ISSN 3072-4120

Bezpieczeństwo

w dobie nowych technologii

Redakcja naukowa

IWONA SZKUDLAREK

ACTA
SECURITAS
TOM 2

STRESZCZENIA / ABSTRACT

słowa kluczowe / keywords

ACTA
SECURITAS
TOM 2

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21456211

Różnorodne podejścia wobec uwarunkowań retrospektywnych bezpieczeństwa. Dylematy naukowe

Diverse Approaches to Retrospective Security Conditions. Scientific Dilemmas

Dariusz Cieślak

Urząd Gminy Sędziejowice
https://orcid.org/0009-0002-1263-2657

Streszczenie: W artykule naukowym podjęto próbę refleksji nad teoretycznym osadzeniem kategorii bezpieczeństwa, analizując jej wielowymiarowy i dynamiczny charakter. Autor artykułu przeanalizował zróżnicowane perspektywy ujmowania bezpieczeństwa w naukach społecznych, poczynając od klasycznych podejść, determinowanych logiką polityczną, a kończąc na współczesnych, uwzględniających aspekty społeczne, ekonomiczne, kulturowe, typowe dla środowisk lokalnych. Szczególną uwagę zwrócono na dylematy definicyjne oraz trudności metodologiczne wynikające z wieloznaczności pojęcia bezpieczeństwa, które w literaturze naukowej funkcjonuje jako kategoria interdyscyplinarna, obejmująca zarówno wymiary jednostkowe, jak i zbiorowe. Autor podjął także próbę ukazania hybrydyczności współczesnych zagrożeń, które wymykają się tradycyjnym schematom analizy bezpieczeństwa, a ich zrozumienie wymaga zastosowania wielu nowych narzędzi badawczych. W artykule uwypuklono, iż teoretyczne dylematy nie stanowią przeszkody badawczej, lecz są punktem wyjścia do pogłębiania refleksji nad bezpieczeństwem jako kategorią centralną dla współczesnych nauk społecznych, najważniejszego elementu infrastruktury bezpieczeństwa społecznego i odporności lokalnych wspólnot.

Słowa kluczowe: bezpieczeństwo, teorie bezpieczeństwa, dylematy definicyjne, interdyscyplinarność, hybrydyczność współczesnych zagrożeń, definicja bezpieczeństwa

Abstract: This academic article attempts to reflect on the theoretical basis of the category of security, analyzing its multidimensional and dynamic nature. The author analyzes the diverse perspectives on security in the social sciences, starting with classical approaches determined by political logic and ending with contemporary ones that consider social, economic, and cultural aspects typical of local communities. Particular attention was paid to definitional dilemmas and methodological difficulties resulting from the ambiguity of the concept of security, which in scientific literature functions as an interdisciplinary category, encompassing both individual and collective dimensions. The author also attempted to show the hybrid nature of contemporary threats, which elude traditional security analysis schemes and require

the use of many new research tools to understand them. The article emphasizes that theoretical dilemmas are not a research obstacle, but rather a starting point for deepening reflection on security as a central category for contemporary social sciences, the most important element of social security infrastructure and the resilience of local communities.

Keywords: security, security theories, definitional dilemmas, interdisciplinarity, hybrid nature of contemporary threats, definition of security

ACTA
SECURITAS
TOM 2

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21563374

Ekosystem – perspektywy rozwoju lotnictwa cywilnego w Polsce w obliczu zmian strukturalnych, klimatycznych i rynkowych

The Ecosystem – Prospects for the Development of Civil Aviation in Poland in the Face of Structural, Climatic and Market Changes

Dariusz Bogusz

Lotnicza Akademia Wojskowa
https://orcid.org/0000-0001-7755-0949

Grzegorz Brychczyński

Stowarzyszenie Inżynierów i Techników Komunikacji RP
https://orcid.org/ 0009-0000-8688-1379

Streszczenie: W niniejszym artykule przeanalizowano przemiany polskiego ekosystemu lotnictwa cywilnego na tle aktualnych wyzwań strukturalnych, klimatycznych i technologicznych. Celem artykułu jest analiza pozycji polskiego rynku lotniczego na arenie międzynarodowej z różnych perspektyw oraz wskazanie kluczowych megatrendów, które będą kształtować jego przyszłość. Problem badawczy wyrażono pytaniem: jakie są perspektywy rozwoju lotnictwa cywilnego w Polsce w obliczu zmian strukturalnych, klimatycznych i rynkowych? W głównej części tekstu zawarto szczegółową analizę koncepcji Centralnego Portu Komunikacyjnego jako węzła intermodalnego w kontekście strategii adaptacyjnych regionalnych portów lotniczych. Kluczowe elementy niniejszej pracy obejmują ocenę wpływu cyfryzacji, automatyzacji i sztucznej inteligencji na efektywność operacji ruchu lotniczego, a także analizę procesów dekarbonizacji i elektryfikacji w obszarach General Aviation i miejskiej mobilności powietrznej (Urban Air Mobility, UAM). Na koniec wykazano, że kompleksowe podejście do innowacji technologicznych oraz elastyczne dostosowanie infrastruktury do wymogów środowiskowych UE są niezbędne, aby polski sektor lotniczy pozostał konkurencyjny.

