Cybersecurity and Law

2025 Nr 2 (14)

DOI: 10.34567/cal/215569

Analysis of the Impact of Regulations on Cybersecurity Threats

Analiza wpływu regulacji na zagrożenia w cyberprzestrzeni

Tomasz ZAWADZKI
Politechnika Warszawska
ORCID: 0000-0003-2758-6454
E-mail: tomasz.zawadzki2@pw.edu.pl

Abstract

Over the past 20 years, the number of various legal acts, standards, and guidelines related to cybersecurity has increased significantly. The expected outcome of these measures was to enhance organizational resilience and reduce the number of incidents. Therefore, the aim of the study described in this article was to review existing regulations and make a preliminary assessment of whether their growing number translates into a decrease in recorded incidents..

The analysis covered data from 2000 to 2025 obtained from open sources and focused on identifying correlations between the number of regulations and the number of incidents. The research methods involved reviewing existing legal acts, standards, and regulations in the field of cybersecurity published worldwide by government bodies, standardization organizations, and technology corporations..

Based on the collected data, final results were developed showing the correlation between the number of regulations and the number of recorded incidents. Subsequently, an attempt was made to analyze the relationships between the examined areas to explain the obtained results.

Conclusions stated that he research should be significantly deepened to explain the nature of the discovered correlation between introduced regulations and the the number of incidents . It was also concluded that regulations are essential, but by themselves may not have a substantial impact on reducing the number of incidents. Furthermore, it is worth considering whether the number of incidents alone is an appropriate metric for assessing the effectiveness of implemented regulations.

Keywords
Incidents, regulation, cybersecurity, law

Streszczenie

W ciągu ostatnich 20 lat liczba różnorakich aktów prawnych, standardów oraz wytycznych dotyczących cyberbezpieczeństwa istotnie wzrosła. Oczekiwanym skutkiem takiego działania było zwiększenie odporności organizacji oraz zmniejszenie liczby incydentów. Tym samym celem badania opisanego w niniejszym artykule był przegląd istniejących regulacji oraz wstępne określenie, czy ich rosnąca liczba przekłada się na zmniejszenie liczby odnotowanych incydentów. Przeprowadzona analiza objęła dane historyczne z lat 2000–2025 pochodzące ze źródeł otwartych oraz skupiła się na znalezieniu korelacji pomiędzy liczbą regulacji a liczbą incydentów

Metody badawcze polegały na przeglądzie istniejących aktów prawnych, norm i regulacji z zakresu cyberbezpieczeństwa, opublikowanych na świecie zarówno przez jednostki rządowe, organizacje normalizacyjne, czy korporacje technologiczne. Przeanalizowano także udostępnione publicznie przez zespoły CSIRT oraz organizacje gromadzące informacje i statystyki dotyczące aktywności cyberprzestępców.

Na podstawie pozyskanych danych opracowane zostały końcowe wyniki przedstawiające korelację pomiędzy liczbą regulacji o liczbą odnotowanych incydentów. W dalszej części w celu wyjaśnienia uzyskanych wyników podjęto próbę przeanalizowania zależności pomiędzy badanymi obszarami.

Uzyskane wyniki stały się także podstawą do wyciągnięcia dalszych wniosków skupiających się na tym, że cyberprzestrzeń jest na tyle rozległą przestrzenią, iż podjęte badania powinny zostać znacząco pogłębione, gdyż wytłumaczenie odkrytych korelacji wymaga poznania zarówno szczegółowej natury wprowadzanych regulacji jak i natury samych incydentów. Wywnioskowano także, że regulacje są niezbędne, ale same w sobie mogą nie mieć, aż tak znacznego wpływu na redukcję liczby incydentów, a ponadto należy się zastanowić, czy sama liczba incydentów jest właściwym miernikiem do oceny skuteczności wprowadzonych regulacji.

Słowa kluczowe

incydenty, normy, cyberbepieczeństwo, prawo

Badania zostały sfinansowane ze środków statutowych Politechniki Warszawskiej.

This research was supported by statutory funds from the Warsaw University of Technology.

Wprowadzenie

W ostatnich dwóch dekadach obserwuje się coraz bardziej dynamiczny rozwój technologii informacyjnych, w szczególności związany z rozwojem sieci Internet, stron www, przenośnych komputerów osobistych oraz telefonów z dostępem do Internetu. Powstałe jeszcze w latach ’90-tych XX w. technologie takie jak HTML, PHP, CSS czy JAVA otworzyły drogę do globalnego oferowania usług komunikacyjnych i handlowych za pomocą Internetu, a ich zwiększająca się dostępność coraz bardziej przyciągała do siebie nie tylko indywidualnych użytkowników, ale z biegiem czasu całe jednostki organizacyjne zarówno komercyjne jak i publiczne oraz rządowe. Trend ten został zauważony przez organizacje przestępcze, które zaczęły upatrywać swoich nowych zysków, nie tylko w tradycyjnych formach działania poza prawem, ale także w nieustannie

poszerzającej się cyberprzestrzeni. Z jednej strony zaczęło powstawać wiele nowych usług oraz innowacyjnych technologii internetowych, a z drugiej coraz bardziej intensywnie poszukiwano sposobów nieuprawnionego dostępu wdrażanych usług oraz przełamywania zabezpieczeń w pojawiających się technologiach. Wraz z upowszechnianiem się usług oferowanych w sposób cyfrowy, pojawiające się w cyberprzestrzeni zagrożenia zaczęły być postrzegane jako poważne ryzyko nie tylko narażające na straty pojedynczych użytkowników, ale także uderzające w bezpieczeństwo dużych organizacji i państw w tym ich stabilność finansową, czy zachowanie poufności przetwarzanych danych osobowych.

W odpowiedzi na te wyzwania zarówno rządy, organizacje międzynarodowe jak i instytucje branżowe wprowadziły liczne regulacje mające na celu podniesienie poziomu ochrony systemów informatycznych, minimalizację ryzyka incydentów oraz zwiększenie odporności organizacji na ataki cybernetyczne. Wraz z upływem lat, co jest procesem naturalnym, zaobserwowano ewolucję podejścia do cyberbezpieczeństwa – od pierwszych regulacji dotyczących ochrony danych osobowych i przestępstw komputerowych, po kompleksowe ramy prawne obejmujące zarządzanie ryzykiem, raportowanie incydentów, certyfikację produktów oraz wymogi dla operatorów usług kluczowych.

