

Spis treści

Wstęp	13
Rozdział 1. Wprowadzenie do filozofii cyberbezpieczeństwa	17
1.1. Krótko o historii	17
1.1.1. Historia wirusów i złośliwego oprogramowania	17
1.1.2. Grupy zainteresowań, grupy hakerskie	18
1.1.3. Dlaczego cyberbezpieczeństwo stało się ważne?	19
1.2. Stopniowy wzrost roli i wagi cyberbezpieczeństwa	21
1.3. Wymiar międzynarodowy i wojskowy	23
1.4. Czym jest filozofia cyberbezpieczeństwa – jak ją rozumieć?	24
1.5. Czy cyberbezpieczeństwo jest osiągalne?	25
1.5.1. Poufność, integralność, dostępność	25
1.5.2. Dla zwykłego użytkownika	25
1.5.3. Użycie biznesowe	25
1.5.4. Państwo	26
1.5.5. Problem światowy	27
1.6. Ważne pytania i pewien mit	27
1.7. Czy cyberbezpieczeństwo jest w ogóle osiągalne?	29
Rozdział 2. Cyberzagrożenia i konieczne wyjaśnienia	30
2.1. Ryzyko	30
2.2. Różne rodzaje ryzyka	32
2.2.1. Sztuczna inteligencja	32
2.2.2. Prawa człowieka	33
2.3. Krótko o cyberataku	33
2.4. Kill chain – użyteczny model myślowy	34
2.4.1. Rozpoznanie	34
2.4.2. Uzbrojenie	34
2.4.3. Dostarczenie	35
2.4.4. Eksploatacja	35
2.4.5. Instalacja	35
2.4.6. Dowodzenie i zarządzanie	35
2.4.7. Realizacja celów	36
2.4.8. Kill chain – podsumowanie	36
2.5. Model MITRE	37
2.6. Socjotechnika i phishing	39
2.7. Grupy zagrożeń	40
2.7.1. Haktywiści	41
2.7.2. Cyberprzestępcy	41
2.7.3. Grupy rządowe, APT	41
2.7.4. Grupy – synteza	42
2.8. Cybernarzędzia czy cyberbroń?	43
2.8.1. Rodzaje narzędzi – kwestia celów	43
2.8.2. Exploit	44

2.9. CVE i branding błędów bezpieczeństwa	45
2.9.1. 20-letnie błędy w zabezpieczeniach?	47
2.9.2. Ekonomia błędów bezpieczeństwa i exploitów	48
2.9.3. Frameworki i inne narzędzia	48
2.10. Ransomware	49
2.10.1. Utrata danych i okup	49
2.10.2. Model biznesowy – celem są pieniądze	50
2.10.3. Jak się zabezpieczyć – zasada 3-2-1	50
2.10.4. Problem geopolityczny i prawny – korsarstwo XXI w.?	51