Słowa kluczowe: lotnictwo cywilne, Centralny Port Komunikacyjny (CPK), lotniska regionalne, sztuczna inteligencja, General Aviation, U-space

Abstract: This article examines the transformation of the Polish civil aviation ecosystem against the backdrop of current structural, climatic, and technological challenges. The aim of the article is to

analyze the position of the Polish aviation market in the international arena from various perspectives and identify key megatrends that will shape its future. The main body of the text provides a detailed analysis of the concept of the Central Communication Port (CCP) as an intermodal hub in the context of regional airports' adaptation strategies. Key elements of this work include an assessment of the impact of digitalization, automation, and artificial intelligence on the efficiency of air traffic operations, as well as an analysis of decarbonization and electrification processes in the areas of General Aviation and urban air mobility (UAM). Finally, it demonstrates that a comprehensive approach to technological innovation and flexible adaptation of infrastructure to EU environmental requirements are essential for the Polish aviation sector to remain competitive.

Keywords: civil aviation, Central Communication Port (CCP), regional airports, artificial intelligence, General Aviation, U-space

ACTA
SECURITAS
TOM 2

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.20279638

Technologia jako projekt cywilizacyjny: chińska wizja przyszłości władzy, bezpieczeństwa i postępu

Technology as a Civilizational Project: China's Vision of Power, Security, and Progress

Gaja Staroń, LL.M.

Niezależna badaczka
https://orcid.org/0009-0005-4908-1280

Streszczenie: Artykuł analizuje raport Prognozy technologiczne i wizje przyszłości 2049 (《科技预见与未来愿景2049》报告中文版) jako dyskursywny projekt cywilizacyjny, w którym technologia zostaje ujęta jako infrastrukturalna forma organizacji życia zbiorowego. Autorska kategoria „społeczeństwa inteligentnej infrastruktury" pozwala odczytać fuzję sztucznej inteligencji, technologii kwantowych, nauk o życiu, nowych materiałów i nowej energii oraz zasadę obliczalności jako podstawy systemu koordynującego procesy biologiczne, energetyczne i społeczne. Raport zostaje zinterpretowany jako propozycja alternatywnej ontologii nowoczesności, w której postęp oznacza wzrost zdolności koordynacyjnych systemu, a nie jedynie ekspansję autonomii jednostki.

Słowa kluczowe: suwerenność technologiczna, Chiny 2049, ontologia postępu, bezpieczeństwo systemowe, projekt cywilizacyjny

Abstract: This article analyzes the report Tech Predictions and Future Visions 2049 (科技预见与未来愿景2049) as a discursive civilizational project in which technology becomes an infrastructural form of organizing collective life.The interpretive category of an "intelligent infrastructure society" frames the fusion of artificial intelligence, quantum technologies, life sciences, new materials, and new energy, together with computability, as the foundations of a system coordinating biological, energetic, and social processes. The report is interpreted as proposing an alternative ontology of modernity in which progress signifies an increase in systemic coordination rather than merely the expansion of individual autonomy.

Keywords: technological sovereignty, China 2049, ontology of progress, systemic security, civilizational project

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.20286380

ACTA
SECURITAS
TOM 2

Współpraca cywilno-wojskowa jako komponent systemu bezpieczeństwa państwa

Civil-Military Cooperation as a Component of the State Security System

Łukasz Jasiński

Uniwersytet Kaliski im. Prezydenta Stanisława Wojciechowskiego
https://orcid.org/0009-0003-4588-804X

Streszczenie: Współpraca cywilno-wojskowa stanowi istotny element systemu bezpieczeństwa państwa, umożliwiający skoordynowaną reakcję na zagrożenia militarne i pozamilitarne. Jej znaczenie rośnie wraz ze wzrostem złożoności środowiska bezpieczeństwa, w którym sfera cywilna i wojskowa są coraz bardziej powiązane, zwłaszcza w kontekście zagrożeń hybrydowych i sytuacji kryzysowych. Celem niniejszego artykułu jest analiza współpracy cywilno-wojskowej jako stałego elementu bezpieczeństwa narodowego, z uwzględnieniem jej genezy, uwarunkowań doktrynalnych oraz instytucjonalnych form funkcjonowania w Polsce.
Artykuł opiera się na analizie literatury przedmiotu, dokumentach doktrynalnych i aktach normatywnych oraz wykorzystuje podejście systemowe. Artykuł przedstawia ewolucję współpracy cywilno-wojskowej, omawia podstawowe formy współdziałania i wskazuje na znaczenie podejścia zintegrowanego. Szczególną uwagę poświęcono wielopoziomowemu i terytorialnemu charakterowi współpracy cywilno-wojskowej w Polsce oraz warunkom jej skuteczności. W pracy sformułowano autorską typologię barier strukturalno-proceduralnych, terytorialnych oraz kulturowych, a także zestawienie czynników sprzyjających trwałemu zakorzenieniu kooperacji w systemie obronnym. Przeprowadzona analiza wskazuje, że skuteczność tej współpracy zależy od interoperacyjności procedur, jakości relacji międzyinstytucjonalnych oraz jej trwałego zakorzenienia w codziennym zarządzaniu bezpieczeństwem.

Słowa kluczowe: współpraca cywilno-wojskowa, system bezpieczeństwa państwa, CIMIC, zarządzanie kryzysowe, odporność państwa, zagrożenia hybrydowe

Abstract: Civil-military cooperation constitutes an essential element of the state security system, enabling a coordinated response to military and non-military threats. Its significance increases along with the growing complexity of the security environment, where the civil and military spheres are increasingly interconnected, particularly in the context of hybrid threats and crisis situations. The purpose of this article is to analyze civil-military cooperation as a permanent element of national security, taking into account its genesis, doctrinal conditions, and institutional forms of functioning in Poland.

