesc-2>.

Motylińska P., Warchoń A., *Phising*, <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/phising/>.

NASK realizuje projekt z zakresu technologii kwantowych, NASK, <https://www.nask.pl/pl/aktualnosci/4250,NASK-realizuje-projekt-z-zakresu-technologii-quantowych.html>.

National Cyber Strategy 2022 (www.gov.uk).

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, The White House, 04.05.2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/>.

NATO releases first ever quantum strategy, NATO, 17.01.2024, https://www.nato.int/cps/en/natohq/news_221601.htm.

Niezdropa D., *Antylaserowa ochrona wzroku funkcjonariuszy*, <https://magazyn-ksp.policja.gov.pl/mag/wyposazenie/120992,Antylaserowa-ochrona-wzroku-funkcjonariuszy.html>.

Nowe konkursy na projekty w obszarze cyberbezpieczeństwa w programie Cyfrowa Europa, Krajowe Centrum Kompetencji Cyberbezpieczeństwa, <https://www.gov.pl/web/cyber-nccpl/nowe-konkursy-na-projekty-w-obszarze-cyberbezpieczenstwa-w-programie-cyfrowa-europa>.

O programie, <https://pl-ua.eu/pl/pages/578>.

Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, wersja 1.0, maj 2019, www.uodo.gov.pl.

Olech A.K., Lis A., *Technologia i terroryzm. Sztuczna inteligencja w dobie zagrożeń terrorystycznych*, Instytut Nowej Europy, <https://ine.org.pl/technologia-i-terroryzm-sztuczna-inteligencja-w-dobie-zagrozen-terrorystycznych/>.

Oltrogge D., *Marshalling Space Traffic Management requirements and expectations in the international context*, ESPI 12th Autumn Conference; <https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/>.

Opracowanie, implementacja i ocena bezpieczeństwa algorytmów postkwantowych pk. APQ, Uniwersytet Warszawski, <http://centrum.tdb.uw.edu.pl/opracowanie-implementacja-i-ocena-bezpieczenstwa-algorytmow-postkwantowych-pk-apq>.

OptoKrypt, TELDAT, <https://www.teldat.com.pl/projekty/projekty-wspolfinansowane-ze-srodkow-krajowych/453-optokrypt.html>.

Paulauskas K., *Przestrzeń kosmiczna: najnowsze graniczne wyzwanie dla NATO*, <https://www.nato.int/docu/review/pl/articles/2020/03/18/przestrzen-kosmiczna-najnowsze-graniczne-wyzwanie-dla-nato/index.html>

PN-EN ISO/IEC 27002 Technika informatyczna – Techniki bezpieczeństwa – Praktyczne zasady zabezpieczania informacji, <https://www.pkn.pl/informacje/2018/01/zarzadzanie-bezpieczenstwem-informacji>.

