# Internet. Cyberodporność

Wstęp

# Wstęp

Cyberodporność to zdolność sprostania wyzwaniom dla bezpieczeństwa związanym z transformacją cyfrową. Jako pojęcie prawnicze odnosi się zarówno do produktów z elementami cyfrowymi jak i do procesów społecznych i gospodarczych oraz systemów informacyjnych i polityczno-organizacyjnych. Obejmuje wykrywanie i redukowanie zagrożeń, reagowanie na zdarzenia niepożądane oraz realizację celów mimo różnych zakłóceń: celowych i przypadkowych, naturalnych i spowodowanych przez ludzi.

To syntetyczne ujęcie jest wynikiem badań, podjętych w związku z uchwaleniem Aktu o cyberodporności (CRA). W tytule tego unijnego rozporządzenia odporność, pojmowana ogólnie jako niepodatność na niekorzystne czynniki zewnętrzne, została opatrzona przedrostkiem cyber-, wywodzonym od greckiego słowa cybernetyka. Oznaczało ono pierwotnie sterowanie – starogreckie słowo κυβερνήτης (kybernḗtēs) – a współcześnie obejmuje ono interdyscyplinarną naukę o systemach sterowania i komunikacji, natomiast prefix cyber – występuje już w kilkuset wyrażeniach związanych z tym obszarem.

W niniejszym tomie najpierw poddano analizie aktualne zagrożenia i sposoby ich przezwyciężania (część 1) oraz ogólne ramy regulacyjne cyberodporności (część 2). Następnie skupiono się na problemach sektorowych – dla których dogodnym obszarem referencyjnym jest cyberodporność systemów ochrony zdrowia (część 3) oraz na technicznych aspektach transformacji cyfrowej, wśród których szczególne wyzwanie stanowi cyberodporność systemów sztucznej inteligencji (część 4). Uwzględniono także społeczne i gospodarcze uwarunkowania cyberodporności systemów przetwarzających dane osobowe (część 5).

Aktualne zagrożenia i sposoby ich przezwyciężania określa projekt nowej „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2025–2029". Diagnoza zagrożeń wskazuje na dynamiczny wzrost liczby incydentów – w tym operacji prowadzonych lub sterowanych przez nieprzyjazne państwa – rosnącą

wrażliwość łańcuchów dostaw, administracji publicznej i infrastruktury krytycznej, a także na intensyfikację kampanii przestępczych i haktywistycznych przeciw Polsce w kontekście wojny Rosji przeciwko Ukrainie. Plan działania, jak wskazano, obejmuje wiele konkretnych, mierzalnych zadań. Za kluczowe dla realizacji Strategii zagadnienia uznaje się: międzysektorową koordynację, wzmocnienie wymogów w zamówieniach publicznych, rozwój krajowych technologii i osiągnięcie suwerenności technologicznej oraz stałą współpracę międzynarodową w formatach Unii Europejskiej i NATO (*Krzysztof Gawkowski*).

Mechanizmy wojny informacyjno-psychologicznej prowadzonej przez Rosję obejmują wykorzystanie dezinformacji jako narzędzia operacji kognitywnej, toteż potrzebne jest zintegrowane wzmacnianie komponentów technicznych i społecznych odporności państwa i demokracji (*Dominika Kasprowicz*). Przedmiotem refleksji i uzgodnień powinno być kreowanie publicznej kultury odporności. Nowa regulacja ustawowa ochrony ludności i obrony cywilnej z 5.12.2024 r. przypisuje zasadnie wiele nowych zadań wspólnotom samorządowym i ich organom, statuując jednocześnie bardzo krótkie *vacatio legis* i powodując, że pozycja prawna samorządu terytorialnego w tym zakresie nie jest jeszcze w pełni racjonalnie ukształtowana. Postulowane jest budowanie w samorządzie terytorialnym wewnętrznego i zewnętrznego partnerstwa jako zabezpieczenia gotowości na sytuacje kryzysowe (*Irena Lipowicz*).