The article is based on the analysis of the subject literature, doctrinal documents, and normative acts, and utilizes a systemic approach. The paper presents the evolution of civil-military cooperation, discusses the basic forms of interaction, and highlights the importance of an integrated approach. Particular attention is paid to the multi-level and territorial nature of civil-military cooperation in Poland, as well as the conditions for its effectiveness. The study formulates an authorial typology of structural-procedural, territorial, and cultural barriers, alongside a compilation of factors conducive to the permanent embedding of cooperation within the defense system. The conducted analysis indicates that the effectiveness of this cooperation depends on the interoperability of procedures, the quality of inter-institutional relations, and its sustainable entrenchment in day-to-day security management.

Keywords: civil-military cooperation, state security system, CIMIC, crisis management, state resilience, hybrid threats

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21456588

ACTA
SECURITAS
TOM 2

Audyt RODO w polskich uczelniach wyższych. Część I: Modele audytu, narzędzia i procedury jako infrastruktura detekcji

GDPR Audit at Polish Universities. Part I: Audit Models, Tools and Procedures as a Detection Infrastructure

Maciej Walaszczyk

Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego
https://orcid.org/0009-0006-5260-9186

Streszczenie: Artykuł stanowi pierwszą z dwóch części opracowania poświęconego audytowi RODO w polskich uczelniach wyższych. Wychodząc od tezy, że brak zgłoszonych naruszeń nie oznacza ich braku, lecz może świadczyć o niedostatecznej zdolności detekcyjnej organizacji, artykuł systematyzuje elementy składowe tej zdolności w kontekście akademickim. Opisano złożoność uczelni jako administratora danych osobowych, przetwarzającego dane w kilku odrębnych strumieniach procesowych i w rozbudowanej strukturze organizacyjnej. Zestawiono modele audytu zgodności (PDCA, AICPA/CICA Privacy Maturity Model, podejście DPIA-centric, ramy ISO 27001/27701), dokonano funkcjonalnego przeglądu narzędzi informatycznych wspierających detekcję naruszeń oraz omówiono kluczowe procedury wewnętrzne, w tym procedurę obsługi naruszeń. Część druga opracowania wykorzysta przedstawiony tu aparat pojęciowy do interpretacji danych sprawozdawczych PUODO za lata 2018-2024.

Słowa kluczowe: RODO, audyt zgodności, Privacy Maturity Model, DPIA, narzędzia compliance

Abstract: This article is the first of a two-part study on GDPR audits in Polish higher education institutions. Starting from the premise that the absence of reported breaches does not imply the absence of actual breaches, but may instead reflect an organisation's insufficient detection capability, the article systematises the components of that capability in the academic context. It describes the complexity of universities as data controllers, processing personal data across several distinct process streams and within extensive organisational structures. It reviews audit models used for compliance (PDCA, the AICPA/CICA Privacy Maturity Model, the DPIA-centric approach, and the ISO 27001/27701 framework), conducts a functional review of IT tools supporting breach detection, and discusses key internal procedures, including breach-handling procedures. Part two of the study will apply the conceptual framework presented here to interpret PUODO's reporting data for 2018–2024.

Keywords: GDPR, compliance audit, Privacy Maturity Model, DPIA, compliance tools

ACTA
SECURITAS
TOM 2

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21456652

Audyt RODO w polskich uczelniach wyższych. Część II: Dynamika zgłoszeń, hipotezy interpretacyjne i kontekst NIS2

GDPR Audit at Polish Universities. Part II: Trends in Reports, Interpretative Hypotheses and the NIS2 Context

Maciej Walaszczyk

Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego
https://orcid.org/0009-0006-5260-9186

Streszczenie: Artykuł stanowi drugą z dwóch części opracowania poświęconego audytowi RODO w polskich uczelniach wyższych. Wykorzystując aparat pojęciowy przedstawiony w części pierwszej (modele audytu, narzędzia detekcji, procedury wewnętrzne), artykuł analizuje dynamikę zgłoszeń naruszeń ochrony danych do PUODO w latach 2018–2024, kiedy ich liczba wzrosła ponad dwuipółkrotnie. Stawia trzy komplementarne hipotezy interpretacyjne, spośród których za centralną uznaje tezę, że wzrost zgłoszeń wynika w istotnej mierze z dojrzewania kultury compliance i poprawy zdolności detekcyjnej organizacji, a nie z pogorszenia stanu bezpieczeństwa danych. Szczególną uwagę poświęcono paradoksowi sektora akademickiego, który mimo wysokiej złożoności przetwarzania notuje najniższy wskaźnik zgłoszeń spośród wszystkich sektorów objętych sprawozdaniami PUODO. Artykuł analizuje typy naruszeń charakterystyczne dla środowiska akademickiego oraz nowy kontekst regulacyjny wynikający z dyrektywy NIS2.

Słowa kluczowe: RODO, PUODO, naruszenia ochrony danych, NIS2, sektor akademicki

Abstract: This article is the second of a two-part study on GDPR audits in Polish higher education institutions. Building on the conceptual framework presented in Part One (audit models, detection tools, internal procedures), the article analyses the dynamics of personal data breach notifications submitted to PUODO between 2018 and 2024, a period in which their number grew more than two-and-a-half-fold. It puts forward three complementary interpretive hypotheses, the central one being that the growth in notifications is substantially driven by maturing compliance culture and improved organisational detection capability, rather than by deterioration in data security. Particular attention is given to the paradox of the academic sector, which, despite the high complexity of its data processing, records the lowest breach notification rate of all sectors tracked by PUODO. The article also examines breach types characteristic of the academic environment and the new regulatory context arising from the NIS2 Directive.