Uwzględniając dynamikę rozwoju usług cyfrowych i pojawiające się wraz z nimi nowe zagrożenia, autor niniejszego artykułu, bazując na ogólnie dostępnych danych, jako cel główny postanowił zbadać, na ile wdrażane na świecie na przestrzeni ostatnich 20 lat regulacje prawne i standardy szeroko rozumianego bezpieczeństwa informacyjnego przeciwdziałają rozwojowi zagrożeń. Przyjęto hipotezę, że rosnąca liczba regulacji zmniejszy liczbę zagrożeń w cyberprzestrzeni.

Ponieważ, ze względów bezpieczeństwa, szczegółowe informacje o wystąpieniu i zmaterializowaniu się zagrożenia, a także o jego następstwach i skutkach, często nie są podawane do publicznej wiadomości, autor zdefiniował pierwszy cel szczegółowy jakim był wybór wymiernego wskaźnika, który w sposób ilościowy pokaże wieloletni trend występowania zagrożeń w cyberprzestrzeni. Drugi celem szczegółowym był przegląd i analiza wprowadzanych do powszechnego stosowania norm i regulacji prawnych związanych z cyberbezpieczeństwem w wybranych krajach świata, które powszechnie uznawane są za kraje o rozwiniętej infrastrukturze teleinformatycznej. Trzecim celem szczegółowym było z kolei stworzenie diagramu przyczynowo-skutkowego oraz bazującego na nim generycznego modelu symulacyjnego, na podstawie którego można analizować relacje pomiędzy wprowadzanymi regulacjami, a zidentyfikowanymi trendami zagrożeń oraz rozbudowywać go o kolejne parametry, które połączone ze sobą pewnymi relacjami mogą tworzyć bardziej rozbudowany system wpływający na funkcjonowanie procesów bezpieczeństwa w cyberprzestrzeni.

Zastosowane przez autora metody badawcze to analiza i przegląd dostępnych regulacji z obszaru cyberbezpieczeństwa, analiza publicznie dostępnych danych dotyczących występujących zagrożeń, analiza korelacji pomiędzy regulacjami a zagrożeniami oraz analiza systemowa mająca za zadanie zidentyfikowanie innych elementów mających wpływ na bezpieczeństwo cyberprzestrzeni.

Niniejszy artykuł został podzielony na cztery części. W pierwszej dokonano przeglądu i analizy pojawiających się regulacji, natomiast w drugiej charakterystyki pojawiających się na przestrzeni lat zagrożeń. Czwarta część artykułu zawiera analizę korelacji pomiędzy regulacjami a zagrożeniami. W ostatniej, piątej części omówione są wnioski końcowe oraz propozycje dalszych badań.

Wybór wskaźnika trendów zagrożeń w cyberprzestrzeni

Ponieważ głównym celem badania było znalezienie korelacji pomiędzy wprowadzanymi regulacjami, a poziomem zagrożeń, w pierwszej kolejności autor skupił się na wyborze wskaźnika, który mógłby posłużyć do oszacowania trendów zagrożeń. Biorąc pod uwagę różnorodność ataków na którą składają się m.in.:

- ransomware – złośliwe oprogramowanie szyfrujące dane i żądające okupu,
- phishing – próby wyłudzenia danych poprzez fałszywe wiadomości e-mail lub strony internetowe,
- DDoS – ataki na dostępność usług poprzez masowe obciążenie serwerów,
- APT (Advanced Persistent Threats) – długotrwałe, ukierunkowane kampanie cyberataków,
- kradzież danych – nieautoryzowany dostęp do poufnych informacji,
- malware – różnorodne formy złośliwego oprogramowania, w tym trojany i wirusy,

oraz szerokie spektrum efektów ich działania, obejmujące:

- straty finansowe,
- straty wizerunkowe,
- niedostępność usług,
- niepoprawne działanie oprogramowania,
- dodatkowe zaangażowanie pracowników,
- kary umowne,

wbrew pozorom nietrywialnie jest wybrać pojedynczy obiektywny wskaźnik, który dałby globalny obraz pojawiających się trendów zagrożeń w cyberprzestrzeni. Ponieważ XX i XXI wiek, to czas w którym dzięki rozwojowi technologii rozkwitł kapitalizm, wydawałoby się, że najlepszym wskaźnikiem byłyby straty finansowe, gdyż każda niedostępność lub dodatkowe zaangażowanie może być wyrażone jako koszt finansowy. Analizując to głębiej nie okazuje się to jednak aż tak oczywiste, z dwóch głównych powodów:

1. dbając o swój wizerunek oraz bezpieczeństwo organizacje nie publikują informacji o stratach finansowych powstałych wskutek ataków cybernetycznych, gdyż mogłoby to przynieść nieprzewidziane konsekwencje np. w postaci odpływu potencjalnych inwestorów,
2. pomimo, iż to możliwe organizacje, nie są chętne do wyceniania każdej odnotowanej próby ataku, w szczególności jeżeli jego efekty da się stosunkowo szybko zniwelować, gdyż wymagałoby zaangażowania dodatkowych zasobów.

Poszukując innego bardziej uniwersalnego wskaźnika autor skupił swoją uwagę na liczbie incydentów. Incydent to przede wszystkim zdarzenie, które faktycznie narusza integralność, poufność lub dostępność systemów informatycznych. W przeciwieństwie do szeregu innych wskaźników, liczba incydentów odzwierciedla realne działania cyberprzestępców. Jest ona

wskaźnikiem łatwym do zdefiniowania i porównania w czasie oraz pomiędzy organizacjami. Inne wskaźniki mogą np. wielkość straty finansowej, mogą być są subiektywne, natomiast incydent jest obiektywnym zdarzeniem binarnym – został odnotowany lub nie. Ponadto, strata finansowa, czas niedostępności, czy błędnie działające oprogramowanie wskazują na efekty zmaterializowanych zagrożeń, lub zdolności do przeciwdziałania nim, a nie na ogólnie występujący trend.

Liczba incydentów okazuje się więc uniwersalnym, obiektywnym i praktycznym miernikiem zagrożeń w cyberprzestrzeni, pozwalając przy tym na analizę trendów. Spadek liczby incydentów w czasie może świadczyć o poprawie przyjętych strategii ochrony, a jej wzrost o pojawieniu się nowych zagrożeń. Dodatkowo, organizacje skłonne są publikować, bądź przekazywać współpracującym z nimi jednostkom odpowiedzialnym za cyberbezpieczeństwo raporty zawierające liczbę odnotowanych incydentów, gdyż nie zdradzają w ten sposób swoich słabości, skutków odnotowanych ataków lub wdrożonych mechanizmów bezpieczeństwa. Dlatego też liczba incydentów jest ogólnodostępnym wskaźnikiem, który daje obraz trendów związanych z rozwojem zagrożeń.

