Rechtswissenschaftliches Institut

Lehrstuhl für Strafrecht und Strafprozessrecht
Prof. Dr. iur. Marc Thommen, LLM
Treichlerstrasse 10
8032 Zürich
Telefon +41 44 634 1531
www.rwi.uzh.ch/thommen/

THEMENLISTE

Seminar „Strafverfolgung zu Beginn des 21. Jahrhunderts - Staatstrojaner, geheime Überwachung, Cybercrime“ im FS 16

Materielles Recht

~~1. Strafrechtliche Relevanz der DDoS-Attacke~~

~~Immer häufiger werden Server von Firmen mittels einer Distributed-Denial-of-Service-Attacke lahmgelegt. Dahinter können verschiedene Motive stecken. Obschon solche DDoS-Attacken grosse Schäden verursachen, ist deren strafrechtliche Relevanz nicht eindeutig geklärt. Insbesondere stellt sich die Frage, welche Tatbestände des StGB unter welchen Voraussetzungen bei einer DDoS-Attacke erfüllt sein könnten.~~

~~2. Phishing mails – nerviger Spam oder strafwürdiger Betrug?~~

~~3. Die strafrechtliche Relevanz von Filesharing, Internet-Piraterie und Streaming~~

~~4. «Identitytheft»: Was versteht man darunter und wird der «Identitytheft» strafrechtlich genügend erfasst?~~

~~Mit dem Internet eröffnen sich für Konsumenten neue Möglichkeiten: Der tägliche Einkauf lässt sich bequem über die entsprechende App tätigen, Kleider können quer über den Atlantik hinweg bestellt werden und Ferien müssen nicht mehr beim lokalen Reisebüro gebucht werden. Gleichzeitig bergen diese Möglichkeiten auch neue Risiken in Form des sog. «Identitytheft». Was versteht man darunter? Wird dieser Sachverhalt strafrechtlich genügend erfasst? Und welche Rolle spielt dabei das Verhalten des unbescholtenen Users?~~

5. ~~Verantwortlichkeit des Host-Providers für schädliche Inhalte (am Beispiel von TagesAnzeiger online)~~

~~Welches sind die verschiedenen Akteure einer Straftat im Internet?~~

~~Inwiefern haftet insbesondere der Host-Provider für die Verbreitung «schädlicher Inhalte» (Rassismus, Pornograpie, Gewaltdarstellung, etc.)?~~

~~Haftet der Host-Provider (nur) nach allgemeinen Grundsätzen (von besonderer Bedeutung ist hier die Kenntnis oder das Kennenmüssen des Inhalts) oder darüber hinaus auch nach den Grundsätzen des Medienstrafrechts (Art. 28, 322, 322bis StGB?~~

~~Welches sind allenfalls die Massnahmen, welche der Host-Provider treffen muss, um sein allfälliges Haftungsrisiko zu reduzieren?~~

6. ~~Internet als öffentlicher Raum: Wie schreckt man die Bevölkerung im Internet?~~

~~Der Personenkreis, „mit welchem der Urheber einer Äusserung durch Freundschaft oder Bekanntschaft im realen oder virtuellen Leben verbunden ist. [kann] nicht als „Bevölkerung" im Sinne von Art. 258 StGB angesehen werden […]" (BGer 6B_256/2014 vom 8. April 2015 (zur amtl. Publikation vorgesehen), E. 2.3.4). Wird Art. 258 StGB im Zusammenhang mit Cybercrime-Delikten damit zum Papiertiger? Oder lässt sich die Bevölkerung auch digital schrecken?~~

7. ~~Quellenschutz für Blogger: Ist jeder User ein Journalist?~~

8. ~~Strafbarkeit durch «Surfen» auf Seiten mit schädlichen Inhalten (z.B. auf Porno-Seiten)~~

~~Welche unterschiedlichen Formen der Strafbarkeit nach Art. 197 StGB gibt es?~~

~~Wird durch das «Surfen» auf Seiten mit schädlichen Inhalten der Tatbestand des «Beschaffens» oder des «Besitzens» verwirklicht? Ab wann «besitzt» man im Internet pornographische Inhalte? Müssen die Daten gezielt abgespeichert werden?~~

~~Was bewirkt die Abspeicherung schädlicher Daten auf eigene Datenträger? Ist dies bereits ein «Herstellen» nach Art. 197 StGB?~~

~~Welches sind die strafbarkeitsbeschränkenden Verhaltensmassnahmen, wenn man zufällig auf Seiten mit schädlichen Inhalten gelangt?~~

Prozessrecht

9. Beschlagnahme von E-Mails: Wann braucht es die Echtzeit-Überwachung, wann muss editiert werden?

Gemäss BGE 140 IV 181 müssen vom Beschuldigten auf dem Server abgerufene E-Mails beschlagnahmt, nicht abgerufene durch eine Echtzeit-Überwachung erhoben werden. DieserEntscheid des Bundesgerichts stellt die Strafverfolger vor verschiedene Umsetzungsprobleme in der Praxis. Beispielsweise stellt sich die Frage, wie festgestellt werden soll, ob eine E-Mail abgerufen wurde oder nicht? Weiter kann heute nicht eindeutig festgestellt werden, von wem eine E-Mail abgerufen wurde. Wie sind E-Mails zu erheben, die zwar abgerufen wurden, aber nicht vom Beschuldigten, sondern von einer Drittperson? Gäbe es nicht tauglichere Ansätze, als auf den Zeitpunkt der letzten Verbindung mit dem Mailserver abzustellen? Wie ist der BGE im Lichte dieser praktischen Probleme zu beurteilen?