Keywords: GDPR, PUODO, personal data breaches, NIS2, higher education sector

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21470919

ACTA
SECURITAS
TOM 2

Wojna informacyjna jako kluczowy element działań hybrydowych we współczesnym środowisku bezpieczeństwa

Information Warfare as a Key Element of Hybrid Operations in the Contemporary Security Environment

Dominik Bryzek

Akademia WSB
https://orcid.org/0009-0000-9879-1071

Streszczenie: Artykuł przedstawia analizę wojny informacyjnej jako jednego z kluczowych elementów współczesnych działań hybrydowych. Celem opracowania jest ukazanie znaczenia oddziaływania informacyjnego we współczesnym środowisku bezpieczeństwa oraz wskazanie mechanizmów wykorzystywanych do osiągania celów politycznych i strategicznych. W pracy zastosowano analizę literatury przedmiotu oraz omówiono konflikt rosyjsko-ukraiński i rywalizację chińsko-tajwańską. Wyniki analizy wskazują, że wojna informacyjna stanowi istotne narzędzie destabilizacji państw, wpływa na procesy decyzyjne oraz wymaga rozwijania skutecznych mechanizmów przeciwdziałania i budowania odporności informacyjnej.

Słowa kluczowe: wojna informacyjna, wojna hybrydowa, dezinformacja, propaganda, bezpieczeństwo

Abstract: This article presents an analysis of informationwarfare as one of the keylements of contemporary hybrid operations. The aim of the studyis to demonstrate the significance of information influence in the contemporarysecurity environment and to indentify the mechanismused to achievepolitical and tratyegicobjectives. The studyisbased on a review of the relevantliterature and discusses the Russian-Ukrainian conflict and the Chinese-Taiwanese rivalry as an example of the application of informationwarfare in contemorary conflicts. The analysis indicates that information warfare constitutes a significant tool for destabilising states, influences decision-making processes and highlights the need to dvelop effectice mechanisms for countering disinfomation and strengthening information resilience.

Keywords: informationwarfare, hybridwarfare, disinformation, propaganda, security

ACTA
SECURITAS
TOM 2

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21455299

Deepfake w wojnie informacyjnej – narzędzie destabilizacji w konfliktach hybrydowych na przykładzie wojny w Ukrainie

Deepfakes in Information Warfare – a Tool for Destabilisation in Hybrid Conflicts, as Illustrated by the War in Ukraine

Ryszard Radwański

Państwowa Akademia Nauk Stosowanych w Krośnie
https://orcid.org/0000-0002-2100-6845

Streszczenie: Deepfake stał się jednym z najbardziej niebezpiecznych narzędzi współczesnej wojny informacyjnej, szczególnie w realiach konfliktów hybrydowych. W czasie wojny w Ukrainie technologia ta była wykorzystywana do podważania zaufania społecznego, dezinformowania opinii publicznej oraz destabilizacji procesów decyzyjnych. Przykładem jest fałszywe nagranie z udziałem Wołodymyra Zełenskiego, w którym rzekomo wzywał on do kapitulacji – materiał szybko zdementowany, lecz skutecznie pokazujący potencjał oddziaływania deepfake'ów. W połączeniu z operacjami psychologicznymi i kampaniami dezinformacyjnymi prowadzonymi m.in. przez Rosję, deepfake'i stają się narzędziem erozji prawdy, utrudniającym odbiorcom odróżnienie faktów od manipulacji. Artykuł analizuje rolę tej technologii jako elementu współczesnej wojny informacyjnej oraz wyzwania, jakie stawia ona przed bezpieczeństwem informacyjnym państw i społeczeństw.

Słowa kluczowe: deepfake, wojna informacyjna, dezinformacja, konflikty hybrydowe

Abstract: Deepfakes have become one of the most dangerous tools of contemporary information warfare, particularly in hybrid conflicts. During the war in Ukraine, this technology was used to undermine public trust, disinform public opinion, and destabilize decision-making processes. An example is the fake recording of Volodymyr Zelensky, in which he allegedly called for surrender – a material quickly debunked but effectively demonstrating the potential impact of deepfakes. Combined with psychological operations and disinformation campaigns conducted by Russia, among others, deepfakes are becoming a tool for the erosion of truth, making it difficult for recipients to distinguish fact from manipulation. This article examines the role of this technology as a component of contemporary information warfare and the challenges it poses to the information security of states and societies.

Keywords: deepfake, information warfare, disinformation, hybrid conflicts

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21626555

ACTA
SECURITAS
TOM 2

Od kanistra na plecach do MQ-25: droga ku autonomii tankowania w powietrzu

From a Back-mounted Fuel Can to the MQ-25: The Path to the Autonomous Air to Air Refueling

Piotr Pawlonka

niezależny badacz
https://orcid.org/0009-0003-5091-2227

Streszczenie: Tankowanie w powietrzu określane jest mianem strategicznego mnożnika siły, umożliwiającego zwiększenie zasięgu, długotrwałości lotu oraz efektywności działań lotnictwa wojskowego. Artykuł przedstawia ewolucję procesu tankowania w powietrzu oraz analizuje wpływ rozwoju bezzałogowych statków powietrznych na przyszłość działań prowadzonych przez siły zbrojne. Zaprezentowano historyczny rozwój koncepcji uzupełniania paliwa w locie – od pierwszych eksperymentów realizowanych na początku XX wieku po współcześnie stosowane systemy tankowania. Szczególną uwagę poświęcono programowi MQ-25 Stingray – pierwszemu pokładowemu bezzałogowemu tankowcowi powietrznemu, którego rozwój może istotnie zmienić sposób realizacji operacji wspierających przez siły powietrzne. Przeanalizowano także potencjał wykorzystania autonomicznych systemów w procesie tankowania w powietrzu w kontekście ograniczenia ryzyka dla personelu lotniczego, zwiększenia zasięgu oraz efektywności operacji lotniczych.