Biorąc powyższe pod uwagę do dalszych badań autor wybrał liczbę incydentów, jako wskaźnik mogący służyć do badania korelacji pomiędzy regulacjami a zagrożeniami w cyberprzestrzeni.

Przegląd światowych regulacji dotyczących cyberbezpieczeństwa

Kolejnym krokiem w prowadzonych badaniach był przegląd istniejących regulacji związanych z cyberbezpieczeństwem oraz sprawdzenie intensywność ich publikacji w ostatnich dwudziestu latach. Aby otrzymać reprezentatywne wyniki wskazujące na trendy globalne, dokonany został przegląd regulacji publikowanych na poziomie krajowym, regionalnym, instytucjonalnym oraz komercyjnym. W pierwszej kolejności wytypowanych zostało 10 krajów z różnych kontynentów, które uznawane są jako dojrzałe cyfrowo. Wytypowane zostały następujące kraje: Brazylia, Chiny, Estonia, Francja, Irlandia, Niemcy, Polska, Rosja, USA oraz Wielka Brytania, a do potwierdzenia ich dojrzałości posłużono się następującymi wskaźnikami:

- DESI (ang. Digital Economy and Society Index) – indeks Gospodarki Cyfrowej i Społeczeństwa Cyfrowego w skali od 0 do 100, opracowany przez Komisję Europejską. Służy do oceny poziomu cyfryzacji państw członkowskich UE oraz porównania ich postępów w rozwoju gospodarki cyfrowej[1],
- DAI (ang. Digital Adoption Index) – opracowany przez Bank Światowy w 2016 roku ogólnoświatowy indeks, mierzący możliwości kraju w zakresie zastosowania technologii cyfrowych w trzech wymiarach gospodarki, tj,: ludzie, rząd, biznes. Indeks ten obejmuje 180 krajów. Jest wyskalowany od 0 do 1. DAI jest średnią trzech podrzędnych indeksów obejmujących technologie niezbędne do promowania rozwoju w erze cyfrowej poprzez zwiększanie produktywności i przyspieszanie szeroko zakrojonego wzrostu dla *biznesu*, rozszerzanie możliwości i poprawa dobrobytu dla ludzi oraz

[1]The Digital Economy and Society Index (DESI), https://digital-strategy.ec.europa. eu/en /policies/desi

zwiększanie efektywności i odpowiedzialności za świadczenie usług dla rządu[2],

- WDCR (ang. World Digital Competitiveness Ranking) – globalny ranking opracowywany przez International Institute for Management Development (IMD), oceniający zdolność krajów do przystosowania się do transformacji cyfrowej i wykorzystania technologii w gospodarce, administracji oraz społeczeństwie[3],
- ITU IDI (ang. ITU ICT Development Index) – wskaźnik opracowany przez Międzynarodowy Związek Telekomunikacyjny (International Telecommunication Union – ITU), mierzący poziom rozwoju technologii informacyjno-komunikacyjnych (ICT) w poszczególnych krajach[4],
- EGDI (ang. E-Government Development Index) – indeks przestawiający stan rozwoju e-administracji w państwach członkowskich Organizacji Narodów Zjednoczonych. Uwzględnia on takie cechy jak: dostęp, infrastruktura, poziom edukacji. Umożliwia jest odzwierciedlenie sposobu, w jaki dany kraj wykorzystuje technologie informacyjne w celu promowania dostępu i integracji usług dla swoich obywateli. EGDI jest zbiorczą miarą trzech ważnych wymiarów e-administracji, tj.: świadczenia usług online, łączności telekomunikacyjnej i potencjału ludzkiego[5].

Zestawienie krajów wraz ze wskaźnikami ich dojrzałości cyfrowej przedstawia Tabela 1.

Tabela 1. *Kraje i ich wartości wskaźników dojrzałosci cyfrowej*

Kraj	DESI	DAI	WDCR	ITU IDI	EGDI
Brazylia	nie dotyczy	0,63	53	82.0	0,84
Chiny	nie dotyczy	0,67	12	85.8	0,87
Estonia	96	0,79	26	97.9	0,97
Francja	71	0,8	21	89.8	0,87
Irlandia	87	0,82	16	90.7	0,91
Niemcy	78	0,81	18	87.8	0,93
Polska	70	0,74	45	95.8	0,86
Rosja	nie dotyczy	0,68	nie dotyczy	90.6	0,85
USA	nie dotyczy	0,87	2	96,7	0,91
Wielka Brytania	nie dotyczy	0,83	19	93.6	0,95

Źródło: *opracowanie własne*

[2]Digital Adopion Index, https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index [dostęp: 13.12.2025].
[3] World Digital Competitiveness Ranking, https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/ [dostęp: 13.12.2025].
[4] ITU IDI https://www.itu.int/itu-d/reports/statistics/idi2025/ [dostęp: 13.12.2025].
[5] EGDI https://publicadministration.un.org/egovkb/en-us/Data-Center [dostęp: 13.12.2025].

Tablę 1 zatytuowaną „Kraje i ich wartości wskaźników dojrzałosci cyfrowej" opracowano na podstawie DESI[6], DAI[7], WDCR[8], ITU IDI[9], EGDI[10].

Dla wybranych krajów oraz dodatkowo dla Unii Europejskiej zidentyfikowano najważniejsze wprowadzone przez nie na szczeblu rządowym regulacje prawnych dotyczących cyberbezpieczeństwo. Ich zestawienie zawarte jest w Tabeli 2.

