

Spis treści

O autorce	15
Podziękowania	17
Przedmowa	19
Słowo wstępne	21
Wprowadzenie	25
Część I. Podstawy OSINT	27
Rozdział 1. OSINT —biały wywiad	29
1.1. Czym jest OSINT?	29
1.2. Krótka historia białego wywiadu (OSINT)	32
Przeszłość	33
Teraźniejszość	34
Przyszłość	36
1.3. Myślenie krytyczne	40
1.4. Zdrowie psychiczne	42
1.5. Osobista tendencyjność	43
1.6. Etyka	45
Rozdział 2. Cykl wywiadowczy	48
2.1. Czym jest cykl wywiadowczy?	48
2.2. Faza planowania i wymagań	49
2.3. Faza gromadzenia	51
Sztuka piwotowania	52
Pokonywanie wyzwań związanych z OSINT	57
Technika RESET	57
Analiza luk	58
Dlaczego mamy tak dużo danych	61
2.4. Metody dokumentacji	63
2.5. Faza przetwarzania i oceny	68
Ustalanie zakresu	69
Wzbogacanie danych	69
2.6. Faza analizy i produkcji	70
Wizualizacje	71
2.7. Raportowanie	73
Ton raportu	75

Projekt raportu	75
Przykładowa sprawa	77
Przykładowy raport	78
2.8. Fazy rozpowszechniania i konsumpcji	79
Podpowiedzi	79
Faza informacji zwrotnej	79
Wyzwania w cyklu wywiadowczym	79
Rozdział 3. Myśl tak jak przeciwnik	81
3.1. Poznaj swojego przeciwnika	81
3.2. Rozpoznanie pasywne kontra aktywne	88
Rozdział 4. Bezpieczeństwo operacyjne	90
4.1. Czym jest bezpieczeństwo operacyjne (OPSEC)?	90
Modelowanie zagrożeń	91
Metoda persona non grata	91
Karty bezpieczeństwa lub karty „profilowe”	92
Drzewa ataków	94
4.2. Kroki strategii OPSEC 95 Pięć kroków OPSEC w zarysie	96
Krok 1. Zdefiniuj informacje krytyczne	96
Krok 2. Przeanalizuj zagrożenia	96
Krok 3. Określ swoje podatności	96
Krok 4. Oceń ryzyko	96
Krok 5. Zastosuj środki zaradcze	97
4.3. Technologia OPSEC	100
Wirtualna sieć prywatna	100
Dlaczego warto korzystać z VPN?	101
Wybór sieci VPN	101
Obawy związane z sieciami VPN	101
Przeglądarki zapewniające prywatność	102
Tor	102
Freenet	104
I2P	105
Maszyna wirtualna	106
Emulator urządzeń mobilnych	108
4.4. Konta badawcze	108
4.5. Gratulacje!	113
Część II. Punkty styku OSINT	115
Rozdział 5. Wywiad podmiotowy	121
5.1. Omówienie	121
Czym jest wywiad podmiotowy?	122
Cyfrowy ślad	122
Badanie wzorca życia podmiotu	125
5.2. Imiona i nazwiska	130
Imiona i nazwiska badanych podmiotów	130

Konwencje nadawania imion i nazwisk	130
Arabskie konwencje nadawania imion i nazwisk	131
Chińskie konwencje nadawania imion i nazwisk	132
Rosyjskie konwencje nadawania imion i nazwisk	133
Techniki wyszukiwania imion i nazwisk	133
5.3. Nazwy użytkownika stosowane przez badany podmiot	134
Techniki wyszukiwania nazwy użytkownika	135
Korelowanie kont i informacji o obserwowanym podmiocie według nazwy użytkownika	136
5.4. Adresy e-mail badanego podmiotu	139
Jak rozpocząć łączenie kont	141
Korelowanie ze sobą kont i informacji o podmiocie za pomocą adresów e-mail	141
Konta Google	142
Korelowanie adresu e-mail z domeną	143
Weryfikacja adresów e-mail	144
Usługi e-mail zapewniające prywatność	146
Naruszenia danych	146
5.5. Numery telefonów badanych podmiotów	149
Dodawanie numerów telefonów do dodatkowych selektorów	150
Korelowanie numeru telefonu z obserwowanym podmiotem	150
Podszywanie się pod prawdziwy numer telefonu	152
5.6. Rejestry publiczne i ujawnienie danych przez osobę prywatną	152
Metody inkorporowania wyników wyszukiwania w rejestrach publicznych	153
Gromadzenie z rejestrów publicznych danych skojarzonych z obserwowanym podmiotem	153
Źródła urzędowych rejestrów publicznych w USA	154
Nieoficjalne źródła amerykańskie	162
Rozdział 6. Analiza mediów społecznościowych	165
6.1. Media społecznościowe	165
Kluczowe elementy mediów społecznościowych	166
Zbieranie danych o obserwowanym podmiocie w mediach społecznościowych	168
Korelowanie kont obserwowanego podmiotu w mediach społecznościowych	169
Skojarzenia i interakcje śledzonego podmiotu w mediach społecznościowych	172
Nośniki i metadane użytkownika	176
Media społecznościowe w skrócie	178
6.2. Ciągłe monitorowanie społeczności	179
Metody ciągłego monitorowania grupy	180
Grupy na Facebooku	181
Kanały na Telegramie	181
Reddit	183
4chan i 8kun	185
Dołączyłem do społeczności, co teraz?	187