Słowa kluczowe: bezzałogowy statek powietrzy (BSP), tankowanie w powietrzu (AAR), MQ-25, lotnictwo

Abstract: Air to air refueling is regarded as a strategic force multiplier, enabling increased operational range, flight endurance and the operational effectiveness of military aviation. The article presents the evolution of air to air refueling and analyzes the impact of unmanned aerial vehicle development on the future of military operations. It outlines the historical development of the in-flight refueling concept, from the first experiments conducted in the early twentieth century to the modern refueling systems currently in service. Particular attention is devoted to the MQ-25 Stingray program, the first carrier-based unmanned aerial refueling aircraft whose development could significantly transform the way aerial support operations are conducted. The article also examines the potential application of autonomous systems in air to air refueling, highlighting their role in reducing risks to aircrew, extending operational range, and improving the effectiveness of air operations.

Keywords: unmanned aerial vehicle (UAV), unmanned aerial system (UAS), Air to Air Refuelling (AAR), MQ-25, aviation

ACTA
SECURITAS
TOM 2

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.20287288

Technologia 5G w aspekcie bezpieczeństwa sieci bezprzewodowych

5G Technology in Terms of Wireless Network Security

Oliwier Pytel

34 Brygada Kawalerii Pancernej w Żaganiu
https://orcid.org/0009-0003-6633-8450

Iwona Szkudlarek

Karkonoska Akademia Nauk Stosowanych w Jeleniej Górze
https://orcid.org/0000-0001-7125-7004

Streszczenie: Artykuł ma charakter przeglądowy i obejmuje tematykę technologii 5G, w tym charakterystykę i założenia tej technologii oraz cele i zalety wdrożenia sieci 5G. Artykuł opisuje także architekturę systemu i stosowanych w nim pasm oraz podstawowe wymagania dotyczące anten przeznaczonych do pracy w omawianej technologii. Artykuł przedstawia powyższe zagadnienia w aspekcie standardów i regulacji dotyczących 5G i pasma N76 w odniesieniu do bezpieczeństwa sieci bezprzewodowych.

Słowa kluczowe: technologia 5G, antena, bezpieczeństwo sieci bezprzewodowych, pasmo N76, architektura sieci 5G

Abstract: This article is a review covering the subject of 5G technology, including its characteristics and assumptions, as well as the objectives and advantages of implementing 5G networks. The article also describes the system, architecture and the bands used in it, as well as the basic requirements for antennas designed to work with this technology. The article presents the above issues in terms of standards and regulations concerning 5G and the N76 band in relation to wireless network security.

Keywords: 5G technology, antenna, wireless network security, 5G N76 frequency band, 5G network architecture

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21455544

ACTA
SECURITAS
TOM 2

Administrowanie informacją w fazie odbudowy zarządzania kryzysowego. Część I

Information Administration during the Recovery Phase of Crisis Management. Part I

Artur Woźny

Politechnika Rzeszowska im. Ignacego Łukasiewicza
https://orcid.org/0000-0002-0294-0157

Kacper Mazurek

Politechnika Rzeszowska im. Ignacego Łukasiewicza
https://orcid.org/0009-0002-0818-7407

Piotr Padula

Politechnika Rzeszowska im. Ignacego Łukasiewicza
https://orcid.org/0009-0004-8353-6675

Streszczenie: Artykuł podejmuje analizę roli informacji w fazie odbudowy zarządzania kryzysowego, traktując ją jako kluczowy czynnik determinujący zdolności adaptacyjne systemu bezpieczeństwa państwa. Wskazano, że faza odbudowy jest często marginalizowana zarówno w badaniach, jak i w praktyce, co prowadzi do fragmentaryzacji danych, ograniczenia możliwości wyciągania wniosków systemowych oraz zwiększenia ryzyka powstawania luk w bezpieczeństwie. Głównym celem niniejszej publikacji – stanowiącej pierwszą, teoretyczno-konceptualną część cyklu badawczego – jest uporządkowanie siatki pojęciowej oraz precyzyjne rozgraniczenie administrowania informacją od zarządzania informacją w strukturach administracji publicznej. W artykule sformułowano problem badawczy dotyczący wpływu sformalizowanych procedur informacyjnych na zdolności systemu do uczenia się po kryzysie. Wykazano, że informacja na tym etapie pełni funkcję poznawczą, ewaluacyjną i systemotwórczą, a jej jakość, bezpośrednio wpływa na sprawność działań adaptacyjnych państwa. Zarysowano również ramy strukturalne dla drugiej części

cyklu, w której zaprezentowana zostanie autorska typologia informacji postkryzysowej oraz jej praktyczne zastosowanie w polskim systemie bezpieczeństwa.

Słowa kluczowe: cykl adaptacyjny, analiza postkryzysowa, ewaluacja procesów decyzyjnych, zarządzanie informacją, odporność systemowa, ewaluacja strategiczna

Abstract: The article examines the role of information in the recovery phase of crisis management, treating it as a key factor determining the adaptive capacity of the state security system. It is argued that the recovery phase is frequently marginalized both in academic research and practical implementation, resulting in data fragmentation, limited potential for drawing systemic conclusions, and an increased risk of security gaps emerging. The primary objective of this publication – constituting the first, theoretical-conceptual part of a research series – is to systematize the conceptual framework and provide a precise distinction between information administration and information management within public administration structures. The article formulates a research problem concerning the impact of formalized information procedures on the system's capacity for post-crisis learning. It demonstrates that, at this stage, information performs cognitive, evaluative, and system-building functions, while its quality directly affects the effectiveness of the state's adaptive actions. The article also outlines the structural framework for the second part of the research series, which will present an original typology of post-crisis information and its practical application within the Polish national security system.