10. Beschlagnahme von Webseiten: Ist eine .ch-Domain auf einem ausländischen Server beschlagnahmefähig?

«Schweizer» Webseiten mit dem Kürzel .ch am Ende sind unter Umständen weniger schweizerisch als man denkt: Die Webseite liegt womöglich auf einem Server im Ausland. Wenn nun Schweizer Strafverfolgungsbehörden die Seite aus welchen Gründen auch immer beschlagnahmen (lassen) wollen: Wie lässt sich eine Webseite technisch überhaupt beschlagnahmen? Und wie muss dabei prozessual vorgegangen werden? Können die Schweizer Behörden selber vorgehen? Oder nur den Auftrag an die zuständige nationale Behörde geben?

~~**11. Nutzung von privaten Informationen: Die strafprozessuale Verwertung von privaten Informationen aus dem Darknet sowie von Cyberdefense-Unternehmen.**~~

~~Die Strafverfolgungsbehörden erhalten immer öfter nicht einfach nur Hinweise auf ein Cybercrime, sondern gleich eine ganze Beweiskette, die den (angeblich) Schuldigen überführt. Dürfen die Strafbehörden solche Informationen ohne weiteres berücksichtigen? Welche Sorgfaltspflichten treffen die Strafbehörden?~~

~~12. Gerichtsverwertbare Beweiserhebung und Beweisführung bei Cyber-Delikten und die Frage der Teilnahmerechte~~

~~Prinzipien der Beweiserhebung und Beweisführung im Strafprozess~~

~~Problematiken der Beweiserhebung und –führung bei Cybercrime-Delikten, insb.: Wie können Abläufe im Internet zur Überzeugung eines Gerichts nachgeweisen werden? Wie kann man den Abruf «schädlicher Inhalte», wie kann man Computerdaten bzw. Datenpakete überhaupt gerichtsverwertbar konservieren? Wie kann man Kommunikationsabläufe im Internet gerichtsverwertbar nachzeichnen?~~

~~Computerforensik als Spezialwissenschaft für die Beweisführung und die Darlegung der Beweiskette vor Gericht (Spurensicherung/Sicherstellung; Datenanalyse und –aufbereitung; Wiederherstellung «gelöschter» Daten).~~

~~Welches sind die Auswirkungen der speziellen Art der Beweiserhebung und Beweisführung auf die Teilnahmerechte der Parteien?~~

13. Convention on Cybercrime: Welche Möglichkeiten gibt es, um grenzüberschreitend und zeitnah (d.h. ohne Rechtshilfeverfahren) Daten zu erhalten?

Die Strafverfolgung im Bereich Cybercrime stösst im wahrsten Sinne des Wortes an ihre Grenzen, wenn es dabei geht, Daten im Ausland zu erheben, da das Territorialitätsprinzip den Schweizerischen Strafverfolgungsbehörden verbietet, direkt im Ausland auf Daten zu greifen. Klassischerweise müssen solche Daten in einem langwierigen und komplizierten Rechtshilfeverfahren erhoben werden. Die sog. «Cybercrime-Convention» bietet verschiedene Instrumente an, um einfacher und schneller grenzüberschreitend Daten zu sichern und Daten zu erheben. Welche Instrumente sind das und unter welchen Voraussetzungen kommen sie zur Anwendung?

~~14. Der Einsatz von Govware ist auch unter geltender StPO rechtmässig.~~

~~Der Einsatz von Govware ist heute rechtlich und politisch umstritten. Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs ist momentan in Revision. Mit der Revision soll sichergestellt werden, dass der Einsatz von Govware rechtlich eine saubere Grundlage erhält. Aber braucht es diese Revion tatsächlich? Oder kann Govware bereits mit der heutigen Rechtslage rechtmässig eingesetzt werden?~~

15~~. Zulässigkeit und Grenzen verdeckter Fahndungen und Ermittlungen im World Wide Web, insb. in (Sex-)Chatrooms~~

~~Unterschiede von verdeckter Fahndung und verdeckter Ermittlung im World Wide Web~~
~~Welches sind die besonderen Probleme von «zivilen elektronischen Streifenfahrten», des «agent provocateurs» etwa in Chatrooms sowie der «geheimen elektronischen Überwachung»?~~
~~Welches sind die Vorausstzungen zulässiger elektronischer verdeckter Fahndung und/oder Ermittlung?~~
~~Welches sind die Folgen unzulässiger verdeckter elektronischer Fahndung und/oder Ermittlung?~~

~~16. Wo finden Internet-Delikte statt und welche Behörde ist letztlich zuständig?~~