Nie mogę dołączyć do społeczności, czy nadal mogę ją monitorować?	187
6.3. Analiza obrazów i materiałów wideo	188
Jak patrzeć na obraz lub materiał wideo	189
Odwrotne wyszukiwanie obrazów	191
Geolokalizacja oparta na obrazie	192
Analiza obrazu	193
Kroki przy geolokalizacji	193
Analiza obrazu	196
Kroki przy geolokalizacji	197
Analiza obrazu i geolokalizacja dla zdarzeń w czasie rzeczywistym	200
6.4. Weryfikacja	203
Dezinformacja niecelowa, dezinformacja celowa i dezinformacja szkodliwa	203
Jak sprawdzić, czy treść należy do kategorii MIS, DIS lub MAL?	204
Wykrywanie konta-bota lub sieci botów	206
Wizualizacja i analiza sieci społecznościowych	208
Wykrywanie treści zmienionych cyfrowo	211
Manipulacja zdjęciami	214
Manipulacja plikami wideo	217
6.5. Łączenie wszystkiego w całość	218
Pogoń za oszustwem „na szczeniaka”	218
Rozdział 7. Wywiad biznesowy i organizacyjny	227
7.1. Omówienie	227
Czym jest wywiad organizacyjny?	227
7.2. Organizacje korporacyjne	230
Zrozumienie podstaw struktury korporacyjnej	230
Typy podmiotów	231
7.3. Metody analizy organizacji	232
Źródła rządowe i oficjalne rejestry	234
EDGAR	236
Raporty roczne i sprawozdania finansowe	236
Roczny raport dla udziałowców	237
Formularze 10-K, 10-Q i 8-K	237
Cyfrowe ujawnienia i przecieki	238
Strony internetowe organizacji	238
Media społecznościowe dla organizacji	242
Biznesowa nieroztropność i pozwy sądowe	244
Umowy i kontrakty	246
Kontrakty rządowe	246
Czytanie kontraktów i umów — wiedza podstawowa	248
Mapowanie władzy	256
Wskazówki dotyczące analizy organizacji spoza Stanów Zjednoczonych	260
Kanada	260
Wielka Brytania	260
Chiny	264
Rosja	264

Bliski Wschód	265
7.4. Rozpoznawanie przestępstw organizacyjnych	266
Korporacje fasadowe	267
„Wskazówki"	268
7.5. Sankcje, czarne listy i wpisywanie na listę podmiotów objętych sankcjami 269 Organizacje nakładające sankcje	270
Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych	270
Biuro Kontroli Aktywów Zagranicznych	270
Inne czarne listy	271
7.6. Organizacje non profit	271
Podstawowe dokumenty źródłowe	272
Formularz IRS 990	272
Wyszukiwanie organizacji zwolnionych z podatku dochodowego przez IRS	273
Raporty roczne	274
Raporty konsumenckie i recenzje	275
Charity Navigator	275
7.7. Rejestracja domeny i analiza adresów IP	276
Adresy IP, nazwy domen i strony internetowe organizacji	277
Czym jest adres IP?	277
Czym jest nazwa domeny internetowej?	277
Czym jest strona internetowa i dlaczego to wszystko ma znaczenie?	277
Analiza stron internetowych organizacji	278
Robots.txt	278
Projektowanie stron internetowych i ich zawartość	279
Metadane strony internetowej	279
Analiza danych rekordów WHOIS	281
Analiza adresów IP	283
Adresy IP — wiedza podstawowa	283
Co mogę zrobić z adresem IP?	286
Słowa przestrogi	286
Rozdział 8. Wywiad transportowy	287
8.1. Omówienie	287
Czym jest wywiad transportowy?	287
Krytyczne znaczenie wywiadu transportowego	288
Wywiad wizualny	289
Spotterzy	289
Ujawnianie informacji w mediach społecznościowych	290
Kamera internetowa	290
Zdjęcia satelitarne	292
Wykrywanie sygnału	295
Zrozumienie systemów nawigacyjnych	295
Ciemne sygnały	298
Fałszowanie (spoofing) sygnału	298
Manipulacja tożsamością	300
Zagłuszanie (jamming) sygnału GNSS	301