Do konkretnych uwag *de lege lata* i postulatów *de lege ferenda* prowadzi także rozpoznanie znaczenia czasu w określaniu zasad i trybu pozyskiwania danych i zabezpieczania materiału dowodowego jako bariery skutecznej reakcji karnoprawnej na cyberprzestępstwa. Postulaty dotyczą zarówno priorytetów w stosowaniu prawa, jak i zmian norm określających organizację i uprawnienia organów ścigania, zasady prowadzenia czynności wykrywczych oraz zakres danych możliwych do pozyskania (*Agnieszka Gryszczyńska*). Nagłe wprowadzanie wielu nowych obowiązków prawnych, może jednak osłabiać odporność organizacji na cyberzagrożenia. Próby szybkiego wdrożenia dużych zbiorów wymagań, np. wynikających z dyrektyw NIS 2 i CER, mogą prowadzić do nieefektywności, paraliżu organizacji oraz złudnego poczucia bezpieczeństwa. Właściwe jest więc podejście etapowe, które pozwala organizacjom znaleźć równowagę – uniknąć chaosu wdrożeniowego i skupić się na budowie solidnych podstaw dla dalszych działań w zakresie zarządzania cyberbezpieczeństwem (*Jakub Syta*).

Kluczowym warunkiem ciągłości działania współczesnych organizacji jest cyberodporność łańcuchów dostaw ICT, będących często celem cyberprzestępców. Wsparciem dla organizacji w racjonalnym zarządzaniu ryzykiem zewnętrznych dostawców ICT mogą być normy i standardy branżowe, pozwalające definiować wymogi bezpieczeństwa, ustanawiać nadzór oraz finalnie zapewnić ciągłość działania. Przy zarządzaniu takim ryzykiem konieczne staje się też uwzględnianie czynników geopolitycznych, gdyż dostawcy nowocze-

snych technologii i rozwiązań spoza UE mogą podlegać innym regulacjom lub ścisłej kontroli państwa. Zatem skuteczne zarządzanie ryzykiem w łańcuchu dostaw ICT wymaga integracji technologii, procesów, współpracy międzyorganizacyjnej i uwzględniania czynników geopolitycznych (*Krzysztof Zieliński*).

Współczesne zagrożenia wymagają precyzyjnych ram regulacyjnych, skutecznego zapobiegania, a także gotowości do szybkiej i sprawnej reakcji na incydenty. Pojęcie odporności Unii obejmowało początkowo wymiary: zdrowotny, cyfrowy, klimatyczny, społeczny i gospodarczy. Dzisiejsze zastosowanie kategorii odporności jako nowego spojrzenia na Unię zdolną do adaptacji, elastyczności i regeneracji, będących istotą odporności, wydaje się łączyć te wymiary, a jednocześnie owocnie wykraczać poza nie. Cyberodporność staje się elementem ważnym zarówno w ujęciu technologicznym, jak i prawnym (*Wojciech R. Wiewiórowski*). Termin ten zawarty w tytule unijnego Aktu o cyberodporności (CRA) nie ma – w przeciwieństwie do samej odporności – prawnej definicji, a występuje w wielu kontekstach i w odniesieniu do nich jest ujmowany jego zakres oraz relacje do odporności i bezpieczeństwa. Zatem pozostaje terminem nieostrym.

Ramy regulacyjne cyberodporności mają charakter wielopoziomowy, przy czym w ich strukturze rośnie udział aktów prawa unijnego. Mimo rozproszenia w wielu rozporządzeniach i dyrektywach, europejskie podejście nabiera coraz bardziej strategicznego i zintegrowanego charakteru. Rozporządzenie CRA z października 2024 r., jest określane jako element domykający regulację (*Krzysztof Silicki*) i wyraźny krok w kierunku ustanowienia jednolitych standardów bezpieczeństwa w UE, którego uzupełnieniem powinna być pełna integracja ochrony danych osobowych z procesami cyberbezpieczeństwa. Także zmieniony w 2025 r. plan działania UE (tzw. Blueprint) istotnie wzmacnia ramy operacyjne współpracy w czasie cyberkryzysu (*Wojciech R. Wiewiórowski*).

