

**Cyberbezpieczeństwo w Polsce : od dyskursów do polityk publicznych /
Robert Siudak. – Kraków, 2022**

Spis treści

Wykaz skrótów	8
Wstęp	13
1. Założenia teoretyczne	23
1.1. Pojęcie dyskursu	25
1.2. Procesy społecznego konstruowania problematyki cyberbezpieczeństwa	34
1.2.1. Sekurytyzacja	38
1.2.2. Ryzyfikacja	57
1.2.3. Polityzacja	63
1.2.4. Prywatyzacja	66
1.2.5. Procesy społeczne a framing	69
2. Technologie informacyjno-komunikacyjne a cyberbezpieczeństwo	73
2.1. Technologie informacyjno-komunikacyjne	75
2.1.1. Poziom fizyczny	76
2.1.2. Poziom logiczny	79
2.1.3. Sieciowość	82
2.2. Zagrożenia w cyberprzestrzeni	86
2.2.1. Poziomy cyberprzestrzeni	87
2.2.2. Zagrożenia - poziom fizyczny	93
2.2.3. Zagrożenia - poziom logiczny	97
2.2.4. Zagrożenia - poziom semantyczny	106
2.2.5. Zagrożenia - poziom społeczny	109
2.3. Ofensywne wykorzystanie TIK na arenie stosunków międzynarodowych	113
2.3.1. Problem atrybucji działań w cyberprzestrzeni	114
2.3.2. Wybrane przykłady ofensywnego wykorzystania TIK na arenie międzynarodowej	122
3. Uwarunkowania zewnętrzne dyskursów o cyberbezpieczeństwie w Polsce	151
3.1. Stany Zjednoczone	152
3.2. Unia Europejska	178
3.3. NATO	202
3.4. Organizacja Narodów Zjednoczonych oraz inne fora współpracy międzynarodowej	209
3.5. Izrael	224

4. Uwarunkowania wewnętrzne dyskursów o cyberbezpieczeństwie w Polsce	227
4.1. Ramy prawne i regulacyjne	227
4.1.1. Krajowy system cyberbezpieczeństwa	238
4.2. Główni interesariusze cyberbezpieczeństwa w Polsce	245
4.3. Dynamika zagrożeń i wyzwań - próba analizy	254
4.3.1. Odnotowywane zagrożenia	254
4.3.2. Wyzwania organizacyjno-administracyjne	258
5. Imaginarium cyberbezpieczeństwa	267
5.1. Cyberprzestrzeń	267
5.2. Cyberbezpieczeństwo	276
5.3. Metafory, symbole, obrazy	284
6. Dyskursy o cyberbezpieczeństwie	303
6.1. Dyskursy, ramy, procesy - synteza	303
6.2. Dyskurs technologiczny	309
6.2.1. Rama ITSec (Ti)	311
6.2.2. Rama zarządzanie bezpieczeństwem informacji (T2)	313
6.2.3. Rama bezpieczeństwo sieci i systemów informatycznych (T3)	320
6.3. Dyskurs bezpieczeństwa narodowego	324
6.3.1. Rama bezpieczeństwo cyberprzestrzeni (B4)	328
6.3.2. Rama dezinformacja (B5)	335
6.4. Dyskurs obywatelski	337
6.4.1. Rama bezpieczeństwo w Internecie (O6)	340
6.4.2. Rama ochrona praw i wolności człowieka (O7)	343
6.5. Dyskurs stosunków międzynarodowych	347
6.5.1. Rama globalna cyberprzestrzeń (S8)	348
6.5.2. Rama suwerenność technologiczna (S9)	350
6.6. Dyskurs gospodarczy	352
6.6.1. Rama innowacyjność- konkurencyjność (E10)	354
7. Dyskursy o cyberbezpieczeństwie a polityki publiczne	359
7.1. 1996-2008: zabezpieczenie sieci wewnętrznych i regulacja prawnokarna	359
7.2. 2008-2015: tworzenie pierwszych polityk rządowych i regulacji sektorowych	363
7.3. 2015-2018: tworzenie krajowego systemu cyberbezpieczeństwa	368
7.4. Po roku 2018: rozszerzanie polityk publicznych	372
7.4.1. Wojska Obrony Cyberprzestrzeni i problem dezinformacji	373
7.4.2. Międzynarodowy wymiar polskich działań dotyczących cyberbezpieczeństwa	375
7.4.3. Bezpieczeństwo młodzieży i dzieci w Internecie	376
7.4.4. Innowacyjność - konkurencyjność	377
7.4.5. Ochrona praw człowieka i obywatela	379
7.4.6. Suwerenność technologiczna	380

7.5. Poszerzanie cyberbezpieczeństwa	381
Zakończenie	387
Bibliografia	395
Spis ilustracji	435
Aneks 1. Lista wywiadów badawczych	441
Aneks 2. Lista wydarzeń i konferencji	445
Streszczenie	447
Summary	449
Indeks	451

oprac. BPK