Rozdział 3. Cyberbezpieczeństwo od strony użytkownika 53

3.1. Cyberbezpieczeństwo jako problem zwykłych ludzi	53
3.1.1. Cyfryzacja postępuje i co z tego wynika	53
3.1.2. Czy sami budujemy zależności?	54
3.1.3. Pożar centrum danych – co za pech!	54
3.2. Trzeba się zabezpieczyć – czy to możliwe i jak to zrobić?	55
3.2.1. Problemy także dla ekspertów	56
3.2.2. Zabezpieczenie to zwiększenie kosztów dla atakujących	56
3.2.3. Zwracaj uwagę na to, co ma znaczenie	57
3.2.4. Modelowanie ryzyka	57
3.2.5. Jakie są faktyczne zagrożenia dla nas?	58
3.3. Żelazne zasady	59
3.3.1. Technologia jest dla ludzi	59
3.3.2. Dostawcy powinni dbać o podstawowe zabezpieczenia – waga ekosystemów	59
3.3.3. Powierzchnia ryzyka	60
3.3.3.1. Mapowanie sposobów korzystania	61
3.3.3.2. Identyfikacja punktów ryzyka i dobór rozwiązań	61
3.3.3.3. Wymogi prawne na pomoc?	62
3.3.4. Mieć aktualne oprogramowanie	62
3.3.5. Zasada ograniczonego zaufania wobec tego, co jest na ekranie	63
3.3.6. Weryfikacja komunikacji	64
3.3.7. Hasła	64
3.3.7.1. Dobre hasła	64
3.3.7.2. Łamanie nie jest takie proste!	66
3.3.7.3. Nie zmieniamy dobrych haseł (chyba że są dobre ku temu powody)	66
3.3.7.4. Dobre hasła to długie hasła	68
3.3.7.5. Diceware	68
3.3.8. Przechowywanie haseł	69
3.3.9. Uwierzytelnianie dwu- bądź wieloskładnikowe	70
3.3.10. Paranoja	71
3.3.11. Aktualna wiedza	72
3.3.12. Przeglądarki internetowe	73
3.3.13. Różne ryzyka do różnych „szufladek”	74
3.3.14. Bezpieczny e-mail	74
3.3.14.1. Webmail	74
3.3.14.2. Duże jest bezpieczniejsze?	75
3.3.15. Komunikatory	76
3.3.16. Media społecznościowe	77
3.3.17. Czy potrzebujemy VPN? Pewnie nie	78
3.3.18. Pamiętaj, że model zagrożeń zależy od tego, kim jesteś i czym się zajmujesz	79

3.4. Czy zawsze nam coś grozi i ktoś chce nas zhakować?	80
3.4.1. Nie wszystkie zagrożenia są techniczne	80
3.4.2. Na niektóre problemy możemy nie mieć wpływu	81
3.5. Oprogramowanie antywirusowe	81
3.6. Prywatność użytkownika – szeroki temat	82
3.6.1. Ustawienia	83
3.6.2. Nie tylko źli ludzie mają coś do ukrycia	83
3.6.3. Smartfon – centrum życia	84
3.6.4. Co o nas wiedzą?	84
3.6.5. Prywatność jako cecha produktu i przewaga biznesowa	85
3.6.6. Prywatność a technologie i standardy	85
Rozdział 4. Cyberbezpieczeństwo infrastruktury zdrowia	86
4.1. Cyfryzacja ochrony zdrowia postępuje	86
4.1.1. Cyfryzacja i problemy?	87
4.1.2. Cyfryzacja danych medycznych w Polsce	87
4.1.3. COVID-19 jako akcelerator cyfryzacji	88
4.2. Cyfryzacja a ryzyka dla cyberbezpieczeństwa	89
4.3. Ryzyka i zagrożenia	89
4.3.1. Cyberataki na szpitale	90
4.3.2. Ransomware WannaCry jako motor nakładów finansowych na cyberbezpieczeństwo?	90
4.3.3. Cyberataki na opiekę zdrowotną w Irlandii	91
4.3.4. Inne cyberataki na ośrodki zdrowia	92
4.3.5. Czy ubezpieczyciel pokryje straty?	92
4.3.6. Czy cyberubezpieczenia mają sens?	93
4.3.7. Priorytetem szpitali nie jest cyberbezpieczeństwo	94
4.4. Cyfryzacja diagnostyki medycznej i nowe podatności	95
4.4.1. Ryzyko implantów	95
4.4.2. Wycieki danych, a może modyfikacja diagnostyki	96
4.4.3. Cyberataki w łańcuchu dostaw	96
4.5. Cyberbezpieczeństwo urządzeń medycznych	96
4.6. Jak zabezpieczyć szpital?	98
4.6.1. Sprzęt, oprogramowanie, licencje, aktualizacje	98
4.6.2. Co w razie dużej skali cyberataku? Scenariusz cyberataku systemowego	98
4.7. Skutki śmiertelne	99
4.7.1. Zły projekt – system Therac-25	100
4.7.2. W pogoni za sensacją?	100
4.7.3. Ostrożnie z doniesieniami?	101
4.7.4. Po co zabijać cyberatakiem?	102
4.7.5. Czy łatwo wykryć śmierć z powodu cyberataku?	102
4.8. No dobrze, ale czy cyberatakiem można zabić?	103
4.8.1. Scenariusz cyberataku z efektami śmiertelnymi – czy taką bombę logiczną się wykryje?	103
4.8.2. Skoordynowane wyczerpywanie baterii implantów? Scenariusz	104
Rozdział 5. Cyberbezpieczeństwo infrastruktury krytycznej	105
5.1. Wrażliwa część państwa	105
5.2. Przykłady cyberataków na infrastrukturę krytyczną	106
5.2.1. Energetyka	106
5.2.1.1. Elektrownie jądrowe	107
5.2.1.2. Cyberataki na dystrybucję energii na Ukrainie	108
5.2.1.3. Co się dzieje po wyłączeniu prądu?	108