Rozporządzenie CRA nakłada na producentów i dostawców produktów z elementami cyfrowymi szereg obowiązków w zakresie bezpiecznego projektowania, wdrażania, wprowadzania aktualizacji, zgłaszania podatności i incydentów do właściwych zespołów reagujących CSIRT. Celem jest zobowiązanie twórców rozwiązań ICT do wprowadzania na rynek tylko takich produktów, które będą gwarantowały klientom, że liczba podatności będzie minimalna, a jeśli się one zdarzą, to będą obsłużone w sposób odpowiedzialny (*Krzysztof Silicki*). W budowaniu cyberodporności państwa i społeczeństwa istotne znaczenie mają zdolności CERT Polska w zakresie identyfikacji i katalogowania publicznie ujawnionych podatności. Implementacja dyrektywy NIS 2 oraz planowane wyznaczenie CSIRT NASK jako krajowego koordynatora procesu ujawniania podatności dodatkowo wzmacnia rolę tej organizacji. Jednak należy wskazać, że istotne jest zapewnienie współpracy ze strony producentów oprogramowania i budowanie kultury odpowiedzialnego ujawniania podatności (*Michał Dondajewski*).

Dla producentów, importerów i dystrybutorów odpowiedzią na narastanie zagrożeń związanych z rozwojem Internetu Rzeczy (IoT) są działania regulacyjne obejmujące zasadę „Security by Design" jako nowy paradygmat projektowania bezpiecznych rozwiązań dla produktów cyfrowych już na etapie planowania i rozwoju technologii. Przepisy CRA nie tylko należycie systematyzują wymagania, lecz także stanowią impuls do rozwoju nowych kompetencji i procedur w organizacjach – szczególnie w sektorze MŚP, dla którego wdrożenie przepisów może stanowić wyzwanie. Zatem kluczowe znaczenie ma równoległe wsparcie edukacyjne i doradcze (*Tomasz Chomicki*, *Joanna Grubicka*).

Istotne znaczenie w systemie ma SOC (Security Operation Center). Zwiększanie cyberoodporności w organizacji (jako jej zdolności do oceny zagrożeń i cyberincydentów, przygotowania się na nie, reagowania i odzyskiwania sprawności po nich) następuje przez identyfikację kluczowych systemów oraz analizę ryzyk, jak również przegląd zasobów IT (*Sebastian Szczerba*). Dla wzmacniania bezpieczeństwa, w tym cyberbezpieczeństwa, podmiotów najważniejszych dla funkcjonowania państwa i ochrony jego podstawowych interesów, nakładane są obowiązki, które należy transponować w sposób zapewniający spójność i zgodność z prawem unijnym. Analizowanie projektów w ramach prac Stałego Komitetu Rady Ministrów, pozwala m.in. na redukowanie możliwości odmiennej wykładni i stosowania prawa przez podmioty krytyczne i organy nadzorcze w zakresie spełnienia wymagań, ustanawianych w ustawie o zarządzaniu kryzysowym oraz ustawie o krajowym systemie cyberbezpieczeństwa (*Marcin Wysocki*). Elementem wzmacniania cyberodporności jest też nowa ustawowa regulacja zwalczania nadużyć w komunikacji elektronicznej, która wprowadza cztery nowe rodzaje czynów zabronionych (generowanie sztucznego ruchu, smishing, spoofing oraz niezgodne z prawem modyfikacje informacji adresowej), a także nakłada nowe, istotne obowiązki na przedsiębiorców telekomunikacyjnych oraz przyznaje nowe kompetencje CSIRT NASK i Prezesowi UKE (*Katarzyna Kupka*).