Symulowanie (meaconing) sygnałów GNSS	301
8.2. Statki	302
Wprowadzenie do wywiadu morskiego	302
Rodzaje podmiotów morskich	303
Terminologia dotycząca statków	303
Metody wykrywania i analizy obiektów morskich	304
Ścieżki i lokalizacje statków	305
Spotkania statków	306
Zawinięcia do portów	310
Właściciele i działalność podmiotu morskiego	313
Podatność morskiej infrastruktury krytycznej i podmiotów morskich na zagrożenia	315
Infrastruktura krytyczna między statkiem a lądem	315
8.3. Koleje	318
Wprowadzenie do wywiadu kolejowego	319
Rodzaje podmiotów kolejowych	320
Terminologia kolejowa	320
Metody wykrywania i analizy połączeń kolejowych	321
Identyfikacja wizualna linii kolejowych	322
Trasy kolejowe i rozkłady jazdy	327
Właściciele i działalność podmiotu kolejowego	331
Podatność kolejowej infrastruktury krytycznej i podmiotów na zagrożenia	331
8.4. Statki powietrzne	336
Wprowadzenie do wywiadu lotniczego	336
Typy statków powietrznych	338
Części składowe typowego odrzutowca	338
Terminologia dotycząca samolotów i podróży lotniczych	340
Metody wykrywania i analizy statków powietrznych	341
Identyfikacja statków powietrznych	342
Trajektorie i lokalizacje lotu	359
Ograniczenie wyświetlanych danych statku powietrznego i listy prywatnych adresów ICAO	362
Śledzenie lotu cargo — ładunku	363
Powiadomienia o misjach lotniczych (NOTAM)	363
Łączność kontroli ruchu lotniczego	365
Aerodromy	365
Geolokalizacja i analiza obrazów statków powietrznych	369
Właściciele i działalność podmiotu lotniczego	371
Podatność lotniczej infrastruktury krytycznej i podmiotów na zagrożenia	373
8.5. Samochody	374
Wprowadzenie do wywiadu motoryzacyjnego	374
Rodzaje podmiotów motoryzacyjnych	375
Terminologia motoryzacyjna	375
Metody wykrywania i analizy samochodów	376
Identyfikacja samochodów	376
Wskazówki dotyczące monitorowania i analizowania tras samochodowych	383
Właściciele i działalność podmiotów motoryzacyjnych	386

