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 Würdigung des Betriebs von Honeypots

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

IV) Technische und strafrechtliche Bewertung von Port-Scans

V) Technische und strafrechtliche Betrachtung von Ransomware

VI) Justiz als kritische Infrastruktur – technische und strafrechtliche Aspekte

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

VIII) Cybermobbing als soziales und strafrechtliches Problem

IX) Strafbarkeit von „Fake-Shops" im Internet

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

XI) Illegale Geschäfte im Darknet als technisches und strafrechtliches Problem

XII) Staatlicher Zugriff auf Krypto-Messenger am Beispiel Telegram

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

XIV) Onion Routing

XV) Cold-Boot-Angriffe

XVI) Angriffe auf Smart Cars

XVII) Das Netzwerkdurchsetzungsgesetz und seine Auswirkungen auf die Meinungs- und Pressefreiheit

XVIII) Vorratsdatenspeicherung und Zugriff der Strafverfolgungsbehörden

XIX) IDS und das Telekommunikationsgeheimnis

Eigene Themenvorschläge können eingereicht werden.