W budowaniu cyberodporności, zgodnie z wymogami dyrektywy NIS 2, wzmacniane jest obecnie podejście sektorowe. Już wcześniej – w związku z pandemią Covid19 – przyjęto takie podejście w sektorze zdrowia. Zatem analizy i oceny rozwiązań dotyczących systemów ochrony zdrowia mogą być bardzo przydatne także dla innych sektorów. Doświadczenia pokazują przykładowo, że świadczenie usług medycznych, z wykorzystaniem systemów teleinformatycznych wiąże się z koniecznością wyznaczania standardów w zakresie ochrony tych systemów oraz wsparcia we wdrażaniu najlepszych praktyk w zakresie bezpieczeństwa IT. Stworzenie wyspecjalizowanych zespołów reagowania na incydenty, w tym dedykowanego ochronie zdrowia, a także zapewnienie bieżącej i ciągłej współpracy między podmiotami tworzącymi system ochrony cyberbezpieczeństwa jest skomplikowane, ale może znacząco poprawić jego

poziom i zapewnić ochronę użytkownikom usług, a także danym medycznym (*Małgorzata Olszewska*).

Istotnym wyzwaniem jest zapewnienie interoperacyjności dokumentacji medycznej, uwzględniającej unijne i krajowe prawo, a także praktyczne aspekty funkcjonowania systemów takich jak Elektroniczna Dokumentacja Medyczna (EDM), Platforma P1 i Internetowe Konto Pacjenta, oraz rolę standardów wymiany danych (HL7, FHIR, DICOM, SNOMED CT, IHE, LOINC). Obok problemów organizacyjnych i technicznych uwagi wymaga ustawowe dopuszczenie digitalizacji dokumentacji medycznej, którego fakultatywność, ogranicza interoperacyjność systemu na kolejne dekady. Dylematy wyważania między potrzebami bezpieczeństwa i rozwoju pokazuje porównanie poziomu zaawansowania w Polsce, Estonii i w Niemczech (*Sebastian Sikorski*, *Michał Dziobkowski*).

Systemy teleinformatyczne wykorzystywane w ochronie zdrowia powinny charakteryzować się niezakłóconym przez środowiskowe zagrożenia działaniem, które realizuje cele związane zarówno z realizacją procesów o charakterze medycznym, jak i niemedycznym, w tym zarządzania podmiotami wykonującymi działalność leczniczą. Ma to kluczowe znaczenie dla zapewnienia pacjentom respektowania ich praw, niezakłóconego dostępu do świadczeń zdrowotnych odpowiedniej jakości i zgodnych z aktualną wiedzą medyczną. Budowanie odporności w cyberprzestrzeni wymaga holistycznego podejścia, uwzględniającego dorobek w rozpatrywanym obszarze nauk prawnych, technicznych, o zarządzaniu i o zdrowiu (*Krzysztof Świtała*, *Bartłomiej Michalak*). Dla podmiotów leczniczych problematyczne są nakłady finansowe i czas niezbędny dla podnoszenia świadomości zagrożeń i osiągania gotowości właściwej reakcji pracowników a dla zarządzających tymi podmiotami także kontrola wdrażania, konieczna aby uniknąć naruszeń i związanych z nimi sankcji, wzmacnianych w implementacji dyrektywy NIS 2 (*Marzenna Miłek*).

