Chemnitzer Linux-Tage 2014

Jakob Kullik, M.A. Lehrbeauftragter an der Professur Internationale Politik der TU Chemnitz

Vortrag: „Deutschlands Sicherheitspolitik im Cyberspace“

Der Siegeszug der modernen Informations- und Kommunikationstechnologien hat zu einer weltweiten digitalen Vernetzung von Unternehmen, staatlichen Einrichtungen und (mobilen) Geräten geführt. Neben den zahlreichen positiven Auswirkungen, die diese Digitalisierungsrevolution mit sich gebracht hat, existiert auch eine bedrohliche Seite des Cyberspace. Neue Phänomene wie Cyberkriminalität, Cyberspionage und Cybersabotage sind in den letzten Jahren zu ernsthaften Bedrohungen für Wirtschaft, Politik und kritische staatliche Infrastrukturen geworden. In militärischen und Geheimdienstkreisen wird bereits das Konzept der Cyberkriegsführung zwischen Staaten diskutiert. Deutschlands Konkurrenten im Cyberspace sind nicht nur bekannte Akteure, wie die Volksrepublik China und die Russische Föderation, sondern, wie im Zuge der NSA-Affäre deutlich wurde, auch die transatlantischen Partnerstaaten USA und Großbritannien. Daneben gibt es eine ganze Reihe weiterer Bedrohungen, wie die (organisierte) Internetkriminalität, extremistische politische und religiöse Cyberaktivisten und professionelle Auftragshacker, die ihre Dienste anbieten und den Cyberspace zu einem neuen Raum für Wirtschaftskriminalität, Industriespionage und militärische Operationen machen.

Der Beitrag will zeigen, welchen Stellenwert das Politikfeld Cybersicherheit in der Sicherheitspolitik Deutschlands einnimmt, welche Ministerien (Innen-, Wirtschafts-, Verteidigungsministerium, Auswärtiges Amt), welche Behörden (Bundesamt für Sicherheit in der Informationstechnik) und neugeschaffenen Einrichtungen (Nationales Cyberabwehrzentrum, Nationaler Cybersicherheitsrat) in der nationalen IT-Sicherheit beteiligt sind und miteinander kooperieren. Darüber hinaus interessiert, welche konkreten operativen IT-Fähigkeiten die verantwortlichen exekutierenden Stellen (Bundeskriminalamt, Bundeswehr, Nachrichtendienste) besitzen, um Deutschland wirksam vor IT-Bedrohungen schützen zu können. Zusätzlich zur nationalen Ebene spielen die Europäische Union (EU) und die Nordatlantische Allianz (NATO) ebenfalls eine wichtige Rolle in der multinationalen Kooperation bei Cybersicherheit.

Darüber hinaus gilt es, die rechtliche Säule dieses neuen und in weiten Teilen noch ungeregelten Politik- und Rechtsfeldes mit zu betrachten und einen Überblick über wesentliche völker-, verfassungs- und strafrechtliche Aspekte zu geben. Diese machen deutlich, dass die Übertragung des derzeit existierenden Rechtsbestandes auf die besonderen Spezifika des (technischen) Cyberraums in einigen wesentlichen Punkten scheitert. Neben bestehenden rechtlichen Lücken und Graubereichen existieren in den Reihen der staatlichen Legislative und Exekutive zudem nach wie vor ernsthafte Wissens-, Kompetenz- und Vollzugsdefizite.

Der Vortrag richtet sich an Studierende aller Studiengänge und die interessierte Öffentlichkeit. Fachbezogene Vorkenntnisse im Bereich moderner IT- und Computersysteme sind von Vorteil, aber keine notwendige Voraussetzung zum Verständnis der Vortragsthematik. Kenntnisse des politisch-institutionellen Systems der Bundesrepublik Deutschland und der Europäischen Union sowie grundlegende Zusammenhänge der internationalen (Sicherheits-)Politik werden vorausgesetzt. Aspekte aktueller Problemfälle aus dem Völker-, Verfassungs- und Strafrecht im Bereich IT-Sicherheit werden ebenfalls thematisiert werden.