Tabela 2. *Zestawienie najważniejszych regulacji z obszaru cyberbezpieczeństwo dla wytypowanych krajów.*

Rok	Kraj	Akt Prawny	Zakres aktu prawnego
1986	USA	Computer Fraud and Abuse Act	Penalizacja nieautoryzowanego dostępu do systemów komputerowych
1996	USA	HIPAA	
2009	USA	HITECH Act	
2002	USA	Federal Information Security Management Act (FISMA)	Ramowy system bezpieczeństwa informacji w agencjach federalnych
2015	USA	Cybersecurity Information Sharing Act	Wymiana informacji o zagrożeniach cybernetycznych
2021	USA	Executive Order 14028	Poprawa bezpieczeństwa cybernetycznego kraju
2023	USA	National Cybersecurity Strategy	Pięć filarów: obrona infrastruktury, zwalczanie cyberprzestępczości, odporność cyfrowa, współpraca międzynarodowa, innowacje
2005	Polska	Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne	Podstawy e-administracji
2018	Polska	Ustawa o krajowym systemie cyberbezpieczeństwa	Implementacja dyrektywy NIS
2019	Polska	Strategia Cyberbezpieczeństwa RP 2019–2024	Ochrona infrastruktury krytycznej, rozwój kompetencji, współpraca międzynarodowa
2025	Polska	Strategia Cyberbezpieczeństwa RP 2025–2029	Kontynuacja działań, nowe cele w zakresie odporności cyfrowej
2025	Polska	Strategia Informatyzacji Państwa do 2035	Rozwój e-administracji, cyfryzacja usług publicznych
1991	Niemcy	Bundesdatenschutzgesetz (BDSG)	Ochrona danych osobowych

[6] The Digital Economy and Society Index (DESI), https://digital-strategy.ec.europa. eu/en/policies/desi [dostęp: 13.12.2025].
[7] Digital Adopion Index, https://www.worldbank.org/en/publication/wdr2016/Digital-Adoption-Index [dostęp: 13.12.2025].
[8] World Digital Competitiveness Ranking, https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking/ [dostęp: 13.12.2025].
[9] ITU IDI https://www.itu.int/itu-d/reports/statistics/idi2025/ [dostęp: 13.12.2025].
[10] EGDI https://publicadministration.un.org/egovkb/en-us/Data-Center [dostęp: 13.12.2025].

2015	Niemcy	IT-Sicherheitsgesetz	Bezpieczeństwo infrastruktury krytycznej
2021	Niemcy	Cybersicherheitsstrategie für Deutschland 2021	Cyfrowa suwerenność, ochrona infrastruktury krytycznej, współpraca UE
1978	Francja	Loi Informatique et Libertés	Ochrona danych osobowych
2018	Francja	Loi de programmation militaire (cyber)	Bezpieczeństwo cybernetyczne w obronności
2021	Francja	Strategie nationale pour la sécurité du numérique	Bezpieczeństwo cyfrowe w polityce obronnej i gospodarczej
1990	Wielka Brytania	Computer Misuse Act	Przestępstwa komputerowe
2018	Wielka Brytania	Data Protection Act	Implementacja GDPR
2022	Wielka Brytania	UK National Cyber Strategy 2022	Rozwój NCSC, National Cyber Force, globalna cyberpotęga
2000	Estonia	Public Information Act	Podstawy e-administracji
2018	Estonia	Cybersecurity Act	Implementacja NIS
2019	Estonia	Estonian Cybersecurity Strategy 2019–2022	Integracja z polityką UE, odporność infrastruktury, e-usługi
1988	Irlandia	Data Protection Act	Ochrona danych osobowych
2018	Irlandia	Data Protection Act (GDPR)	Implementacja GDPR
2019	Irlandia	National Cyber Security Strategy 2019–2024	Ochrona usług krytycznych, rozwój kompetencji, współpraca międzynarodowa
2006	Rosja	Federal Law on Personal Data	Ochrona danych osobowych
2016	Rosja	Doktryna bezpieczeństwa informacyjnego FR	Bezpieczeństwo informacji w sektorze publicznym i prywatnym
2017	Rosja	Yarovaya Law	Regulacje dotyczące przechowywania danych i bezpieczeństwa
2017	Rosja	Strategia rozwoju społeczeństwa informacyjnego 2017–2030	Rozwój cyfryzacji i bezpieczeństwa danych
2014	Brazylia	Marco Civil da Internet	Ramowy akt dotyczący internetu
2018	Brazylia	Lei Geral de Proteção de Dados (LGPD)	Ochrona danych osobowych
2020	Brazylia	Estratégia Nacional de Segurança Cibernética (E-Ciber)	Ochrona infrastruktury krytycznej, ramy dla bezpieczeństwa danych
2016	Chiny	Cybersecurity Strategy of China	Bezpieczeństwo sieci i danych, rozwój regulacji
2017	Chiny	Cybersecurity Law	Bezpieczeństwo sieci i danych
2021	Chiny	Data Security Law	Bezpieczeństwo danych
1995	UE	Dyrektywa 95/46/WE	Ochrona danych osobowych
2014	UE	Rozporządzenie eIDAS	Identyfikacja elektroniczna i usługi zaufania dla transakcji elektronicznych
2015	UE	PSD2	
2016	UE	Ogólne Rozporządzenie o Ochronie Danych (GDPR)	Ochrona danych osobowych
2016	UE	Dyrketywa NIS	Bezpieczeństwo sieci i systemów
2019	UE	Cybersecurity Act	Certyfikacja bezpieczeństwa ICT

2020	UE	EU Cybersecurity Strategy for the Digital Decade	Bezpieczeństwo sieci, odporność cyfrowa, współpraca międzynarodowa
2022	UE	Dyrektywa NIS2	Bezpieczeństwo sieci i systemów
2022	UE	DORA	
2024	UE	CRA	Wymogi bezpieczeństwa dla produktów cyfrowych wprowadzanych na rynek UE

Źródło: *opracowanie własne*

Poza dokumentami rządowymi wraz z rozwojem technologii informacyjnych pojawiały się dokumenty normalizacyjne wydawane przez organizacje międzynarodowe jakie jak ISO oraz organizacje krajowe takie jak NIST, którego rekomendacje mają ogólnoświatowe zastosowanie. Chronologiczne zestawienie najważniejszych z nich przedstawia Tabela 3.

