

Agnieszka Bógdał-Brzezińska
Marcin Florian Gawrycki

The background of the cover is a deep purple. It features a large, stylized globe in the center, composed of concentric circles of binary code (0s and 1s). From the top left, several white, arrow-like shapes point towards the center. The overall aesthetic is digital and futuristic.

Cyberterroryzm
i problemy bezpieczeństwa
informacyjnego
we współczesnym świecie

Cyberterroryzm
i problemy bezpieczeństwa
informacyjnego
we współczesnym świecie

Agnieszka Bógdał-Brzezińska
Marcin Florian Gawrycki

Cyberterroryzm
i problemy bezpieczeństwa
informacyjnego
we współczesnym świecie

Warszawa 2003

Projekt okładki:
Barbara Kuropiejska-Przybyszewska

Recenzja naukowa:
Prof. dr hab. Stanisław Koziej

Przygotowanie rozdziałów:
I, VII, VIII, IX, X, XI — Agnieszka Bógdał-Brzezińska
II, III, IV, V, VI — Marcin Florian Gawrycki

Skład i łamanie:
Alex Barnaś — Studio OFI

Redakcja językowa i korekta:
Iwona Gawrycka

© Copyright by Agnieszka Bógdał-Brzezińska
© Copyright by Marcin Florian Gawrycki
© Copyright by Oficyna Wydawnicza ASPRA-JR, 2003
© Copyright by Fundacja Studiów Międzynarodowych

Wydawcy:
Fundacja Studiów Międzynarodowych, Warszawa
tel. (0-22) 553-16-35, fax 553-16-36
www.fundacjasm.edu.pl



Oficyna Wydawnicza ASPRA-JR, Warszawa
tel. 0602 24-73-67, fax (0-22) 613-53-03
e-mail: asprajr@friko.sos.com.pl

ISBN 83-89050-09-9
ISBN 83-88766-59-7

Sprzedaż wysyłkową prowadzi
GŁÓWNA KSIĘGARNIA NAUKOWA IM. B. PRUSA
00-068 Warszawa, ul. Krakowskie Przedmieście 7
tel. (0-22) 826-18-35, fax 827-64-79

Druk i oprawa
DRUKARNIA J.J. Maciejewscy
Przasnysz, ul. Gdańska 1

Spis treści

Wstęp	9
Rozdział I. Wyzwania i zagrożenia współczesnych procesów globalizacji w dobie społeczeństwa informacyjnego	14
1. Globalizacja i jej wpływ na sytuację podmiotów stosunków międzynarodowych	14
2. Tradycyjne rozumienie pojęcia wspólnota. Tożsamość i podmiotowość jednostki a aktywność nowych wspólnot	22
3. Cybernetyzacja współczesnego świata i jej skutki. Cywilizacja informacyjna	26
4. Społeczeństwo informacyjne. Przedmiot badań i definicje	31
5. Nowe media a społeczeństwo informacyjne	36
6. Zmiany w postrzeganiu parametru przestrzeni. Cyberprzestrzeń (cyberspace)	37
7. Pojęcie bezpieczeństwa informacyjnego i jego zagrożenia	40
Rozdział II. Cyberterroryzm – nowe oblicze terroryzmu	44
1. Krótka historia Internetu	44
2. Hakerzy	53
3. Aktywista, hakywista, cyberterrorysta	58
4. Problemy definicyjne	63
Rozdział III. „Cybernetyczne Pearl Harbor”	74
1. Nowa broń masowego rażenia	74
2. Cyberterroryści atakują! – case studies	83
3. Cyberterroryzm – wyzwanie XXI wieku	88
Rozdział IV. Propaganda i komunikacja	92
1. Wild West World	92
2. CyberZapatyści – case study	95
3. Internet – propaganda i komunikacja	107
3.1 Propaganda	109
3.2 Komunikacja	115
3.3 Echelon i Carnivore	121
Rozdział V. Atak cyberterrorystyczny	130
1. The Great Cyberwar of 2002	130
2. Wybór celów	134
3. Dwa rodzaje ataków cyberterrorystycznych	138
4. Klasyfikacja ataków	141
5. Wybrane metody ataków cyberterrorystycznych	144

