

BOGUSŁAW PACEK  
ROMUALD HOFFMANN

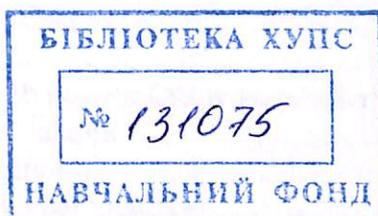
**Działania  
sił zbrojnych  
w cyberprzestrzeni**

355  
P24

AKADEMIA OBRONY NARODOWEJ

BOGUSŁAW PACEK  
ROMUALD HOFFMANN

**Działania  
sił zbrojnych  
w cyberprzestrzeni**



Warszawa 2013

**Recenzenci**

dr hab. Dariusz S. Kozerański

dr hab. Jeremiasz Ślipiec

**Adiustacja stylistyczna**

Renata Czerwińska

**Projekt okładki**

Dariusz Łysio

**Skład komputerowy**

Małgorzata Gawłowska

**Korekta**

Małgorzata Sęktas

© Copyright by Akademia Obrony Narodowej, Warszawa 2013

ISBN 978-83-7523-270-7

Sygn. AON 6162/13

Skład, druk i oprawa: Wydawnictwo Akademii Obrony Narodowej  
00-910 Warszawa, al. gen. A. Chruściela 103, tel: 681-40-55, tel./faks 681-37-52  
e-mail: wydawnictwo@aon.edu.pl  
Zam. nr 505/2013

# Spis treści

Wstęp .....	7
1. Zagrożenia bezpieczeństwa w XXI wieku .....	9
1.1. Informacja, jako determinant działań sił zbrojnych .....	71
1.2. Podejście sieciocentryczne .....	73
2. Bezpieczeństwo w cyberprzestrzeni .....	81
2.1. Rys historyczny .....	81
2.2. Czym jest bezpieczeństwo cyberprzestrzeni? .....	84
3. Bezpieczeństwo cyberprzestrzeni w wybranych krajach .....	87
3.1. USA .....	87
3.2. Kanada .....	88
3.3. Australia .....	88
3.4. Niemcy .....	89
3.5. Chiny .....	90
3.6. Korea Północna .....	90
3.7. Izrael .....	91
3.8. Rosja .....	91
4. Działania zmierzające do ochrony cyberprzestrzeni na szczeblu rządowym .....	92
4.1. Rys historyczny .....	92
4.2. Stan oczekiwany .....	95
4.3. Rola i miejsce służb resortu ON w systemie rządowym .....	96
4.4. Dotychczasowe działania .....	97
4.4.1. Rozwój zdolności .....	104
4.4.2. Ćwiczenia Cyber Defence .....	105
4.4.3. Działalność szkoleniowa .....	106
4.4.4. Implementacja i wdrożenia .....	107

5. Struktury organów bezpieczeństwa teleinformatycznego w Polsce .....	108
5.1. Rys historyczny .....	108
5.2. Stan obecny .....	108
5.3. Stan docelowy .....	109
6. Rola i miejsce organów bezpieczeństwa teleinformatycznego w układzie sojuszniczym .....	110
6.1. Rys historyczny .....	110
6.2. Stan obecny .....	110
6.2.1. NATO .....	110
6.2.2. MoU z USA .....	111
6.2.3. Współpraca z MICROSOFT .....	112
6.2.4. Centrum Doskonalenia Obrony Cybernetycznej NATO .....	112
6.3. Stan oczekiwany .....	113
7. Działania aktywne w cyberprzestrzeni .....	115
7.1. Rys historyczny .....	115
7.2. Stan aktualny .....	115
7.3. Stan proponowany .....	116
7.4. Uwarunkowania prawne .....	117
7.5. Działania na teatrze .....	117
7.6. Działania przygotowawcze, technologiczne, edukacyjne i szkoleniowe .....	118
7.7. Jak zbudować wojskowy zespół reagowania na incydenty komputerowe? .....	118
Wnioski .....	121
Bibliografia .....	123