Tabela 3. *Zestawienie najważniejszych ogólnoświatowych standardów z obszaru cyberbezpieczeństwa.*

Rok	Organizacja	Nazwa standardu lub rekomendacji	Zakres
1999	ISO	ISO/IEC 15408 (Common Criteria)	Podstawa certyfikacji bezpieczeństwa produktów i systemów
2000	ISO	ITSec	Poprzednik Common Criteria, stosowany w UE
2005	ISO	ISO/IEC 27001	Norma certyfikacyjna dla ISMS
2005	ISO	ISO/IEC 27002	Zbiór kontroli bezpieczeństwa, aktualizacja 2022
2009	ISO	ISO/IEC 27003	Pomoc w implementacji ISO/IEC 27001
2010	ISO	ISO/IEC 27004	Metody monitorowania i oceny
2011	ISO	ISO/IEC 27005	Analiza i ocena ryzyka
2013	ISO	ISO/IEC 27006	Audyt i certyfikacja zgodności z ISO/IEC 27001
2012	ISO	ISO/IEC 27032	Rozszerzenie poza ISMS, ochrona przed cyberzagrożeniami
2010	ISO	ISO/IEC 27033	Projektowanie i zarządzanie bezpiecznymi sieciami
2010	NIST	NIST SP 800-37	Proces zarządzania ryzykiem dla systemów federalnych
2011	NIST	NIST SP 800-88 Rev. 1	Bezpieczne usuwanie danych z nośników
2011	ISO	ISO/IEC 27034	Zasady tworzenia bezpiecznego oprogramowania
2011	ISO	ISO/IEC 27035	Procedury reagowania na incydenty
2012	ISO	ISO/IEC 27037	Wytyczne dla dochodzeń cyfrowych
2012		NIST SP 800-30	Metodyka oceny ryzyka w systemach informatycznych
2013	ISO	ISO/IEC 27036	Zarządzanie ryzykiem w łańcuchu dostaw
2013		NIST SP 800-115	Metody testowania i oceny bezpieczeństwa systemów IT

2014	NIST	NIST Cybersecurity Framework (CSF)	Model zarządzania ryzykiem oparty na pięciu funkcjach: Identify, Protect, Detect, Respond, Recover
2015	ISO	ISO/IEC 27040	Ochrona danych w systemach storage
2015	ISO	ITIL v3	Najlepsze praktyki ITSM, elementy bezpieczeństwa
2015	NIST	NIST SP 800-82 Rev. 2	Bezpieczeństwo systemów sterowania przemysłowego
2016	NIST	NIST SP 800-171 Rev. 2	Wymagania ochrony informacji w systemach niejawnych
2017	NIST	NIST SP 800-63-3	Wytyczne dotyczące zarządzania tożsamością cyfrową i uwierzytelniania
2018	NIST	NIST SP 800-61 Rev. 2	Wytyczne dotyczące reagowania na incydenty bezpieczeństwa
2019	ISO	ISO/IEC 27017	Wytyczne dla dostawców i klientów cloud computing
2019	ISO	ISO/IEC 27018	Prywatność w środowiskach cloud
2019	ISO	ISO/IEC 27701	System zarządzania informacjami o prywatności (PIMS)
2020	NIST	NIST SP 800-53 Rev. 5	Zbiór kontroli bezpieczeństwa i prywatności dla systemów IT
2020	NIST	NIST SP 800-207	Architektura bezpieczeństwa oparta na zasadzie „nigdy nie ufaj, zawsze weryfikuj” (Zero Trust)
2022	ISO	ISO/IEC 27002 (aktualizacja)	Dodanie atrybutów ułatwiających zarządzanie ryzykiem

Źródło: *opracowanie własne*

Dodatkowa, tego poza normami międzynarodowymi pojawiły się liczne standardy sektorowe oraz korporacyjne opracowane przez firmy technologiczne takie jak IBM, Oracle czy Microsoft. Ich chronologiczne zestawienie zawiera Tabela 4.

Tabela 4. *Zestawienie najważniejszych sektorowych i korporacyjnych standardów z obszaru cyberbezpieczeństwa*

Rok	Sektor / Organizacja	Nazwa standardu lub rekomendacji	Zakres
2004	Microsoft	MS SDL	Zasady bezpiecznego wytwarzania oprogramowania
2010	OWASP	OWASP Secure Coding Practices Quick Reference Guide	Przewodnik pod dobrych praktykach programowania, które można wdrożyć bez konieczności dogłębnej znajomości luk w zabezpieczeniach
2018	IBM	IBM Secure Engineering Framework (Redguide)	Dobre praktyki bezpieczeństwa coraz bardziej niezbędne przy tworzeniu produktów i aplikacji działających w światowej infrastrukturze cyfrowej
2024	Bankowość	PCI DSS v4.0.1	12 wymagań bezpieczeństwa dla środowiska danych kart (CDE); kontrola techniczna i organizacyjna

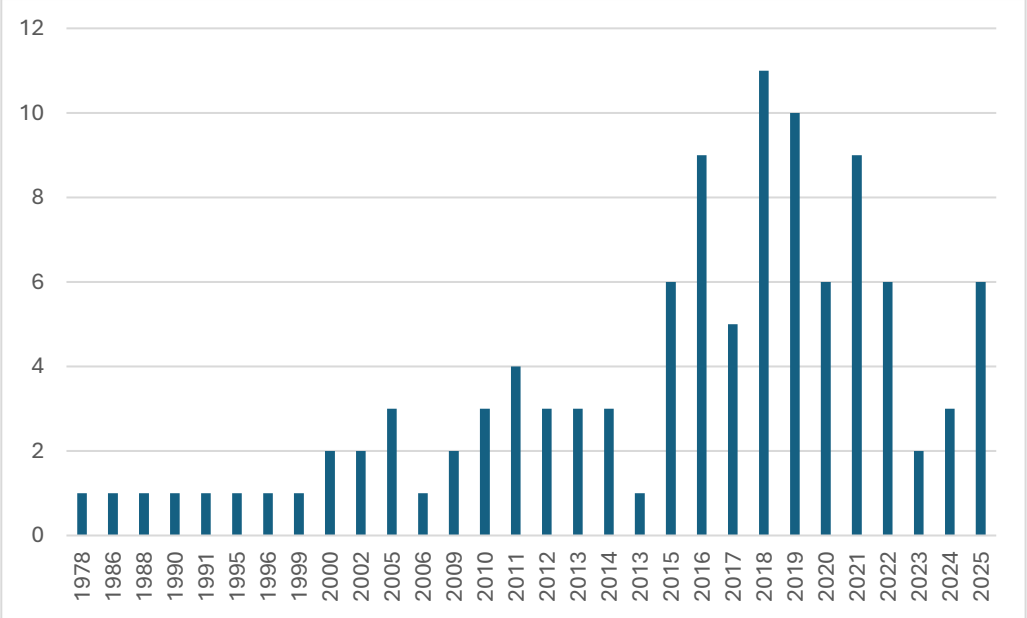
2025	Oracle	Oracle Database Security Guide 19c	Przewodnik konfiguracji zabezpieczeń baz danych Oracle.
2025	Oracle	Oracle Secure Coding Standards	Przewodnik dla programistów w dążeniu do tworzenia bezpiecznego kodu

Źródło: *opracowanie własne*

Należy tutaj zaznaczyć, że, przedstawione w Tabeli od 2 do 4 zestawienia mogę nie ujmować wszystkich przygotowanych w badanym okresie regulacji, gdyż celem badania nie było uzyskanie pełnego ich zbioru, lecz poznanie związanych z nimi trendów. Roczna intensywność publikacji oraz ich sumaryczna liczba w każdym roku przedstawione są odpowiednio na Rys. 1 oraz Rys. 2. Na pierwszym z nich widoczny jest wyraźny wzrost intensywności publikacji od roku 2015, natomiast na drugim widoczna jest stale powiększająca się ich liczba. Co istotne zaobserwowany trend ma charakterystykę nieliniową, którą można przybliżyć za pomocą wielomianu drugiego stopnia przedstawionego za pomocą formuły (1).