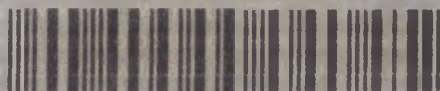
5.1 Najprostszy atak	144
5.2 Wirusy, robaki, bakterie	145
5.3 Bomba logiczna	148
5.4 Koń trojański	149
5.5 Chipping	150
5.6 Tylne drzwi	150
5.7 Spoofing	151
5.8 Hijacking	151
5.9 Sniffing	152
5.10 Receptory van Ecka	152
5.11 Denial of service (DoS) i distributed denial of service (DDoS)	153
5.12 E-mail bombing	154
5.13 Broń o częstotliwości radiowej	155
5.14 Inżynieria społeczna	158
6. Szacowanie strat	158
Rozdział VI. Wojny internetowe	164
1. Definicja wojny internetowej	164
2. Wojna w Kosowie	165
3. Konflikt indyjsko-pakistański	169
4. Konflikt chińsko-tajwański	170
5. Konflikt izraelsko-arabski	172
6. Konflikt chińsko-amerykański	174
Rozdział VII. Stany Zjednoczone – światowy lider w dziedzinie bezpieczeństwa informacyjnego	178
1. Uwarunkowania polityki bezpieczeństwa informacyjnego USA	178
2. Zasady i kierunki bezpieczeństwa informacyjnego USA.	
Rola ochrony infrastruktury krytycznej	181
3. Zarys amerykańskich regulacji prawnych w sprawach bezpieczeństwa informacyjnego i zwalczania cyberterroryzmu	187
3.1 Inicjatywy i projekty rządowe	187
3.2 Działalność legislacyjna Kongresu	190
4. Instytucjonalizacja bezpieczeństwa informacyjnego USA	191
5. Zagadnienia kooperacji i zagrożeń międzynarodowych	195
6. Podsumowanie	197
Rozdział VIII. Bezpieczeństwo informacyjne Federacji Rosyjskiej	200
1. Źródła rosyjskiej polityki bezpieczeństwa informacyjnego	200
2. Wskaźniki rozwoju ICT w Federacji Rosyjskiej	201
3. Ewolucja i rola Internetu w Federacji Rosyjskiej	202
4. Podstawy ochrony prawnej Internetu w Federacji Rosyjskiej	203
5. Tendencje rozwoju Internetu w Rosji	204
6. E-Russia jako implementacja koncepcji społeczeństwa informacyjnego	206
7. Doktryna bezpieczeństwa informacyjnego FR	208
8. Walka informacyjna i monitoring informacji w Federacji Rosyjskiej	212
9. Podsumowanie	215

Rozdział IX. Globalne i europejskie rozwiązania w zakresie społeczeństwa informacyjnego i w dziedzinie ICT	216
1. Debata na temat cyberprzestępczości.	
Początki rozwiązań legislacyjnych	216
2. Bezpieczeństwo informacyjne w debatach i regulacjach wybranych organizacji międzynarodowych	219
2.1 ONZ wobec dyskusji o rozwoju ICT i jego zagrożeniach	219
2.2 OECD – główne obszary zainteresowania bezpieczeństwem informacyjnym	222
2.3 Grupa G-7/G-8, COCOM – instytucje współpracy państw wysoko rozwiniętych wobec bezpieczeństwa informacyjnego	225
3. Rozwiązania europejskie i transatlantyckie w sektorze ICT	227
3.1 Unia Europejska – społeczeństwo informacyjne i regulacje bezpieczeństwa informacyjnego	227
3.1.1 Uwarunkowania rozwoju ICT w Unii Europejskiej	227
3.1.2 Programy rozwoju społeczeństwa informacyjnego w regulacjach UE	229
3.1.3 Inicjatywa eEurope	231
3.1.4 Regulacje dotyczące rozwoju sieci informacyjnych w Unii Europejskiej	234
3.1.5 Regulacje prawne związane z ochroną kluczowych obszarów zastosowania ICT w Unii Europejskiej	235
3.1.6 Ogólne regulacje w zakresie bezpieczeństwa informacyjnego w Unii Europejskiej	237
3.1.7 Programy operacyjne ICT w Unii Europejskiej	240
3.2 Działalność Rady Europy w sprawie cyberprzestępczości	243
3.3. Cyberterroryzm w polityce bezpieczeństwa NATO	245
4. Podsumowanie	246
Rozdział X. Społeczeństwo informacyjne i bezpieczeństwo informacji w krajach Azji, Australii i Oceanii, Afryki i Ameryki Łacińskiej	248
1. Status Internetu w krajach Azji	248
2. Azja Południowa jako obszar działań cyberterrorystycznych	249
3. Polityka bezpieczeństwa informacyjnego wybranych krajów regionu Azji i Pacyfiku	252
3.1 Chińska Republika Ludowa – cyber rogue power	252
3.2 Korea Południowa – kraj tranzytu cyberataków	255
3.3 Australia i Nowa Zelandia – antypody cyberzagrożeń	256
3.4 Japonia – świadomość zagrożeń i wyzwań	260
3.4.1 Cyberentuzjaści i cyberkrytycy	262
3.4.2 Instytucjonalizacja japońskiej polityki bezpieczeństwa informacyjnego	265
4. Współpraca krajów APEC na rzecz pogłębienia bezpieczeństwa informacyjnego	266
5. Bezpieczeństwo informacyjne w Ameryce Łacińskiej	269
6. Świadomość zagrożeń bezpieczeństwa informacyjnego w krajach Afryki	272
7. Podsumowanie	278