- Podręcznik Programu Interreg Polska-Słowacja 2021–2027, <https://pl.plsk.eu/dokumenty-dla-wnioskodawcow>.
- Polska-Słowacja, <https://www.ewt.gov.pl/strony/o-programach/programy-interreg-2021-2027/program-interreg-polska-slowacja-2021-2027/>.
- Porras D.A., *Nowe wojny kosmiczne*, <https://krytykapolityczna.pl/swiat/nowe-wojny-kosmiczne/>.
- Priorytetowe kierunki badań naukowych w resorcie obrony narodowej w latach 2021–2035, MON, Warszawa 2023, <https://www.gov.pl/attachment/8d8d60db-92ec-4c03-8714-148d0e2a6899>.
- Program Interreg A NEXT Poland-Ukraine, <https://pl-ua.eu/pl/pages/579>.
- Program Polska-Ukraina z nowym budżetem!, <https://pl-ua.eu/pl/news/2983>.
- Program współpracy transgranicznej Interreg Polska-Słowacja 2021–2027, https://pl.plsk.eu/documents/15954/751291/Program+wspolpracy+transgranicznej+Interreg+Polska+%E2%88%92+Słowacja+2021-2027_obowiazujacy+od+20.09.2023+r/aaddec0e-8ac8-4a46-a07a-f48b16b90467.
- Program współpracy transgranicznej Interreg Polska-Słowacja 2021–2027, <https://pl.plsk.eu>.
- Programy Europejskiej Współpracy Terytorialnej i Europejskiego Instrumentu Sąsiedztwa, <https://www.ewt.gov.pl/strony/o-programach/przeczytaj-o-programach/>.
- Programy Interreg 2021–2027 – podstawowe informacje, <https://www.ewt.gov.pl/strony/o-programach/programy-interreg-2021-2027/programy-interreg-2021-2027-podstawowe-informacje/>.
- Projekt Pionier-Q*, Akademickie Centrum Komputerowe Cyfronet AGH, https://www.cyfronet.pl/projekty/19407,artykul,projekt_pionier_q.html.
- Przełomowa technologia kwantowa z WAT*, Wojskowa Akademia Techniczna, 11.08.2023, <https://www.wojsko-polskie.pl/wat/articles/aktualnosci-w/2-przelomowa-technologia-kwantowa-z-wat/>.
- Przemoc słowna – sześć sygnałów, że jesteś ofiarą* – <https://krokdozdrowia.com/przemoc-slowna-jestes-ofiara>.
- Rekomendacje Pełnomocnika Rządu ds. cyberbezpieczeństwa dotycząca oprogramowania Kaspersky, Ministerstwo Cyfryzacji, 30.05.2022, <https://www.gov.pl/web/baza-wiedzy/rekomendacje-pelnomocnika-rzadu-ds-cyberbezpieczenstwa-dotyczaca-oprogramowania-kaspersky>.
- Roczne sprawozdanie dyrektora NASK-PIB z wykonania zadań w 2022 r., NASK, <https://bip.nask.pl/download/2/2665/RoczneSprawozdanieDyrektoraNASKPIBza2022rok.pdf> Warszawa 2023.
- RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, Warszawa 2018, art. 32, <https://sip.lex.pl/#/commentary/587747173/544613/bielak-jomaa-edytared-lubasz-dominik-red-rodo-ogolne-rozporzadzenie-o-ochronie-danych-komentarz?pit=2024-01-29&cm=URELATIONS>.
- Sallam M., *ChatGPT utility in healthcare education, research, and practice: Systematic review on the promising perspectives and valid concerns*, „Healthcare” 2023, 11(6).
- Samuels B., *Feinstein to tech execs: ‘I don’t think you get it’*, <https://thehill.com/business-a-lobbying/358232-feinstein-to-tech-cos-i-dont-think-you-get-it/>.
- Sanger D.E., Broad W.J., *How U.S. Intelligence Agencies Underestimated*, „New York Times”, <https://www.nytimes.com/2018/01/06/world/asia/north-korea-nuclear-missile-intelligence.html>.

- Sanger D.E., Kirkpatrick D., Perloth N., *The World Once Laughed at North Korean Cyberpower. No More*, <https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html>.
- Sanger D.E., Markoff J., *After Google's Loud Stance on China, US Treads Lightly*, „The New York Times”, <https://www.cnn.com/2010/01/15/after-googles-loud-stance-on-china-us-treads-lightly.html>.
- Sanger D.E., *Tiny Satellites From Silicon Valley May Help Track North Korea Missiles*, New York Times, <https://www.nytimes.com/2017/07/06/world/asia/pentagon-spy-satellites-north-korea-missiles.html>.
- Science & Technology Trends 2023–2043*, NATO Science & Technology Organization, 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf.
- Sejfer R., Marti J., *Have ecolabels had their day? The truth behind sustainability labels from the people who integrate them*, IMD, 2012, https://imd.widen.net/view/pdf/9im6zwqnpn/tc032-12_have-ecolabels-had-their-days.pdf.
- Slownik terminów i definicji NATO AAP-6*, http://wcnjk.wp.mil.pl/plik/file/N_20130808_AAP6PL.pdf.
- Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2022, <https://uodo.gov.pl/pl/487/2279>.
- Steves M.P., Greene K.K., Theofanos M.F., *A phish scale: rating human phishing message detection difficulty*, https://www.ndss-symposium.org/wp-content/uploads/2019/02/usec2019_02-4_Steves_paper.pdf.
- Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.
- Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, <https://www.dziennikustaw.gov.pl/M2019000103701.pdf>.
- Strategia Narodowa USA z 12 października 2022 r. (www.whitehouse.gov).
- Systemy CRM i nowoczesny marketing relacyjny*, <https://www.egospodarka.pl/25401,Systemy-CRM-i-nowoczesny-marketing-relacyjny,1,20,2.html>.
- Technologie kwantowe w ITWL*, Instytut Techniczny Wojsk Lotniczych, 15.06.2021, <https://itwl.pl/aktualnosci/424-technologie-quantowe-w-itwl>.
- The European Quantum Communication Infrastructure (EuroQCI) Initiative*, Komisja Europejska, <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>.
- The EU's Cybersecurity Strategy for the Digital Decade, Komisja Europejska, 16.12.2020, <https://ec.europa.eu/newsroom/dae/redirection/document/72164>.
- The Hacktivism Declaration*. cDc communications, http://www.cultdeadcow.com/cDc_files/declaration.html.
- Toulas B., *Signal adds quantum-resistant encryption to its E2EE messaging protocol*, Bleeping Computer, 20.11.2023, <https://www.bleepingcomputer.com/news/security/signal-adds-quantum-resistant-encryption-to-its-e2ee-messaging-protocol/>.
- Trimble S., *UK Minister: Military Aircraft Must Be Ready For Quantum Computing*, Aviation Week, 14.07.2023, <https://aviationweek.com/defense-space/aircraft-propulsion/uk-minister-military-aircraft-must-be-ready-quantum-computing>.
- Ukraine power cut 'was cyber-attack'*, BBC News, <https://www.bbc.com/news/technology-38573074>.