Keywords: adaptive cycle, post-crisis analysis, evaluation of decision-making processes, information management, systemic resilience, strategic evaluation

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21455544

ACTA
SECURITAS
TOM 2

Administrowanie informacją w fazie odbudowy zarządzania kryzysowego. Część II

Information Administration during the Recovery Phase of Crisis Management. Part II

Artur Woźny

Politechnika Rzeszowska im. Ignacego Łukasiewicza
https://orcid.org/0000-0002-0294-0157

Kacper Mazurek

Politechnika Rzeszowska im. Ignacego Łukasiewicza
https://orcid.org/0009-0002-0818-7407

Piotr Padula

Politechnika Rzeszowska im. Ignacego Łukasiewicza
https://orcid.org/0009-0004-8353-6675

Streszczenie: Artykuł podejmuje analizę roli informacji w fazie odbudowy zarządzania kryzysowego, traktując ją jako kluczowy czynnik determinujący zdolności adaptacyjne systemu bezpieczeństwa państwa. Wskazano, że faza odbudowy jest często marginalizowana zarówno w badaniach, jak i w praktyce, co prowadzi do fragmentaryzacji danych, ograniczenia możliwości wyciągania wniosków systemowych oraz zwiększenia ryzyka powstawania luk w bezpieczeństwie. Głównym celem niniejszej publikacji – stanowiącej pierwszą, teoretyczno-konceptualną część cyklu badawczego – jest uporządkowanie siatki pojęciowej oraz precyzyjne rozgraniczenie administrowania informacją od zarządzania informacją w strukturach administracji publicznej. W artykule sformułowano problem badawczy dotyczący wpływu sformalizowanych procedur informacyjnych na zdolności systemu do uczenia się po kryzysie. Wykazano, że informacja na tym etapie pełni funkcję poznawczą, ewaluacyjną i systemotwórczą, a jej jakość, bezpośrednio wpływa na sprawność działań adaptacyjnych państwa. Zarysowano również ramy strukturalne dla drugiej części

cyklu, w której zaprezentowana zostanie autorska typologia informacji postkryzysowej oraz jej praktyczne zastosowanie w polskim systemie bezpieczeństwa.

Słowa kluczowe: cykl adaptacyjny, analiza postkryzysowa, ewaluacja procesów decyzyjnych, zarządzanie informacją, odporność systemowa, ewaluacja strategiczna

Abstract: The article examines the role of information in the recovery phase of crisis management, treating it as a key factor determining the adaptive capacity of the state security system. It is argued that the recovery phase is frequently marginalized both in academic research and practical implementation, resulting in data fragmentation, limited potential for drawing systemic conclusions, and an increased risk of security gaps emerging. The primary objective of this publication – constituting the first, theoretical-conceptual part of a research series – is to systematize the conceptual framework and provide a precise distinction between information administration and information management within public administration structures. The article formulates a research problem concerning the impact of formalized information procedures on the system's capacity for post-crisis learning. It demonstrates that, at this stage, information performs cognitive, evaluative, and system-building functions, while its quality directly affects the effectiveness of the state's adaptive actions. The article also outlines the structural framework for the second part of the research series, which will present an original typology of post-crisis information and its practical application within the Polish national security system.

Keywords: adaptive cycle, post-crisis analysis, evaluation of decision-making processes, information management, systemic resilience, strategic evaluation

ISBN 978-83-68332-35-3
ISSN 3072-4120
DOI: https://doi.org/10.5281/zenodo.21456901

ACTA
SECURITAS
TOM 2

Teoretyczne aspekty bezpieczeństwa zdrowotnego. Dylematy definicyjne

Theoretical Aspects of Health Security. Definitional Dilemmas

Wioletta Dalidowicz

Wojewódzki Szpital Specjalistyczny we Wrocławiu
https://orcid.org/0009-0002-6132-2436

Streszczenie: W artykule naukowym podjęto problematykę teoretycznego uchwycenia bezpieczeństwa zdrowotnego w kontekście współczesnych wyzwań systemów ochrony zdrowia, ze szczególnym uwzględnieniem doświadczenia pacjenta, zaufania instytucjonalnego oraz warunków relacyjnych. Wychodząc od analizy pojęć dobrostanu, bezpieczeństwa i ochrony zdrowia, przedstawiono autorskie definicje tych kategorii, których dominantą semantyczną jest bezpieczeństwo rozumiane jako proces dynamiczny, relacyjny i instytucjonalny. W odróżnieniu od podejść technokratycznych i epidemiologicznych, zaproponowane przez autora ujęcie integruje perspektywę socjologiczną[1], aksjologiczną i organizacyjną, ukazując ochronę zdrowia publicznego jako rezultat współdziałania pacjenta i instytucji w warunkach niepewności, ryzyka i deficytu zaufania. Analiza teoretyczna wskazuje, że brak sprawiedliwości proceduralnej i relacyjnego uznania może prowadzić do subiektywnego poczucia zagrożenia, nawet przy formalnej sprawności systemu. W artykule naukowym autor podkreśla kluczową rolę zaufania, przewidywalności oraz traktowania pacjenta z poszanowaniem jego godności w budowaniu efektywnego i inkluzyjnego systemu ochrony zdrowia. W zakończeniu przedstawiono kierunki dalszych badań, m.in. walidację operacyjną definicji, badania jakościowe wśród pacjentów oraz analizę możliwości implementacji narzędzi Lean Management w procesach wzmacniania odporności zdrowotnej systemu ochrony zdrowia.

