

Darknet

Seminar im Sommersemester 2019

Mit dem Schlagwort »Darknet« wird zumeist die Nutzung des TOR-Netzwerks im Internet und spezifisch die Nutzung von »Hidden Services« im TOR-Netzwerk bezeichnet. Diese Technologien ermöglichen ein hohes Maß an technischer Anonymität. Sie werden indes nicht nur zu legitimen und legalen Zwecken genutzt, sondern auch zu kriminellen Zwecken. Die technischen Grundlagen und die Phänomenologie des Darknets werden in zwei Einführungsveranstaltungen in den ersten Wochen des Sommersemesters 2019 beleuchtet. Auf dieser Grundlage folgt in der Blockveranstaltung gegen Ende des Sommersemesters eine materiell-strafrechtliche Analyse von verschiedenen Phänomenen im Darknet sowie eine strafprozessual ausgerichtete Bewertung von Ermittlungsmethoden, die zur Verfolgung von »Darknet«-Kriminalität Verwendung finden.

Administrativa: Das Seminar richtet sich an alle Studierende der Rechtswissenschaften, insbesondere an Studierende der Schwerpunktbereiche 6 und 9. Eine Vorbesprechung am **Montag, den 15. April 2019, von 16 bis 18 Uhr (Gebäude C3 1 – Raum 1.01)** statt. Anmeldungen zur Vorbesprechung (gerne bereits mit Themenwünschen) sind unter dominik.brodowski@uni-saarland.de möglich, aber nicht verpflichtend.

An Themen für Seminararbeiten sind insbesondere noch zu vergeben:

1. Waffenhandel im Darknet – eine strafrechtliche Analyse
2. Drogenhandel im Darknet – eine strafrechtliche Analyse
3. Handel mit »gestohlenen« Kreditkartendaten im Darknet – eine strafrechtliche Analyse
4. Handel mit »gestohlenen« Zugangsdaten im Darknet – eine strafrechtliche Analyse
5. Handel mit Schadsoftware im Darknet – eine strafrechtliche Analyse
6. »Crime as a Service«: das Anbieten einer Dienstleistung zur »digitalen« Erpressung im Darknet – eine strafrechtliche Analyse
7. Das Betreiben einer Handelsplattform im Darknet – eine strafrechtliche Analyse
8. Strafrechtliche Verantwortlichkeit von Betreibern von TOR-Nodes für über TOR begangene Straftaten
9. Strafrechtliche Verantwortlichkeit von Betreibern von Darknet-Suchmaschinen und Darknet-Übersichtsportalen
10. Personale Ermittlungen im Darknet – Rechtsgrundlagen, Beweisgewinnung, Beweisverwertung
11. Die Übernahme von »Profilen« im Darknet durch Ermittlungsbehörden – Rechtsgrundlagen, Beweisgewinnung, Beweisverwertung
12. »Keuschheitsproben« im Darknet – Legitimation und Grenzen der Straftatbegehung durch Ermittler zur Ausforschung von Kriminalitätsstrukturen im Darknet
13. Strafprozessualer Zugriff auf »Täter-IT« – Möglichkeiten und Grenzen einer Telekommunikationsüberwachung von Server-Systemen und Exit-Nodes im Darknet
14. Telekommunikationsüberwachung, Quellen-TKÜ und Computerstraftaten: bedürfen die §§ 100a, 100b StPO einer Reform?
15. Informationsaustausch zwischen Nachrichtendiensten und Strafverfolgungsbehörden zur Verfolgung von Darknet-Kriminalität