Ukraińscy hakerzy włamali się do rosyjskiego systemu rezerwacji biletów, Informacyjna Agencja Radiowa, <https://radioszczecin.pl/6,462214,ukrainscy-hakerzy-wlamali-sie-do-rosyjskiego-sys>, informacja z 05.10.2023 r.

UNHCR (2022), *GLOBAL TRENDS – FORCED DISPLACEMENT IN 2022*, <https://www.unhcr.org/sites/default/files/2023-06/global-trends-report-2022.pdf>.

United Nations, Agenda 21. The United Nations Programme of Action from Rio. Rio de Janeiro, Brazil 1992. United Nations Conference on Environment and Development, <http://www.un.org/esa/dsd/agenda21/>.

UNOPS (2009), *A GUIDE TO ENVIRONMENTAL LABELS – for Procurement Practitioners of the United Nations System*, https://www.un.org/Areas/Public/Downloads/Env_Labels_Guide.pdf.

van Amerongen M., *Quantum technologies in defence & security*, NATO Review, 22.01.2024, <https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html>.

Vaughan-Nichols S., *GPT-3.5 vs GPT-4: Is chatgpt plus worth its subscription fee?*, “ZDNET” 2023, <https://www.zdnet.com/article/gpt-3-5-vs-gpt-4-is-chatgpt-plus-worth-its-subscription-fee/>.

Zaloga śmigłowca LPR oślepią laserem. Lekarz ma uszkodzony wzrok, <https://www.polsat-news.pl/wiadomosc/2019-09-23/zaloga-smiglowca-lpr-oslepiona-laserem-lekarz-ma-uszkodzony-wzrok/>.

Zieliński J., *Budowanie relacji z klientami. 7 dobrych praktyk (2022)*, <https://zielinskijezry.com/blog/budowanie-relacji-z-klientem/>.

Сквозные цифровые технологии”, Технополис ЭРА, <https://www.era-tehnopolis.ru/technologies/skvoznnye-tsifrovye-tekhnologii/>.

Указ Президента Российской Федерации от 02.07.2021 № 400 "О Стратегии национальной безопасности Российской Федерации", <http://publication.pravo.gov.ru/Document/View/0001202107030001>.

Inne

Decyzja Prezesa Urzędu Ochrony Danych Osobowych z dnia 30 listopada 2022 r., DKN.5112.5.2021, Legalis.

Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie: „Postawy przedsiębiorcze a strategia lizbońska”, Dz.U. UE. C. 2008.44.84 z dnia 16.02.2008 r., lex el.

Opinia Komitetu Regionów „Usługa powszechna w łączności elektronicznej” oraz „Przyszłość sieci i Internetu”, Dz.U. UE. C. 2009.120.41 z dnia 28.05.2009 r.

Final Report National Security Commission on Artificial Intelligence. 2021. Final Report – NSCAI.

Opinia 3/2014 w sprawie powiadamiania o przypadkach naruszenia danych osobowych z dnia 25 marca 2014 roku (wersja polska).