5.2.1.4.	Próba wyłączenia prądu w warunkach wojny?	109
5.2.1.5.	Jak się zabezpieczyć?	109
5.2.1.6.	Blackout cyberatakiem? Scenariusze	110
5.2.2.	Scenariusz: fizyczne niszczenie transformatora	110
5.2.2.1.	Praktyczna demonstracja zniszczeń fizycznych	112
5.2.2.2.	Sceptycyzm wobec doniesień zalecany	112
5.2.3.	Systemy uzdatniania wody	113
5.2.4.	Gaz, ropa	114
5.3.	Zabezpieczanie infrastruktury krytycznej	114
5.4.	Hakowanie elementów fizycznych	115
5.5.	Efekty fizyczne	116
5.5.1.	Stuxnet	117
5.5.2.	Niemiecka huta stali	117
5.6.	Systemy transportowe	118
5.7.	Co na to państwa?	119
5.8.	Kluczowa kwestia cywilizacyjna	120
Rozdział 6. Cyberbezpieczeństwo państwa		121
6.1.	Czym jest cyberbezpieczeństwo państwa?	121
6.2.	Państwa były już hakowane	122
6.2.1.	Cyberoperacje wymierzone w system polityczny w USA	122
6.2.2.	Wybory, wywiad i ludzka natura	122
6.2.3.	Celowe wycieki danych i ich efekty	123
6.2.4.	Cyberoperacje wymierzone w system polityczny we Francji	123
6.2.5.	Incydenty w Polsce	124
6.2.6.	Cyberoperacje profesjonalne	124
6.2.7.	Cyberatak na KNF w Polsce	125
6.2.8.	Przypadek Tajwanu – działania informacyjne i człowiek znikąd	126
6.2.9.	Ataki w innych miejscach	126
6.3.	Głosowanie elektroniczne jako systemowy punkt słabości państwa	126
6.3.1.	Kwestie przejrzystości	127
6.3.2.	Ostrożnie z cyfryzacją	127
6.4.	Ogólny scenariusz	128
6.5.	Jak zabezpieczają się państwa?	129
6.5.1.	RODO, NIS – kiedy warto lub trzeba działać?	129
6.5.2.	KSC, CERT-y, inne instytucje	129
6.6.	Czy można zabezpieczyć państwo?	130
6.6.1.	Wybory	130
6.6.2.	Partie polityczne	130
6.6.3.	Cyberbezpieczeństwo sztabu wyborczego – wyzwanie	131
6.6.3.1.	Kwestia osobowa	132
6.6.3.2.	Strategia cyberbezpieczeństwa sztabu	132
6.6.3.3.	Znów o czynniku ludzkim	132
6.6.3.4.	Środki techniczne, chmurowe	133
6.6.3.5.	Rutynowe usuwanie danych	133
6.6.4.	Cyberbezpieczeństwo jako problem PR	134
6.7.	Konieczność strategii cyberbezpieczeństwa państwa	134
6.8.	A może odłączyć się od internetu?	135