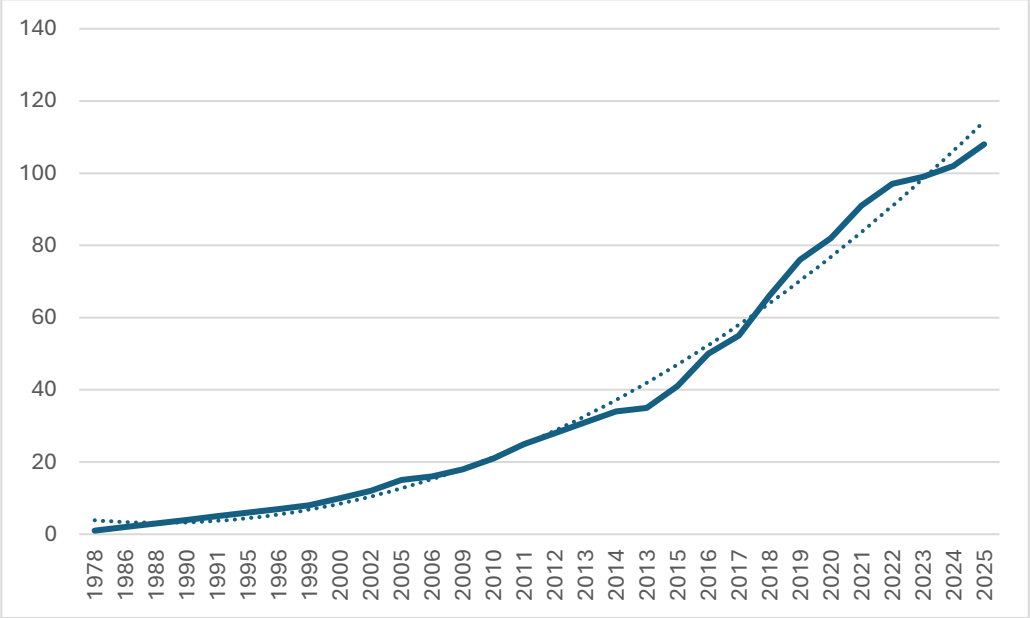
$$y = 0{,}1541x^2 - 0{,}9676x + 4{,}7103 \quad przy\ R^2 = 0{,}9902 \tag{1}$$

Rys. 1. *Roczna intensywność zidentyfikowanych regulacji z obszaru cyberbezpieczeństwo w latach 1978-2025*



Źródło: *opracowanie własne*.

Rys. 2. *Łączna liczba zidentyfikowanych regulacji z obszaru cyberbezpieczeństwo na przestrzeni lat 1978-2025*

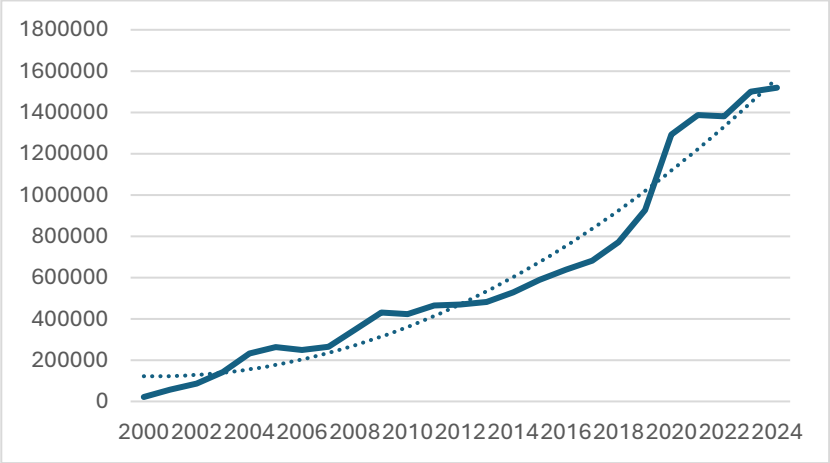


Źródło: *opracowanie własne*

Analiza korelacji

Kolejnym krokiem badań była analiza opublikowanej liczby incydentów w wytypowanych krajach na przestrzeni lat 2000-2025. Okazało się, że informacje takie w początkowym okresie nie były upubliczniane, niemniej wraz z upływem lat były udostępniane głównie przez powołane do tego celu instytucje pełniące rolę krajowych zespołów CSIRT. Rys. 3. przedstawia coroczną liczbę odnotowanych w badanym okresie incydentów.. Zaobserwowany trend ma charakter nieliniowy i można go aproksymować za pomocą wielomianu drugiego stopnia, przedstawionego za pomocą formuły (2).

Rys. 3. *Sumaryczna liczba incydentów odnotowanych w wytypowanych krajach*



Źródło: *opracowanie własne*

$$y = 2588{,}9x^2 - 7152{,}8x + 126658$$
$$przy: R^2 = 0{,}9605 \quad (2)$$

Ostatnim etapem badań było zestawienie liczby dostępnych w danym roku publikacji z zakresu cyberbezpieczeństwo wraz z liczbą zgłoszonych incydentów, co przedstawia Tabela 4 oraz wyliczenie współczynnika korelacji liniowej Pearsona pomiędzy tymi dwoma zmiennymi. Wartość współczynnika korelacji przedstawia formuła (3).