Zagrożenia i wyzwania bezpieczeństwa w cyberprzestrzeni

Streszczenie

We współczesnym świecie zagrożenia w cyberprzestrzeni są coraz poważniejszym wyzwaniem i obejmują coraz więcej obszarów, zagrażając już nie tylko bezpieczeństwu wewnętrznemu, ale też bezpieczeństwu poszczególnych państw. Wydaje się, że w najbliższej przyszłości będą one poddawane dalszej ewolucji i różnicowaniu, w miarę jak zaawansowane technologie informatyczne będą się rozprzestrzeniać na kolejne obszary życia społecznego. Będzie też wzrastać liczba podmiotów zdolnych i zamierzających obrać za cel państwo w cyberprzestrzeni, a państwa będą prowadziły coraz częściej działania zakłócające, w tym z wykorzystaniem podmiotów zastępczych. Przejście na pracę hybrydową i ograniczenia w podróżach międzynarodowych, będące skutkiem pandemii COVID-19, doprowadziły do większego uzależnienia od usług cyfrowych i zachęciły zorganizowane grupy przestępcze do zwiększenia intensywności ataków w cyberprzestrzeni. Sytuacja ta przyniosła znacznie szybszy niż do tej pory wzrost liczby cyberprzestępstw.

Celem monografii jest przekrojowa i interdyscyplinarna analiza problemów bezpieczeństwa państwa w cyberprzestrzeni oraz zagrożeń z tym związanych. Dlatego też autorzy podjęli próbę wskazania zarówno istoty cyberprzestrzeni jako nowej kategorii badań nad bezpieczeństwem państwa, jak również identyfikacji uwarunkowań cyberbezpieczeństwa państwa, głównych przestępstw powiązanych z cyberprzestrzenią i ochroną danych osobowych oraz wyzwań, jakie pociąga za sobą gospodarka funkcjonująca w obszarze cybersfery. Przedmiotem badawczym są zatem zagrożenia w cyberprzestrzeni, natomiast podmiotem badawczym jest państwo, obywatele i podmioty pozapaństwowe. W pracy zostały przedstawione i przeanalizowane zależności i rozbieżności problemów bezpieczeństwa wewnętrznego państwa i organizacji międzynarodowych oraz uwarunkowania polityki bezpieczeństwa państwa.

Monografia składa się z pięciu części, podzielonych na obszary tematyczne: problemy definiowania cyberbezpieczeństwa, zwalczanie cyberprzestępczości, cyberbezpieczeństwo w obszarze ochrony danych osobowych, wyzwania cyberbezpieczeństwa w obszarze gospodarki, cyberbezpieczeństwo a obronność.

Threats and security challenges in cyberspace

Summary

In today's world, cyber threats are an increasingly serious challenge and cover more and more areas, no longer threatening not only internal security, but also the security of individual states. It seems that they will undergo further evolution and diversification in the near future, as advanced information technologies spread to more areas of society. There will also be an increase in the number of actors capable of and intent on targeting the state in cyberspace, and states will use a wider range of levers to conduct disruptive activities, including using proxy actors. The shift to hybrid work and restrictions on international travel as a result of the COVID-19 pandemic have led to greater reliance on digital services and encouraged organized crime groups to increase the intensity of attacks in cyberspace. This situation has resulted in a much faster increase in cybercrimes than before.

The purpose of the monograph is a cross-cutting and interdisciplinary analysis of the problems of state security in cyberspace and the risks associated with it. Therefore, the authors have attempted to identify both the essence of cyberspace as a new category of state security research, as well as to identify the determinants of state cyber security, the main crimes related to cyberspace and the protection of personal data, and the challenges posed by the economy operating in the cybersphere. Thus, the research subject is the threats in cyberspace, while the research subject is the state, citizens and non-state actors. The work presents and analyzes the interrelationships and divergence of internal security problems of the state and international organizations, and the determinants of state security policy.

The monograph consists of five parts, divided into thematic areas: problems of defining cyber security, combating cyber crime, cyber security in the area of personal data protection, challenges of cyber security in the area of economy, cyber security and defense.

DOCUMENT
CREATED
WITH



PDF
COMBINER

PDF Combiner is a free application that you can use to combine multiple PDF documents into one.

Three simple steps are needed to merge several PDF documents. First, we must add files to the program. This can be done using the Add files button or by dragging files to the list via the Drag and Drop mechanism. Then you need to adjust the order of files if list order is not suitable. The last step is joining files. To do this, click button Combine PDFs.

Main features:

secure PDF merging - everything is done on your computer and documents are not sent anywhere

simplicity - you need to follow three steps to merge documents

possibility to rearrange document - change the order of merged documents and page selection

reliability - application is not modifying a content of merged documents.

Visit the homepage to download the application:

www.jankowskimichal.pl/pdf-combiner

To remove this page from your document, please donate a project.