Wielkie zmiany w ochronie zdrowia wiążą się z rozwojem sztucznej inteligencji. Jej stosowanie daje spektakularne korzyści w badaniach naukowych (np. epidemiologii), diagnostyce (m.in. obrazowej), terapii (zwłaszcza chorób przewlekłych) i organizacji świadczeń (np. w triażu). Jednak towarzyszą im też nowe zagrożenia – nie tylko wobec pacjentów, ale także wobec przedstawicieli zawodów medycznych, którym przeciwdziałać ma regulacja prawna. AI Act będący podstawą kwalifikowania systemów e-zdrowia jako systemów sztucznej inteligencji wysokiego ryzyka, obliguje do oceny skutków dla praw podstawowych. W kontekście AI powinny być też weryfikowane tradycyjne instrumenty prawa medycznego, w tym wymogi świadomej zgody pacjenta (*Kamil Strzępek*).

W transformacji cyfrowej istotna jest obecnie synergia masowego rejestrowania śladów cyfrowych, rozwoju skalowalnych usług chmurowych oraz postępu w dziedzinie zaawansowanej analizy danych niestrukturalnych, w tym

metod głębokiego uczenia. Duże modele językowe (LLM), które potrafią generować spójne i semantycznie złożone treści, stają się ważnymi narzędziami w automatyzacji procesów intelektualnych i kreatywnych. Wdrażanie systemów AI w obszarach wysokiego ryzyka, zwiększa znaczenie ich odporności na intencjonalne zakłócenia. W zarządzaniu ryzykiem operacyjnym obok poufności, integralności i dostępności uwzględnienia wymaga specyfika zagrożeń AI, obejmujących próby wydobycia poufnych danych treningowych lub architektury modelu, manipulacje danymi uczącymi lub wejściowymi w celu uzyskania błędnych decyzji oraz działania prowadzące do zablokowania systemu lub znaczącego obniżenia jego dostępności. Przyjęcie scenariuszowej metodologii oceny ryzyka i zastosowanie do regulacji systemów LLM „testu proporcjonalności" mogą być podstawą rewizji klasyfikacji dla systemów pierwotnie uznanych za „wysokiego ryzyka" oraz narzędziem dynamicznego dopasowywania poziomów ochrony dla krajowych i międzynarodowych organów nadzorczych (*Jerzy Surma*).

Duże modele językowe (LLM) – ze względu na ich potencjał innowacyjny związany ze zdolnością do adaptacji i rozumienia złożonych kontekstów komunikacyjnych – stanowią coraz ważniejszą część krytycznej warstwy infrastruktury informacyjnej wielu organizacji. Równolegle narasta liczba incydentów związanych z tzw. jailbreak AI. To zjawisko – polegające na obchodzeniu mechanizmów ochronnych modeli w celu uzyskania nieautoryzowanych lub szkodliwych rezultatów – umożliwia atakującym trwałe osłabienie mechanizmów kontroli, eskalację ataków socjotechnicznych, wyciek danych oraz automatyzację generowania dezinformacji czy mowy nienawiści. Za niezbędne dla zmniejszenia skuteczności tych ataków i budowania cyberodporności uznaje się wdrażanie wielowarstwowych, adaptacyjnych mechanizmów bezpieczeństwa, stosowanie złożonych strategii obrony, łączących filtrowanie treści, analizę intencji, detekcję anomalii, monitorowanie kontekstu oraz automatyczne mechanizmy „wyrzucania z pamięci" szkodliwych wzorców, a także wdrożenie rygorystycznych procedur walidacji i monitorowania danych treningowych, co wymaga współpracy interdyscyplinarnej (*Agata Ślusarek*).

Wyzwaniem technicznym i prawnym stało się obecnie np. zapewnienie skutecznej wideoweryfikacji, w związku z wykorzystywaniem AI do generowania fałszywych treści audiowizualnych (deepfakes). Wymaga to środków skutecznych a nie naruszających praw weryfikowanego. AI Act nakłada obowiązek ujawnienia, że treści deepfake, zostały sztucznie wygenerowane lub zmanipulowane. Do wykrywania deepfakes może zostać użyty także system AI, przy czym należy zapewnić odpowiedni poziom jego odporności. Te trzy wymiary relacji między AI a cyberbezpieczeństwem: cyberbezpieczeństwo rozwiązań bazujących na AI, AI w służbie cyberbezpieczeństwa oraz przestępcze wykorzystanie AI pojawiają się w wielu obszarach (*Agnieszka Besiekierska*). Jednym z nich jest obrót i zarządzanie nieruchomościami. Wykorzysta-