Rozdział 7. Cyberkonflikt, cyberwojna	137
7.1. Rywalizacja państw	137
7.2. Cyberwywiad	138
7.3. Cyberpolicja	138
7.4. Cyberwojska	138
7.4.1. Standardowe narzędzia państw	139
7.4.2. Cyberatak to nie atak	139
7.4.3. Cyberoperacje	140
7.4.3.1. Cyberoperacje obronne	140
7.4.3.2. Operacje ISR	141
7.4.3.3. Operacje ofensywne	141
7.4.4. Proporcje w odniesieniu do różnych operacji	142
7.5. Cyberzdolności	142
7.5.1. Efekty fizyczne	142
7.5.2. Efekty zakłócające	143
7.5.3. Odmowa usługi, blokowanie	143
7.5.4. Pozyskiwanie informacji, zbieranie danych	144
7.5.5. Sygnalizowanie	144
7.5.6. Dostarczanie	144
7.5.6.1. Cyberoperacja z bliskim dostępem w Rotterdamie?	145
7.5.6.2. Przekupywanie pracowników	145
7.6. Czym jest cyberwojna?	146
7.6.1. Wojna ograniczona do cyberataków?	146
7.6.2. Cyberataki towarzyszące innym działaniom zbrojnym?	147
7.6.3. Cyberwojna w Polsce?	148
7.7. Działania cyberofensywne	149
7.7.1. Cyberoperacje fizyczne	149
7.7.2. Czy można zabić za pomocą cyberataku? Ujęcie operacyjno-wojskowe	149
7.7.3. Targeting – czy cyberataki mogą celować w konkretne cele, ludzi?	150
7.8. Cyberbezpieczeństwo systemów uzbrojenia	151
7.8.1. Do czego to prowadzi?	152
7.8.2. Dobre wieści?	152
7.9. Czy można odpowiedzieć zbrojnie na cyberatak?	153
7.9.1. Artykuł 51 KNZ	154
7.9.2. Atrybucja	155
7.9.3. Poziomy atrybucji	156
7.9.4. Praktyka państwowa	157
7.9.5. Po co wskazywać?	157
7.10. Czy w ramach cyberwojny obowiązywałyby jakieś zasady?	158
7.10.1. Pomysły na wykorzystanie nowych technologii i uchronienie się przed zagrożeniem	158
7.10.2. Prawo wojny	159
7.10.3. Scenariusz cyberataku wywołującego zatrucie gazem	160
7.11. Środki do cyberataku – cyberbroń	160
7.11.1. Narzędzia	161
7.11.2. Metody	161
7.11.3. Podwójne przeznaczenie	162
7.12. Skąd brać cyberzdolności?	162
7.12.1. Budowa	163
7.12.2. Zakup	163

7.13. Cyberodstraszenie. Narzędzie projekcji siły	164
7.13.1. Cyberdestabilizacja?	165
7.13.2. Eskalacja	166
7.13.3. Drabina eskalacyjna	167
7.14. Ryzyko eskalacji	170
7.15. Jak przygotowują się państwa?	171
7.15.1. Co nam grozi?	172
7.15.2. Ryzyko eskalacji i wojny	172
7.15.3. Cyberataki integralnym elementem działań bojowych, zaczepnych, wojskowych	173
7.15.4. Czy można wspomóc stabilizację?	173
7.15.5. Normy	174
7.16. Cyber a sprawa polska	175
7.16.1. Zagrożenia i ich realność	176
7.16.2. Cyberoperacje w zdobywaniu informacji wywiadowczych	176
7.16.3. Czy warto dawać środki na wojsko?	177
7.16.4. Separacja cyberjednostek jest konieczna	177
7.16.5. Czy Polska potrzebuje zdolności ofensywnych?	177
7.16.6. Specyfika problemu – kto zechce to zrozumieć?	178
7.16.7. Czego uczy nas kardynał Richelieu o cyberbezpieczeństwie?	178
7.16.8. Zagrożenia z powodu posiadania cyberzdolności?	179
7.16.8.1. Ryzyko nadużyć wewnętrznych	179
7.16.8.2. Zagrożenie zewnętrzne	180
7.17. Cyberwojna na Ukrainie w 2022 r.	181
7.17.1. Sytuacja przed konfliktem zbrojnym	181
7.17.2. Sytuacja w trakcie konfliktu zbrojnego	183
7.17.2.1. Brak cyberapokalipsy	184
7.17.2.2. W działaniu jednostki różnych państw	185
7.17.2.3. Jednostki nieoficjalne, amatorskie	185
7.17.2.4. Ryzyko rozlania się cyberkonfliktu na inne kraje	185
Zakończenie	186
O autorach	187