Słowa kluczowe: dobrostan, bezpieczeństwo, bezpieczeństwo zdrowotne, ochrona zdrowia, Lean Management, zaufanie, socjologia zdrowia

[1] W. Dalidowicz, *Perspektywy badawcze bezpieczeństwa zdrowotnego wobec percepcji społecznej*, "Acta Securitas" 2025, t. 1, s. 323-336, [w:] *Wielowymiarowość współczesnego bezpieczeństwa. Odporność Obronność Organizacja*, I. Szkudlarek. (red.), Poznań: Wydawnictwo Naukowe Kontekst, 2025. DOI: https://doi.org/10.5281/zenodo.20133663

ACTA
SECURITAS
TOM 2

Abstract: The scientific article addresses the issue of theoretically conceptualizing health security in the context of contemporary challenges faced by healthcare systems, with particular emphasis on patient experience, institutional trust, and relational conditions. Starting from an analysis of the concepts of well-being, security, and healthcare, the author presents original definitions of these categories, whose semantic dominant is security understood as a dynamic, relational, and institutional process. In contrast to technocratic and epidemiological approaches, the proposed framework integrates sociological, axiological, and organizational perspectives, presenting public healthcare as the result of cooperation between patients and institutions under conditions of uncertainty, risk, and trust deficits. The theoretical analysis indicates that the absence of procedural justice and relational recognition may lead to a subjective sense of threat, even when the system is formally efficient. The author emphasizes the key role of trust, predictability, and treating patients with respect for their dignity in building an effective and inclusive healthcare system. The conclusion outlines directions for further research, including the operational validation of the proposed definitions, qualitative studies among patients, and analysis of the potential implementation of Lean Management tools in processes aimed at strengthening the health resilience of the healthcare system.

Keywords: well-being, security, health security, healthcare, Lean Management, trust, sociology of health

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.20279828

ACTA
SECURITAS
TOM 2

Dezinformacja i bezpieczeństwo pracowników – wyzwania dla bezpieczeństwa i higieny pracy oraz zarządzania kryzysowego w miejscu pracy

Disinformation and Employee Safety – Challenges for Occupational Health, Safety and Crisis Management in the Workplace

Magdalena Tkacz

Politechnika Rzeszowska im. Ignacego Łukasiewicza
https://orcid.org/0000-0002-0999-1643

Streszczenie: Artykuł analizuje wpływ dezinformacji na bezpieczeństwo pracowników oraz na skuteczność systemów zarządzania bezpieczeństwem i higieną pracy (BHP) w organizacjach. Wskazuje, że rozpowszechnianie fałszywych informacji – zarówno w przestrzeni cyfrowej, jak i wewnątrz zakładu pracy – może prowadzić do obniżenia zaufania, błędnych decyzji i wzrostu ryzyka w sytuacjach kryzysowych. Omówiono kluczowe wyzwania stojące przed pracodawcami i służbami BHP w zakresie zarządzania informacją, komunikacji kryzysowej oraz budowania odporności informacyjnej zespołów. Podkreślono znaczenie edukacji pracowników, rzetelnych źródeł informacji i transparentnej polityki komunikacyjnej jako podstaw skutecznego zarządzania bezpieczeństwem pracy w dobie dezinformacji.

Słowa kluczowe: dezinformacja, bezpieczeństwo i higiena pracy (BHP), zarządzanie kryzysowe, komunikacja kryzysowa, odporność informacyjna, zarządzanie ryzykiem

Abstract: The article examines the impact of disinformation on employee safety and the effectiveness of occupational health and safety (OHS) management systems in organizations. It demonstrates that the dissemination of false information – both digitally and within the workplace – can lead to reduced trust, poor decision-making, and increased risk in crisis situations. It discusses the key challenges facing employers and OHS services in information management, crisis communication, and building team resilience. It emphasizes the importance of employee education, reliable sources of information, and a transparent communication policy as the foundations for effective occupational health and safety management in the age of disinformation.

Keywords: disinformation, occupational health and safety (OHS), crisis management, crisis communication, information resilience, risk management

ACTA
SECURITAS
TOM 2

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.21455879

Aplikacje mHealth jako narzędzie wspierania zdrowia psychicznego i zachowań zdrowotnych – możliwości, ograniczenia i wyzwania dla bezpieczeństwa użytkowników

mHealth Applications as a Tool for Supporting Mental Health and Health Behaviors: Opportunities, Limitations, and Challenges to User Safety

Agnieszka E. Kobus-Bogucka

Federacja Naukowa Uniwersytet Vizja
https://orcid.org/0009-0005-9819-6658

Streszczenie: Dynamiczny rozwój technologii mobilnych przyczynił się do wzrostu znaczenia aplikacji mHealth (mobile health) jako narzędzi wspierających promocję zdrowia, profilaktykę oraz opiekę nad osobami z problemami zdrowotnymi. Celem opracowania jest analiza możliwości, ograniczeń i wyzwań związanych z wykorzystaniem aplikacji mHealth, ze szczególnym uwzględnieniem bezpieczeństwa użytkowników. Praca ma charakter narracyjnego przeglądu literatury dotyczącego skuteczności, mechanizmów działania, ograniczeń oraz bezpieczeństwa rozwiązań mobilnych stosowanych w ochronie zdrowia. Omówiono definicję i zakres zastosowań mHealth, a także mechanizmy wspierające utrzymanie zachowań zdrowotnych i adherencję terapeutyczną, w tym samomonitorowanie, informację zwrotną, techniki zmiany zachowania oraz personalizację interwencji. Przedstawiono potencjalne korzyści wynikające z wykorzystania aplikacji mobilnych w obszarze zdrowia psychicznego, zachowań zdrowotnych i realizacji zaleceń terapeutycznych. Wskazano również ograniczenia związane z utrzymaniem zaangażowania użytkowników, zróżnicowaną jakością dostępnych rozwiązań, interoperacyjnością oraz barierami wdrażania technologii cyfrowych w praktyce klinicznej.
Szczególną uwagę poświęcono zagadnieniom bezpieczeństwa, obejmującym ochronę danych zdrowotnych i prywatności, bezpieczeństwo psychologiczne użytkowników oraz ryzyko wykluczenia cyfrowego.
Analiza dostępnych badań wskazuje, że aplikacje mHealth mogą stanowić wartościowe uzupełnienie współczesnej opieki zdrowotnej, jednak ich skuteczność zależy od rodzaju interwencji, jakości zastosowanych rozwiązań oraz sposobu ich wdrożenia. Odpowiedzialne wykorzystanie tych narzędzi wymaga uwzględnienia zarówno efektów zdrowotnych, jak i aspektów technologicznych, organizacyjnych oraz związanych z bezpieczeństwem użytkowników.

