DISCIPLINA: Inteligência Cibernética

Polo: Florianópolis

Ementa: Conceitos do funcionamento da internet; Introdução à Inteligência Cibernética: Definição, objetivos e aplicações no contexto de segurança pública; Táticas, Técnicas e Procedimentos (TTPs) de Organizações Criminosas Cibernéticas; Fontes de Inteligência Cibernética (OSINT, HUMINT, SIGINT); Atividades e processos de inteligência cibernética voltados para a coleta, análise e uso de informações; Preparação de ambientes seguros para investigação e atividade de inteligência; Ferramentas de Investigação Digital: scanners de rede, sistemas de análise de infraestrutura de rede, indexadores de dispositivos, raspadores de dados, blockchain; Contramedidas e OPSEC (Segurança Operacional): Controle de Informações Sensíveis, Gestão de Riscos Operacionais, Anonimização, Ferramentas de Segurança Operacional (TOR, VPNs, proxy chains, criptografia ponta a ponta e local, e redes seguras); Análise e compreensão de Ameaças: Principais ameaças, riscos e vulnerabilidades: Engenharia Social, phishing, malwares, defacement, DDoS - Negação de Serviço, trojan, hijack, ransomware; Principais crimes em ambientes cibernéticos: estelionato (leilões, bancos, precatórios, e-commerce), extorsão (sequestro de estações de trabalho, sequestro de perfis em redes sociais, sextorsão), falsidade ideológica (perfis falsos), crimes contra a honra, ameaça, fake news (caráter eleitoral); Investigação Cibernética Aplicada: cadastro e interação com principais plataformas (Google Lers, Uber Lert, Facebook/Instagram/WhatsApp Records, Microsoft/Skype LE e Twitter Legal Requests); Preservação de evidências (formatações programadas e remotas, criptografias forçadas, evidências digitais), análises de metadados. Estudos de caso: sextorsão, sites falsos, crimes contra a honra (remoção de conteúdo); Atividades Práticas: Análises de dados obtidos de plataformas, casos práticos e exemplos reais.

Objetivo: Atualizar o conhecimento dos profissionais da Segurança Pública que atuam nas equipes de investigação, com técnicas e ferramentas de investigação cibernética.

Carga horária: 30h

nº de créditos: 2

Bibliografia básica:

BARRETO, A. G.; WENDT, E.; CASELLI, G. Investigação Digital em fontes abertas. Rio de Janeiro, Editora Brasport, 2017.

BRASIL. Lei n° 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 31 maio 2020.

COELHO, Paulo Cesar. Contrainteligência em Segurança Pública. Campo Grande: 2012.

CORRÊA G. T. Aspectos Jurídicos da Internet. São Paulo: Editora Saraiva, 2010.

JORGE, H. V. N. Investigação Criminal Tecnológica - Volume 1. Rio de Janeiro, Editora Brasport, 2018.

LAUDON, K. C.; LAUDON, J. P. Sistema de Informação com Internet - 4ª edição. Rio de Janeiro. Editora LTC, 1999.

WENDT, E.; NOGUEIRA JORGE, H. V. Crimes cibernéticos: Ameaças e procedimentos de investigação. Rio de Janeiro: Editora Brasport, 2012.

BARRETO, Alesandro Gonçalves. Cyberdicas Eleições 2020: Atribuição de autoria, preservação e remoção de conteúdo no ambiente cibernético. BRASPORT Editora. Rio de Janeiro. 2020.

Nome do docente que irá ministrar a disciplina: Bruno da Cunha Vieira; Fernando Alvaro Ostuni Gauthier