Rozdział XI. Bezpieczeństwo informacyjne Polski	280
1. Determinanty rozwoju sektora ICT w Polsce	280
2. Raporty i oceny rozwoju polskiego ICT	281
3. Strategia ePolska 2001–2006	288
4. Zmiany legislacyjne związane z rozwojem ICT i zagrożeniami bezpieczeństwa informacyjnego	291
4.1 Odpowiedzialność karna za przestępstwa cybernetyczne w prawie polskim	292
4.2 Ustawa o podpisie elektronicznym	293
4.3 Ustawa o ochronie danych osobowych	296
5. Bezpieczeństwo informacyjne w Polsce: strategie i instytucje	298
6. Podsumowanie	302
Zakończenie	304
Ilustracje	312
Aneks I. Słownik wybranych pojęć	322
Aneks 2. Wybrane linki stron internetowych	340
Bibliografia	346

Biblioteka Główna
Akademii Obrony Narodowej

Agnieszka Bógdał-Brzezinska 8811/P



06-008811-004-0

Agnieszka Bógdał-Brzezinska, dr hab. nauk humanistycznych, specjalizacja polityki Stanów Zjednoczonych. Jej zainteresowania naukowe dotyczą teorii stosunków międzynarodowych i teorii stosunków informacyjnego współczesnych państw i organizacji międzynarodowych.

Czyt.

004.056

Marcin Florian Gawrycki ukończył studia w Instytucie Studiów Międzynarodowych Uniwersytetu Warszawskiego (2000), a ponadto — w Center for Latin American Studies (2000) i Studium Bezpieczeństwa Narodowego (2001). Jest doktorantem w ISM UW. Jego zainteresowania badawcze dotyczą problematyki latynoamerykańskiej (historia stosunków międzynarodowych w Ameryce Łacińskiej, polityka zagraniczna Kuby, historia Kolumbii, polityka USA wobec państw Ameryki Łacińskiej, *guerrilla* latynoamerykańska), cyberterroryzmu i bezpieczeństwa informacyjnego.

Autorzy podjęli, pionierski jak na polskie warunki, trud ukazania wielu różnorodnych aspektów problematyki bezpieczeństwa informacyjnego. (...) Zajmują się pojęciem cyberterroryzmu, jego istotą i treścią, oraz współcześnie możliwymi rodzajami i metodami ataków cyberterrorystycznych, a także przywołują konkretne przykłady wojen internetowych. (...) W związku z pracami nad nową strategią bezpieczeństwa narodowego i, w konsekwencji, niewątpliwym wzrostem zapotrzebowania w Polsce na wiedzę o zagrożeniach, koncepcjach i systemach bezpieczeństwa informacyjnego, można oceniać, że niniejsza publikacja ma duże szanse stać się książką poszukiwaną przez wszystkich, którzy interesują się sprawami szeroko rozumianego bezpieczeństwa państwa.

Prof. dr hab. Stanisław Koziej
(Z recenzji)

ISBN 83-89050-09-9
ISBN 83-88766-59-7

39.90