Słowa kluczowe: mHealth, zdrowie psychiczne, zachowania zdrowotne, adherencja terapeutyczna, bezpieczeństwo użytkowników

Abstract: Advances in mobile technologies have contributed to the growing importance of mHealth (mobile health) applications as tools supporting health promotion, disease prevention, and the care of individuals with health-related conditions. This paper aims to analyze the opportunities, limitations, and challenges associated with the use of mHealth applications, with particular emphasis on user safety. The study takes the form of a narrative literature review focusing on the effectiveness, mechanisms of action, limitations, and safety of mobile solutions used in healthcare.

The paper discusses the definition and scope of mHealth, as well as mechanisms that support the maintenance of health behaviors and treatment adherence, including self-monitoring, feedback, behavior change techniques, and intervention personalization. Potential benefits of mobile applications in the areas of mental health, health behaviors, and adherence to therapeutic recommendations are presented. The review also highlights limitations related to sustaining user engagement, the varying quality of available solutions, interoperability issues, and barriers to the implementation of digital technologies in clinical practice.

Particular attention is paid to safety-related issues, including the protection of health data and privacy, users' psychological safety, and the risk of digital exclusion.

The analysis of available evidence suggests that mHealth applications may constitute a valuable complement to contemporary healthcare. However, their effectiveness depends on the type of intervention, the quality of the solutions employed, and the manner in which they are implemented. The responsible use of these tools requires consideration not only of health outcomes but also of technological, organizational, and user safety-related factors.

Keywords: mHealth, mental health, healthy behaviours, treatment adherence, user safety

ACTA
SECURITAS
TOM 2

ISBN 978-83-68332-35-3
ISSN 3072-4120
https://doi.org/10.5281/zenodo.20279332

Recenzja monografii naukowej pt. *Kobiety Obronność Bezpieczeństwo. Aspiracje oficerów-kobiet a doskonalenie zawodowe żołnierzy* autorstwa Iwony Szkudlarek

Scientific Review of the Monograph *Women, Defense, Security. The Aspirations of Female Officers and the Professional Development of Soldiers* written by Iwona Szkudlarek

Andrzej Łydka

Uniwersytet Opolski
https://orcid.org/0000-0002-0098-878X

Streszczenie: Monografia naukowa pt. *Kobiety Obronność Bezpieczeństwo. Aspiracje oficerów-kobiet a doskonalenie zawodowe żołnierzy* autorstwa por. dr inż. Iwony Szkudlarek analizuje służbę wojskową kobiet w Polsce w ujęciu historycznym, prawnym i społecznym. Autorka omawia aspiracje zawodowe oficerów-kobiet, motywy wyboru zawodu żołnierza oraz możliwości rozwoju kariery w Siłach Zbrojnych. Praca przedstawia także zarys udziału Polek w działaniach militarnych od średniowiecza po czasy współczesne, wskazując na niedostatki pamięci instytucjonalnej i stereotypy. Istotną część stanowią wyniki badań własnych dotyczących aspiracji i ścieżek kariery oficerów-kobiet oraz rekomendacje dla decydentów wojskowych. Książka adresowana jest do kadry dowódczej, środowiska akademii wojskowych i nauczycieli edukacji dla bezpieczeństwa, a jej celem jest zwiększenie potencjału Sił Zbrojnych poprzez lepsze wykorzystanie kompetencji kobiet. Publikacja, wydana przez Wydawnictwo Naukowe Kontekst, stanowi ważne i uniwersalne studium problematyki służby kobiet w wojsku.

Słowa kluczowe: wojskowa służba kobiet, oficerowie-kobiety, aspiracje zawodowe, Siły Zbrojne RP, doskonalenie zawodowe, historia wojskowości

Abstract: The monograph entitled *Kobiety Obronność Bezpieczeństwo. Aspiracje oficerów-kobiet a doskonalenie zawodowe żołnierzy* written by Lt. Iwona Szkudlarek, Phd (Eng). examines women's military service in Poland from historical, legal, and social perspectives. It analyzes the professional aspirations of female officers, their motivations for joining the armed forces, and their career development opportunities. The book also outlines the participation of Polish women in military structures from the Middle Ages to the present, highlighting gaps in institutional memory and persistent stereotypes. A key section presents the author's empirical research on female officers' aspirations and career paths, along with recommendations for military decision-makers. Intended for commanders, military academics, and security

education teachers, the study aims to strengthen the armed forces by better utilizing women's potential. Published by Kontekst Scientific Publisher, it offers a comprehensive and practical contribution to the field.

Keywords: women military service, female officers, career aspirations, Polish Armed Forces, professional development, military history