Tabela 5. *Porównanie liczby korporacyjnych standardów z obszaru cyberbezpieczeństwa*

Rok	Liczba incydentów	Liczba regulacji
2000	21500	10
2001	57200	10
2002	87000	12
2003	142000	12
2004	232000	12
2005	263000	15
2006	249000	16
2007	264000	16
2008	347000	18
2009	431000	18
2010	423000	21
2011	464000	25
2012	469000	28
2013	482000	31
2014	529000	34
2015	588000	41
2016	638000	50
2017	681000	55
2018	771000	66
2019	927000	76
2020	1291790	82
2021	1387376	91
2022	1380944	97
2023	1500418	99
2024	1519532	102

Źródło: *opracowanie własne*

$$cor = 0{,}97976 \quad (3)$$

Podsumowanie

Uzyskane w efekcie przeprowadzenia badań wyniki wykazały, że współczynnik korelacji Pearsona pomiędzy liczbą dostępnych regulacji z obszaru cyberbezpieczeństwa, a liczbą incydentów jest bliski wartości 1, co z zgodnie z definicją tego współczynnika oznacza, że wzrost regulacji powoduje także wzrost liczby incydentów. Należy więc dokonać analizy i interpretacji uzyskanych wyników, gdyż celem wprowadzanych regulacji jest możliwe szeroka eliminacja zagrożeń, a tym samym zmniejszenie się liczby incydentów, a nie ich wzrostu.

Jako jeden z głównych powodów takiego wyniki należy wskazać, że publikowane regulacje, w ostatnich latach regulacje, w szczególności o charakterze legislacyjnym, wymuszają utworzenie szeregu instytucji takich jak krajowe lub sektorowe zespoły CSIRT, które są odpowiedzialne za przyjmowanie zgłoszeń o incydentach oraz publikowanie rocznych raportów ze swojej działalności. Raporty te zawierają m.in. liczbę odnotowanych incydentów. W przeszłości, w szczególności przed rokiem 2015 zespoły tego typu często działały wyłącznie wewnątrz organizacji, nie upubliczniając swoich obserwacji o dotyczących zaobserwowanych ataków.

Drugim powodem uzyskania tak wysokiego współczynnika korelacji jest fakt, że wdrożenie regulacji dotyczących cyberbezpieczeństwa wymusza w organizacjach formalne prowadzenie ewidencji potencjalnych zagrożeń oraz odnotowanych incydentów. Zapisy z ewidencji są później podstawą do przygotowywania corocznych raportów, których mowa powyżej. W początkowych latach badanego okresu, wdrażanie regulacji bezpieczeństwa nie było aż tak popularne, w związku z czym organizacje nie miały obowiązku prowadzenia ewidencji incydentów, w związku z czym nie były one publicznie raportowane.

Kolejnymi ważnymi przyczynami uzyskanych wyników są: dynamiczny wzrost powierzchni ataku związany z rozwojem IoT, chmury, sztucznej inteligencji i pracy zdalnej; profesjonalizacja cyberprzestępczości, w tym rozwój usług typu ransomware-as-a-service; luka między regulacją a jej wdrożeniem wynikająca z wysokich kosztów i niedoboru kompetencji; złożoność ekosystemów i łańcucha dostaw; opóźnienie efektu regulacji, które jest widoczne dopiero po latach; oraz większa transparentność raportowania, co zwiększa liczbę zgłoszeń w statystykach.

Przeprowadzone badanie oraz odpowiednia interpretacja wyników pokazała jak złożona jest cyberprzestrzeń. Z kolei regulacje są niezbędne, ale same w sobie nie redukują liczby incydentów. Kluczowe jest ich skuteczne wdrożenie i egzekwowanie, integracja z technologiami ochronnymi (np. architektura Zero Trust, automatyzacja zarządzania podatnościami), edukacja i budowa kultury bezpieczeństwa, a także współpraca międzynarodowa i wymiana informacji o zagrożeniach.

Bibliografia

Brown J., Brown M., The Guideto Cyber and Data Privacy Investigations - Fourth Edition, https://globalinvestigationsreview.com/guide/the-guide-cyber-investigations/fourth-edition/article/the-shifting-nature-of-cyber-incident-regulatory-reporting-obligations-in-the-united-states, 2025.

Bundesdatenschutzgesetz (BDSG), https://www.gesetze-im-internet.de/bdsg_2018/
Computer Fraud and Abuse Act of 1986 (Public Law 99-474), https://www.congress.gov/bill/99th-congress/house-bill/4718
Computer Misuse Act 1990, https://www.legislation.gov.uk/ukpga/1990/18/contents
Cyber Resilience Act (CRA), https://eur-lex.europa.eu/
Cybersecurity Act, https://www.riigiteataja.ee/en/
Cybersecurity Act (UE 2019/881), https://eur-lex.europa.eu /
Cybersecurity Information Sharing Act of 2015, https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%2015.pdf
Cybersecurity Law, http://www.npc.gov.cn/
Cybersecurity Strategy of China, http://www.cac.gov.cn/
Cybersicherheitsstrategie für Deutschland 2021, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/cybersicherheitsstrategie-2021.pdf
Data Protection Act (Ireland), https://www.irishstatutebook.ie/
Data Protection Act 2018, https://www.legislation.gov.uk/ukpga/2018/12/contents,
Data Security Law, http://www.npc.gov.cn/
Doktryna bezpieczeństwa informacyjnego FR, http://www.kremlin.ru/
DORA (Digital Operational Resilience Act), https://eur-lex.europa.eu/
DORA (Rozporządzenie (UE) 2022/2554), https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX%3A32022R2554
Dyrektywa 95/46/WE, https://eur-lex.europa.eu/
Dyrektywa NIS (UE 2016/1148), https://eur-lex.europa.eu/
Dyrektywa NIS2 (UE 2022/2555), https://eur-lex.europa.eu/
ePrivacy Directive 2002/58/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32002L0058
Estonian Cybersecurity Strategy 2019–2022, https://www.ria.ee/en/publications.html
Estratégia Nacional de Segurança Cibernética (E-Ciber), https://www.gov.br/
EU Cybersecurity Strategy for the Digital Decade (2020), https://digital-strategy.ec.europa.eu/
Executive Order 14028 – Improving the Nation's Cybersecurity (2021), https://www.federalregister. gov/documents/2021/05/17/2021-10460/improving- the-nations-cybersecurity
Federal Information Security Management Act (FISMA), https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma
Federal Law on Personal Data, http://www.consultant.ru/
GDPR (RODO) – Rozporządzenie (UE) 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
Health Information Technology for Economic and Clinical Health Act (HITECH Act), https://www.congress.gov/crs-product/R40161
Health Insurance Portability and Accountability Act of 1996 (HIPAA), https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html
HIPAA – Security Rule, https://www.hhs.gov/hipaa/for-professionals/security/index.html
HITECH Act, https://www.congress.gov/crs-product/R40161
IBM Secure Engineering Framework (Redguide), https://www.ibm.com/redbooks
ISO/IEC 15408 (Common Criteria), https://www.iso.org/standard/50341.html
ISO/IEC 27001, https://www.iso.org/standard/27001.html
ISO/IEC 27002, https://www.iso.org/standard/27002.html
ISO/IEC 27002 (aktualizacja), https://www.iso.org/standard/27002.html
ISO/IEC 27003, https://www.iso.org/standard/27003.html
ISO/IEC 27004, https://www.iso.org/standard/27004.html
ISO/IEC 27005, https://www.iso.org/standard/27005.html
ISO/IEC 27006, https://www.iso.org/standard/27006.html