nie sztucznej inteligencji pozytywnie wpływa na rozwój rynku nieruchomości oraz usprawnianie zarządzania i obrotu nieruchomościami, ale także czyni ten rynek coraz bardziej podatnym na cyberzagrożenia. Są one związane z jednej strony z niekontrolowanym przetwarzaniem danych, a z drugiej – z cyfryzacją infrastruktury wykorzystywanej do zarządzania nieruchomościami (*Mateusz Badowski*).

Rozwój zastosowań systemów AI i uwzględnianie w nim ochrony praw podstawowych zależeć będzie m.in. od krajowej regulacji zagadnień instytucjonalnych, które w projekcie ustawy nie były jeszcze optymalne i na podstawie analizy prawnoporównawczej uzasadniały m.in. wzmocnienie pozycji Prezesa UODO zgodnie z brzmieniem AI Act; ustanowienie klarownych mechanizmów współdziałania między organami; oraz rozważenie wprowadzenia dalej idących instrumentów nakierowanych na przeciwdziałanie konfliktom interesów (*Paweł Hajduk*). Pozytywnie w tym kontekście oceniane jest natomiast CRA, które stanowi, że nie narusza przepisów rozporządzenia 2016/679 (RODO) i zakłada współstosowanie obu rozporządzeń oraz współpracę organów. Organy ochrony danych uzyskują m.in. prawo dostępu do dokumentacji istotnej dla realizacji ich zadań, co sprzyja tworzeniu synergii między systemami ochrony danych osobowych i cyberodporności, zarówno w obszarze normalizacji, jak i certyfikacji poszczególnych aspektów cyberbezpieczeństwa w ramach współpracy między Komisją Europejską, europejskimi organizacjami normalizacyjnymi, Agencją Unii Europejskiej ds. Cyberbezpieczeństwa, Europejską Radą Ochrony Danych oraz krajowymi organami nadzorczymi odpowiedzialnymi za ochronę danych. W ten sposób można mówić o stopniowym powstawaniu nowych elementów europejskiego ekosystemu organów, w których katalogu zadań leży zapewnianie w różnorodny sposób i w różnych kontekstach cyberbezpieczeństwa, cyberodporności i ochrony przetwarzanych danych (*Mirosław Wróblewski*).

Chociaż nowe przepisy wzmacniają obowiązki organizacji w zakresie analizy ryzyka i planu reagowania na incydenty – kluczowych dla jej cyberodporności, to w ich stosowaniu pojawiają się nieprawidłowości. Barierami w realizacji polityk bezpieczeństwa są braki kompetencyjne, organizacyjne i finansowe w organizacjach. Brakuje też przypisania odpowiedzialności za analizę ryzyka konkretnym osobom (*Małgorzata Ganczar*). W dostosowywaniu rozwiązań do stanu faktycznego, wzmacnianiu podziału zadań, wyciąganiu konsekwencji wobec dopuszczających się naruszeń, istotne znaczenie mają procedury, przyjmowane w wykonaniu przepisów prawa, ale też kształtujące się jako dobre praktyki w poszczególnych obszarach, np. zarządzania dostępem czy szkoleń (*Marlena Sakowska-Baryła*).

