VL	Informationstechnologie und Grundlagen der IT-Sicherheit für Verwaltungs- und Politikwissenschafter
Veranstalter[1]	Robert Müller-Török, Alexander Prosser
Zeit	10. und 11.9.2014, 9.30-17.45
Ort	PC-Raum
Anrechnungscode	POWI047
Kreditpunkte	3
Kontaktstunde	vor und nach der Lehrveranstaltung
Prüfungsanmeldung	über das elektronische Studienverwaltungssystem (ETN)

Inhalt und Ziele

Kursbeschreibung: IT-Kenntnisse sind üblicherweise für Verwaltungs- und Politikwissenschafter nicht so wichtig. Dennoch gewinnt das Thema Cyber security für Verwaltungen und Staaten erheblich an Bedeutung.

Beispielsweise ändert sich der Begriff und das Wesen von Verbrechen völlig: Während ein bspw. Diebstahl bisher physische Anwesenheit voraussetzte, ist es mittlerweile problemlos möglich, über Internetbetrug, Hacken der elektronischen Identitäten und Passwörter der Opfer aus zigtausend Kilometer Entfernung zu stehlen. Natürlich auch aus dem Ausland. Die Instrumente der Strafverfolgung reichen dafür nicht aus, weder faktisch noch theoretisch. Ist eine Kopie einer Datei ein Diebstahl? Ein U.S. District Court hat diese Frage vor wenigen Jahren verneint.
Es ist deshalb notwendig, mehr als nur rein Grundlagenverständnis zu entwickeln und zu verstehen, zu durchdringen, wie elektronische Medien, insbesondere das Internet funktionieren und wie das in den bestehenden Kanon der Verwaltungs- und Politikwissenschaften eingebracht werden kann. Sie lernen hier

- zu verstehen, wie Computernetzwerke funktionieren
- zu verstehen, wie das Internet funktioniert, wie es organisiert ist und was die rechtlichen Implikationen hiervon sind
- Überwachungs- und Zensurmethoden im Internet und ihre technischen Grenzen
- Grundlagen der Kryptographie und wie man sich damit selbst sichern kann
- zu verstehen, wie eine digitale Signatur funktioniert und wie sicher z. B. eine https-Verbindung wirklich ist
- zu verstehen, wie die Technik Kriminelle, Terroristen und ausländische Nachrichtendienste dabei unterstützt, abzuhören, zu sabotieren und die Kommunikation zwischen Computern zu verfälschen
- Methodologie für die Einschätzung der Verwundbarkeit kritischer nationaler Infrastruktur gegen Angriffe
- Einschätzung des Wertes von elektronischen „Beweisen" im Hinblick auf ihre Beweiswürdigkeit
    - Wie man E-Mails mit falschem Absender und falschen IP-Adressen erzeugt und wie man die rechtliche Qualität von E-Mails richtig einschätzt
    - Wie man MAC und IP Adressen auf Computer und Smartphone/Tablet manipuliert und sich als jemand anderer ausgeben kann
    - wie man IP Adressen fälscht oder verschleiert
- welche Sicherheitsstandards letztlich im Internet, im e-Government möglich sind und welche Kosten hiermit verbunden sind
- was CALEA, FISA und andere US-Gesetze für US-basierte Computer- und Telekommunikationsfirmen bedeuten und wie Sie davon betroffen werden
- zu verstehen, was die wichtigsten und möglicherweise unlösbaren Gegensätze zwischen Technologie und Recht sind
- wie ERP Systeme wie z. B. SAP funktionieren und was für Betrugsmöglichkeiten sie bieten bzw. welche Beweismöglichkeiten
- wie Webservices funktionieren und welche Möglichkeiten sie z. B. Strafverfolgungsbehörden bieten

Form und Umfang der zu erbringenden Leistungen: Hausarbeit

[1] Die Namen der Veranstalter sind ohne Titel aufzuführen.