

Spis treści

Przedmowa	9
O autorze	13
O recenzencie	14
Wprowadzenie	15
Rozdział 1. Krótka historia zagrożeń cybernetycznych i pojawienie się APT	19
Hakerzy nie są tacy, jak pokazuje nam Hollywood	19
Bitwa na więzki	22
Hakowanie z użyciem modemów	22
Rozwój oprogramowania antywirusowego	23
Początki zagrożeń APT	24
Wczesne ataki APT	28
Zamieszanie w cyberbronie	30
Amerykańskie i sojusznicze agencje do spraw bezpieczeństwa cybernetycznego	30
Atak cybernetyczny słyszany na całym świecie	31
Cyfrowa wojna oko za oko	34
Puszka Pandory zostaje otwarta	35
Podsumowanie	37
Źródła	38
Rozdział 2. Perymetr sieciowy odchodzi do lamusa...	39
Scenariusz, który ilustruje luki w modelu opartym na perymetrze sieciowym	40
Upadek perymetrów globalnych	41
Perymetr sieciowy nie sprawdza się nawet w organizacjach spełniających wymogi bezpieczeństwa	44
Perymetry systemów rządowych też zawodzą	46

Użytkownicy, BYOD i całkowity zanik perymetru sieciowego	48
Aplikacje zwiększają poziom zagrożenia	51
Niepowodzenia metod uwierzytelniania	52
Urządzenia IoT robią dziury w każdym perymetrze	56
Nie możesz naprawić głupoty ani złośliwości	57
Podsumowanie	61
Źródła	62
Rozdział 3. Nowe taktyki i trendy — co nas czeka w niedalekiej przyszłości?	65
Ataki zmieniają kierunek	66
Pojazdy autonomiczne... Niepoprawne dane, pechowy dzień	68
Drony... Śmierć nadchodzi z nieba	72
Napastnicy integrują działania i taktykę w celu optymalizacji skuteczności ataków	78
Ransomware wchodzi na platformy mobilne	82
Ataki DDoS osiągają poziom broni	85
Podsumowanie	87
Źródła	88
Rozdział 4. Ataki z wywieraniem wpływu — wykorzystywanie mediów społecznościowych do złośliwych celów	89
Nowy atak cybernetyczny	90
Cyfrowe pole bitwy ulega zmianom	91
Tylko #hashtag czy już amunicja?	92
Wywieranie wpływu na osoby wpływowe	99
Podsumowanie	104
Źródła	104
Rozdział 5. DeepFakes, uczenie maszynowe i sztuczna inteligencja w cyberprzestrzeni	105
Z dużego ekranu na smartfony — narodziny DeepFakes	106
Czym są DeepFakes?	106
Sieci GAN napędzają DeepFakes	107
DeepFakes w praktyce, czyli DeepMastersPrints	112
Podrabianie głosu za pomocą uczenia maszynowego — technologia DeepVoice	116
ReadFakes	119
Wiadomości z ostatniej chwili mogą być źródłem problemów	122
Kiedy „badania” danych i sztucznej inteligencji idą na marne	123
Podsumowanie	126
Źródła	127
Rozdział 6. Zaawansowane działania w wojnie cybernetycznej	129
Kampanie wojny cybernetycznej	130
Kampania ataków na indyjskie elektrownie jądrowe	131
Chińska kampania „transferu technologii”	133
Kampania ingerowania w przebieg wyborów w USA i Libii	135

Operacje pod fałszywą flagą mylą tropy w cyberprzestrzeni	137
Klasyfikacja etapów ataków cybernetycznych	138
Grupy hakerów celowo unikają rozgłosu	144
Kampanie cyberataków w nadchodzącej dekadzie	147
Fałszerstwa	148
Podsumowanie	152
 Rozdział 7. Planowanie strategiczne dla przyszłych działań w wojnie cybernetycznej	 155
Każdy ma plan, dopóki nie zostanie w zęby	156
Jaka strategia?	157
Kiedy charakter konfliktu wymaga zmiany strategii	158
Infiltracja nie jest równoznaczna z dominacją	159
Liderzy również muszą umieć „pobrudzić sobie ręce”	161
To środowisko, a nie sprzęt, decyduje o tym, co działa, a co nie	161
Gromadzenie informacji i wywiad to nie zawsze jedno i to samo	163
Zbyt wiele to czasem naprawdę zbyt wiele	165
Wielkie mury mogą powodować wielkie problemy	166
Misja nie została zrealizowana...	168
Jak wygląda skuteczna strategia w cyberprzestrzeni?	172
Zmiana koncepcji strategicznych	173
Strategiczna obrona „granic”	174
Małymi krokami do przodu	176
Orkiestracja umożliwia realizację strategii	178
Podsumowanie	179
 Rozdział 8. Innowacje strategiczne i mnożniki siły w cyberprzestrzeni	 181
Narzędzia obronne i czynniki strategiczne	182
Poznaj Małpę	182
Co jeszcze potrafi Infection Monkey?	185
Zaawansowane możliwości pakietu Infection Monkey	187
Perymetr definiowany programowo	189
Białe listy aplikacji	194
Narzędzia ofensywne i czynniki strategiczne	197
Po co nam hasła?	197
Pakiet WhatBreach	198
Pakiet SNAP_R	202
Fałszywe komentarze w celu wywierania wpływu	203
Podsumowanie	205
Źródła	205
 Rozdział 9. Przygotowanie do uderzenia	 207
Wyłączenie odpowiedzialności	208
Mikrosegmentacja jest kluczem do przetrwania	208
Czym jest mikrosegmentacja?	208
Narzędzia i technologie mikrosegmentacji	211

Pragmatyczne zastosowanie sieci SDN	212
Możliwe pułapki w mikrosegmentacji	213
Odzyskanie „wzgórza”	215
Hasła z wozu, koniom lżej	218
Zbieranie informacji	224
Podsumowanie	228
Źródła	229
 Rozdział 10. Zdolność przetrwania w wojnie cybernetycznej i potencjalne skutki ataków	 231
Po co komu prawa w czasie wojny?	232
Reguła 1. — „Domyślny” oznacza „martwy”	233
Reguła 2. — Myśl strategicznie, działaj taktycznie	237
Reguła 3. — Szczegóły, szczegóły	239
Reguła 4. — Pozbądź się haseł	241
Reguła 5. — Ogranicz promień rażenia	244
Wpływ porażki	248
Ataki na system opieki zdrowotnej	248
Ataki na systemy ICS (przemysłowe systemy sterowania)	249
Zagrożenie dla losu całych narodów	249
Podsumowanie	252
 Dodatek. Poważne incydenty cybernetyczne wykryte lub ujawnione w 2019 roku	 253