ISO/IEC 27017, https://www.iso.org/standard/27017.html
ISO/IEC 27018, https://www.iso.org/standard/27018.html
ISO/IEC 27032, https://www.iso.org/standard/27032.html
ISO/IEC 27033, https://www.iso.org/standard/27033.html
ISO/IEC 27034, https://www.iso.org/standard/27034.html
ISO/IEC 27035, https://www.iso.org/standard/27035.html
ISO/IEC 27036, https://www.iso.org/standard/27036.html
ISO/IEC 27037, https://www.iso.org/standard/27037.html
ISO/IEC 27040, https://www.iso.org/standard/27040.html
ISO/IEC 27701, https://www.iso.org/standard/27701.html
ITIL v3, https://www.axelos.com/best-practice-solutions/itil
ITSec, https://www.bsi.bund.de
IT-Sicherheitsgesetz, https://www.bsi.bund.de/
Lei Geral de Proteção de Dados (LGPD), https://www.planalto.gov.br/
Loi de programmation militaire (cyber), https://www.legifrance.gouv.fr/
Loi Informatique et Libertés, https://www.cnil.fr/fr/loi-informatique-et-libertes
Marco Civil da Internet, https://www.planalto.gov.br/
Microsoft Security Development Lifecycle (SDL) – Process Guidance v5, https://learn.microsoft.com/en-us/security/sdl/
Milik P., Pilarski G., Cyberattacks and the bank's liability for unauthorized payment transactions in the online banking system: theory and practice, Cybersecurity and Law - 2023, nr 1(9).
National Cyber Security Strategy 2019–202, https://www.gov.ie/en/publication/national-cyber-security-strategy/
National Cybersecurity Strategy (2023), https://www.cybercom.mil/Portals/56/Documents/Mission%20and%20Vision/National-Cybersecurity-Strategy-2023.pdf
NIST Cybersecurity Framework (CSF), https://www.nist.gov/cyberframework
NIST SP 800-115 – Technical Guide to Information Security Testing, https://csrc.nist.gov/publications/detail/sp/800-115/final
NIST SP 800-171 Rev. 2 – Protecting Controlled Unclassified Information https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
NIST SP 800-207 – Zero Trust Architecture https://csrc.nist.gov/publications/detail/sp/800-207/final
NIST SP 800-30 – Guide for Conducting Risk Assessments https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
NIST SP 800-37 – Guide for Applying the Risk Management Framework https://csrc.nist.gov/ publications/detail/sp/800-37/rev-2/final
NIST SP 800-53 Rev. 5 – Security and Privacy Controls https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
NIST SP 800-61 Rev. 2 – Computer Security Incident Handling Guide https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
NIST SP 800-63-3 – Digital Identity Guidelines https://csrc.nist.gov/publications/detail/sp/800-63/3/final
NIST SP 800-82 Rev. 2 – Guide to Industrial Control Systems Security https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
NIST SP 800-88 Rev. 1 – Guidelines for Media Sanitization https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final
Ok E., Javiera A., Dylan J., Catalina D., The Impact of Cybersecurity Laws on Legal Procedures and Case Law, https://www.researchgate.net/publication/387625093_The_Impact_of_Cybersecurity_Laws_on_Legal_Procedures_and_Case_Law , 2025.
Ogólne Rozporządzenie o Ochronie Danych (GDPR) https://eur-lex.europa.eu/
Oracle Database Security Guide 19c https://docs.oracle.com/en/database/oracle/ oracle-database/19/dbseg/index.html

Oracle Secure Coding Standards https://docs.oracle.com/en/
PCI DSS v4.0.1, https://www.pcisecuritystandards.org/document_library
Pilarski G., Podejście „zero trust" w obszarze bezpieczeństwa informacyjnego, „Rocznik Bezpieczeństwa Morskiego" 2024, vol. XVIII.
Pilarski G., Przegląd współczesnych zagrożeń w cyberprzestrzeni, „Problemy Techniki Uzbrojenia" 2023, T. 167, Nr 5.
Pilarski G., Cybersecurity – choosen aspects, "Wiedza Obronna" 2022, t. 279, nr 2.
Pilarski G., Zawadzki T., Zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, „Wiedza Obronna" 2025, T. 292, Nr 3 (Numer specjalny).
PSD2 (Dyrektywa (UE) 2015/2366), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L2366
PSD2 (Dyrektywa 2015/2366), https://eur-lex.europa.eu/
Public Information Act, https://www.riigiteataja.ee/en/
Rozporządzenie eIDAS (UE 910/2014), https://eur-lex.europa.eu/
Strategia Cyberbezpieczeństwa RP 2019–2024, https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024
Strategia Cyberbezpieczeństwa RP 2025–2029, https://www.gov.pl/web/premier/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2025-2029
Strategia Informatyzacji Państwa do 2035, https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-polski-do-2035-roku
Stratégie nationale pour la sécurité du numérique https://www.ssi.gouv.fr/
UK National Cyber Strategy 2022, https://www.gov.uk/government/publications/national-cyber-strategy-2022
Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne, https://api.sejm.gov.pl/eli/acts/DU/2024/307/text.pdf
Yarovaya Law, http://www.consultant.ru/
Zawadzki T., Comparison of Capabilities of Modern LLM Models in Analyzing and Developing National Security Strategies, "Cybersecurity and Law" 2025, nr 1 (13).
Zawadzki T. et al., Introduction to Methods of Modelling Information Wars as a 21st Century Threat, European Research Studies Journal - 2020, Volume XXIII, Special Issue 2.
Zawadzki T., Wyzwania dla bezpieczeństwa informacyjnego w kontekście rozwoju sztucznej inteligencji, „Rocznik Bezpieczeństwa Morskiego" 2024, vol. XVIII.