Technische und strafrechtliche Betrachtung von Cyberangriffen

– Interdisziplinäres Seminar für Informatiker und Juristen –

Themen

I) Technische und strafrechtliche Betrachtung von DDoS-Angriffen

II) Technische und strafrechtliche Betrachtung von TDoS-Angriffen

III) Technische und strafrechtliche Würdigung beim Betreiben von Honeypots (mit und ohne Limitierung)

IV) Sonderproblem i.R.d. § 303b StGB: DDoS-Angriffe als Form des politischen Protests (sog. Online-Demonstrationen)

V) Technische und strafrechtliche Bewertung von Port-Scans

VI) Technische und strafrechtliche Betrachtung von Ransomware

VII) Angriffe auf Hausautomationssysteme – technische und strafrechtliche Aspekte

VIII) Justiz als kritische Infrastruktur – technische und strafrechtliche Aspekte

IX) Technische und strafrechtliche Betrachtung von Hard- und Software-Keyloggern

X) Gesetzentwurf zum „Digitalen Hausfriedensbruch" – technische und strafrechtliche Aspekte

XI) Cybermobbing als soziales und strafrechtliches Problem

XII) Strafbarkeit von „Fake-Shops" im Internet

XIII) Aufbau und Betrieb von Botnetzen aus strafrechtlicher und technischer Sicht

XIV) Missbrauch von Notrufen – strafrechtliche Betrachtung des „Swatting"

XV) Problem: Bitcoin und Geldwäsche; Anonymität von Bitcoins

XVI) Illegale Geschäfte im Darknet als technisches und strafrechtliches Problem

XVII) Staatlicher Zugriff auf Krypto-Messenger am Beispiel Telegram

XVIII) Beweisverwertungsverbot bei durch „Hacks" erlangten Daten: LuxLeaks, Pegasus und Panama Papers

XIX) §202d StGB: Datenhehlerei vs. Journalismus und Anwaltschaft

XX) Onion Routing

XXI) Detektion von Social Bots; Fake News und Social Bots

XXII) Cold-Boot-Angriffe

XXIII) Dateisystemforensik

XXIV) Angriffe auf Smart Cars

Eigene Themenvorschläge können eingereicht werden.