Narzędzia zapewniające dostęp do e-usług, jak szeroko używana aplikacja mObywatel, zawierają coraz bardziej zaawansowane mechanizmy zabezpieczające. Jednak redukowanie poziomu ryzyka skutecznego ataku i naruszenia

danych osobowych wymaga też podnoszenia poziomu świadomości użytkowników (*Kamil Czaplicki*). Działania te powinny być zróżnicowane. Budowanie świadomości algorytmicznej oraz krytycznej refleksyjności wobec zjawisk cyfrowych może być remedium na uprzedmiotowienie, polegające na doświadczaniu przemocy w sieci oraz ekspozycje na treści destrukcyjne i zagrażające dobrostanowi, zwłaszcza osób młodych, związane z istnieniem systemów rekomendacyjnych opartych na algorytmach (*Konrad Ciesiołkiewicz*). W odniesieniu do osób starszych – jak pokazuje analiza ścigania tzw. przestępstw na wnuczka – istotne staje się zwiększanie odporności na manipulację (*Adam Białas*). Efektywność podnoszenia świadomości i korygowania postaw zależy też od form edukacji, wśród których proponowane są gry video podnoszące poziom cyberhigieny i zwiększające odporność społeczną (*Konrad Radomiński*).

Sygnalizowane wyżej ustalenia pokazują wielość aspektów cyberodporności i jej jurydyzacji. Możliwość multidyscyplinarnej analizy zawdzięczamy włączeniu się kolejny już raz pracowników naukowych kilkunastu szkół wyższych oraz wybitnych ekspertów-praktyków, do badań koordynowanych przez Naukowe Centrum Prawno-Informatyczne i Centrum Liderów Transformacji Cyfrowej UKSW. Były one wielostronnie wspierane przez władze publiczne, podmioty biznesowe i organizacje pozarządowe.

Przypomnijmy, że problemami badawczymi podejmowanymi w poprzednich tomach serii Internet były: Ochrona wolności, własności i bezpieczeństwa; Prawno-informatyczne problemy sieci, portali i e-usług; Cloud computing. Przetwarzanie w chmurach; Publiczne bazy danych i Big data; Internet rzeczy. Bezpieczeństwo w Smart city; Strategie bezpieczeństwa; Informacja przestrzenna; Przetwarzanie danych osobowych; Analityka danych; Cyberpandemia; Globalne gry; Hacking oraz Solidarność cyfrowa[1].

W kolejnym tomie tej serii, konsekwentnie od 15 lat skupionej na problemach bezpieczeństwa w Internecie, referowane będą wyniki naszych badań nad cyberodpowiedzialnością.

*Prof. dr hab. Grażyna Szpor*

[1] Monografie recenzowane w wyd. C.H. Beck, tomy serii Internet: Ochrona wolności, własności i bezpieczeństwa, red. *G. Szpor*, Warszawa 2011; Prawno-informatyczne problemy sieci, portali i e-usług, red. *G. Szpor*, *W.R. Wiewiórowski*, Warszawa 2012; Cloud computing. Przetwarzanie w chmurach, red. *G. Szpor*, Warszawa 2013; Publiczne bazy danych i Big data, red. *G. Szpor*, Warszawa 2014; Internet rzeczy. Bezpieczeństwo w Smart city, red. *G. Szpor*, Warszawa 2016; Strategie bezpieczeństwa, red. *G. Szpor*, *A. Gryszczyńska*, Warszawa 2017; Informacja przestrzenna, red. *G. Szpor*, *K. Czaplicki*, Warszawa 2018; Przetwarzanie danych osobowych, red. *G. Szpor*, *K. Czaplicki*, Warszawa 2019; Analityka danych, red. *G. Szpor*, *K. Czaplicki*, Warszawa 2019; Cyberpandemia, red. *A. Gryszczyńska*, *G. Szpor*, Warszawa 2020; Globalne gry, red. *A. Gryszczyńska*, *G. Szpor*, *W.R. Wiewiórowski*, Warszawa 2022; Hacking, red. *A. Gryszczyńska*, *G. Szpor*, *W.R. Wiewiórowski*, Warszawa 2023; Solidarność cyfrowa, red. *A. Gryszczyńska*, *G. Szpor*, *W.R. Wiewiórowski*, Warszawa 2024.