



Contenido

Prólogo

Introducción

Capítulo 1. Pensamiento complejo-sistémico en ciberinteligencia/cibercontrainteligencia

El continuo combate de ingenios

Ambiente operativo-organizacional

Preparando el escenario para un análisis avanzado

Análisis avanzado

Mecanismo de análisis, mediante juego de estrategias

Creando Modelos-escenarios

Visualizando negación y falacias de escenarios-modelo

Modelo de redes

Modelo de redes geo-espacial y temporal

Análisis predictivo

Modelo simulado, sus alcances

Fuerza de escenarios

Roles de la informática forense

Pensando como el intruso

Técnicas comunes del intruso

Capítulo 2. Seguridad de la información

Análisis y administración de riesgos

Activos en los sistemas de Información

Entorno

Análisis y clasificación de datos para la transformación a información para la determinación del riesgo

Vulnerabilidad, debilidad

Amenazas

Análisis sistémico de riesgos

Controles de amenazas

Grado de ciberamenazas

Técnicas de mitigación de amenazas

Identificación, evaluación y valoración de sistemas críticos

Inteligencia estructural vs. operativa

Tecnología para la obtención de datos

Tecnología para la valoración y evaluación de información

Ingeniería social evolucionada

Manejo de datos en fuentes abiertas para una correcta información en ciberinteligencia

Formas de análisis en OSINT

Análisis de datos simulados

Buscando vectores de ataques



Capítulo 3. Metodología de contrainteligencia aplicada en la auditoría para la seguridad de datos-información

Construyendo la metodología

- Epistemología sistémica

- Red de métodos para la protección de información

Planeación de auditoría

- Análisis Gap

- Metodología de buscador Maltego

- Análisis FAIR del riesgo

Proceso y análisis desde el método FAIR

- Construcción de escenarios de riesgo FAIR

- Interpretación de resultados por el método FAIR

- Manejo de controles FAIR

Reunión de datos, método RIOT

- Administración de datos método RIOT

- Mitigación del riesgo con método RIOT

- Métodos técnicos para evaluación y administración de riesgo en el objetivo

Ingeniería de la resiliencia para la contrainteligencia

- Análisis de datos en eventos ciberterroristas

Resiliencia de análisis

Capítulo 4. Expectativas de ciberinteligencia/cibercontrainteligencia a enfrentar

Aplicación de la ciberinteligencia en la detección de las llamadas fake news

- Mapeando fake news hostpots en Facebook

- Estudio de memes políticos en Facebook

Ciberamenazas y tendencias

- Elementos facilitadores de ciberataques

- Ciberterrorismo y ciberyihadismo

¿La tecnología se está volviendo más inteligente que el humano?

- Ciberinteligencia cuántica artificial en la programación social

- Desinformación cuántica

Tomando la delantera con ciberriesgo

- ¿Construyendo ciberseguridad o mecanismos de ataque?

- Factor Humano

Ciberespionaje

Recopilación de datos en ciberespionaje



Capítulo 5. El proceso de ciberinteligencia y cibercontrainteligencia para la seguridad nacional

Ciberinteligencia/cibercontrainteligencia en el sector salud

Escenarios de amenazas-riesgos mundiales de pandemias y su impacto en México

Monitoreo estratégico

Sector corporativo-social y el Estado mexicano

La vulnerabilidad empresarial ante el crimen organizado y pandemias

Avances del espionaje empresarial

Sector corporativo-económico en controversias jurídico-administrativas

Cuotas compensatorias

Comercio exterior

Sector estatal y Municipal

Uso de ciberinteligencia/contrainteligencia en las alcaldías urbanas

Uso de ciberinteligencia/contrainteligencia a nivel estatal

Mapeo a redes de riesgo con innovadoras metodologías