Bezpieczeństwo i technologia motoryzacyjna	387
Rozdział 9. Wywiad infrastrukturalno-przemysłowy	390
9.1. Omówienie wywiadu infrastrukturalno-przemysłowego	390
Czym jest technologia operacyjna?	395
Czym jest internet rzeczy i przemysłowy internet rzeczy?	396
9.2. Metody analizy infrastruktury krytycznej, systemów OT i IoT	398
Planowanie analizy	399
Pięć możliwych dróg zbierania informacji	399
Wizualizacje	401
Wykreślanie lokalizacji za pomocą Google Earth Pro	401
Korzystanie z gotowych wizualizacji	406
Ujawnienia publiczne	411
Umowy i kontrakty	411
Media społecznościowe	413
Ogłoszenia o pracę	414
Informacje ujawniane przez spółkę	414
Narzędzia wyszukiwania infrastruktury	415
Censys.io	415
Kamerka	415
9.3. Komunikacja bezprzewodowa i mobilna	418
Omówienie sieci bezprzewodowych i mobilnych	418
Sieci mobilne	419
Wardriving	420
Sieci rozległe o niskim poborze mocy (LPWAN)	422
Radio dalekiego zasięgu (LoRa)	422
Bezprzewodowe identyfikatory SSID, BSSID, MAC	422
Identyfikator zestawu usług (SSID)	422
Podstawowy identyfikator zestawu usług (BSSID)	423
Rozszerzony identyfikator zestawu usług (ESSID)	423
Adres MAC	423
9.4. Metody analizy sieci bezprzewodowych	424
Techniki zbierania informacji	425
Oto kilka punktów zwrotnych przydatnych podczas zbierania informacji o sieci bezprzewodowej	425
Techniki wyszukiwania sieci wi-fi	427
WiGLE	427
Wykreślanie lokalizacji sieci bezprzewodowych za pomocą Google Earth Pro	430
Techniki wyszukiwania wież sieci telefonii komórkowej	432
Rozdział 10. Wywiad finansowy	434
10.1. Omówienie	434
Organizacje zajmujące się wywiadem finansowym	435
Komórki wywiadu finansowego	435
Sieć ścigania przestępstw finansowych	435
Grupa specjalna do spraw działań finansowych	435

Federalna Korporacja Ubezpieczeń Depozytów	436
Międzynarodowy Fundusz Walutowy	436
Federalna Rada Badania Instytucji Finansowych	437
Biuro Kontroli Aktywów Zagranicznych	437
10.2. Przestępczość finansowa i przestępczość zorganizowana	
— na zawsze razem	438
Międzynarodowe organizacje przestępcze	439
Osoba zajmująca eksponowane stanowisko polityczne	441
Przeciwdziałanie praniu pieniędzy	442
Przeciwdziałanie finansowaniu terroryzmu	444
Uchylenie się od płacenia podatków, oszustwa podatkowe i defraudacje	445
10.3. Metody analizy	447
Identyfikatory finansowe	449
Numer identyfikacyjny wydawcy	449
Numer rozliczeniowy ABA	449
Kod SWIFT	449
Podatek od wartości dodanej — VAT	451
Numer BIN	451
Zasoby oparte na lokalizacji	453
Zasoby do analizy finansowania narkotyków	455
Zasoby do analizy przestępczości zorganizowanej	456
Wyszukiwanie ciągów negatywnych newsów	458
Rozdział 11. Kryptowaluty	459
11.1. Omówienie kryptowalut	459
Podstawy kryptowaluty	461
Jak kryptowaluta jest używana i transferowana?	461
Czym jest portfel kryptowalutowy?	461
Czym jest blockchain?	463
Rodzaje kryptowalut	465
Skrócona instrukcja dotycząca monet i tokenów	465
Bitcoin	465
Ether	466
Binance	466
Tether	466
Solana	466
Dogecoin	466
Monero (XMR)	467
Czym jest wydobywanie i wybijanie kryptowalut?	467
Rodzaje weryfikacji	469
Blockchainy publiczne a blockchainy prywatne	470
Dlaczego śledzenie kryptowalut ma znaczenie?	470
Pranie brudnych pieniędzy	471
Oszustwa, nielegalna sprzedaż i materiały dotyczące seksualnego wykorzystywania dzieci	476
11.2. Dark Web	478
Omówienie Dark Webu	478

Rynki darknetowe	480
11.3. Metody analizy kryptowalut	483
Od czego zacząć?	483
Rozpoczęcie od śledzonego podmiotu	483
Rozpoczęcie od śledzonego portfela	485
Śledzenie wypłat gotówkowych na giełdzie	487
Podążanie za skryptami do wydobywania kryptowalut	491
Rozpoczęcie od śledzonej transakcji	491
Rozdział 12. Tokeny niepodzielne	493
12.1. Omówienie tokenów niepodzielnych	493
Przestępstwa związane z tokenami niepodzielnymi	494
Schematy Ponziego i Rug Pulls	494
Fałszywe tokeny niepodzielne	495
Szybkie wzbogacenie się	495
Phishing	495
12.2. Metody analizy tokenów niepodzielnych	495
Według numeru portfela lub adresu	495
Według obrazu	498
Czym jest ENS?	500
Szukaj metadanych	501
Rozdział 13. Co dalej?	502
13.1. Dziękuję Ci za WSPÓLNY skok ze mną	502
Ważne przypomnienia	503

oprac. BPK