Author built version of : Diesner, J., & Carley, K. M. (2010) Relation Extraction from Texts (in German, title: Extraktion relationaler Daten aus Texten). In C. Stegbauer & R. Häußling (Eds.), Handbook Network Research (Handbuch Netzwerkforschung). Vs Verlag.

Relationale Verfahren in der Erforschung, Ermittlung und Prävention von Kriminalität

Jana Diesner und Kathleen M. Carley

Dieser Beitrag vermittelt aus der Perspektive akademischer Forschung nach einer kurzen Einleitung einen Überblick über die wesentlichen Gruppen von netzwerkanalytischen Methoden, die bei der Erforschung, Ermittlung und Verhinderung von Kriminalität Einsatz gefunden haben. Im Anschluss daran erläutern wir verschiedene inhaltliche Unterbereiche von Kriminalität aus dem Blickwinkel der Netzwerkanalyse. Der Beitrag schließt mit einer kurzen Diskussion zu Datenschutz und Datensicherheit.

Analyseeinheit in der Netzwerkforschung sind nicht das Individuum und seine Merkmale, sondern die Verbindungen bzw. Relationen zwischen Einheiten. Diese Einheiten können unter anderem Personen, Organisationen, Orte und Ressourcen sein. Wieso sollte ein relationaler Ansatz bei der Untersuchung von Kriminalität sinnvoll sein? Reiss (1988) beklagt für den Fall der Ermittlung von Gruppendelikten die künstliche Reduktion von tatsächlichen Tätergruppen auf unverbundene Einzelpersonen. Sarnecki (2001) kritisiert, dass Analysen oft auf der Ebene von unverbundenen Individuen und deren Aggregaten durchgeführt werden, obwohl empirische sozialwissenschaftliche und kriminologische[1] Studien einen Zusammenhang zwischen den sozialen Verbindungen einer Person und deren kriminellem Verhalten gezeigt haben. Zudem setzten Exekutivorgane auf die Abschreckung von Einzelpersonen statt von strategischen Verbindungen und von Personen in relevanten Netzwerkrollen (ebd.). Relationale Verfahren bieten eine Ergänzung oder Alternative zu Methoden, die Verbindungen nicht zwischen Individuen, sondern zwischen Merkmalen von Einzelpersonen herstellen, wie z.B. die Rasterfahndung (Taipale, 2003). Bei der Rasterfahndung definieren Sachverständige ein Personenprofil, das sich hauptsächlich aus physischen und soziodemografischen Angaben zusammensetzt. Anschließend werden Daten aus verschiedenen Beständen nach diesem Profil durchsucht, um mögliche Verdächtige zu identifizieren (Pehl, 2008). Ressler (2001) weist darauf hin, dass die Netzwerkanalyse personenbezogene Merkmale in Form von Knotenattributen berücksichtigen kann, zusätzlich aber auch die Relationen zwischen Knoten in Betracht zu ziehen vermag.

Welchen potenziellen Nutzen birgt die Netzwerkanalyse bei der Untersuchung von Kriminalität? Exekutivorgane verfügen in der Regel über große Datenmengen, aber knappe zeitliche und personelle Ressourcen. Die Netzwerkanalyse kann helfen, knappe Mittel nicht auf die Untersuchung aller Hinweise und möglicherweise involvierten Personen gleichmäßig aufzuteilen, sondern gegebene Mittel strategisch auf Schlüsselfiguren und Schüsselverbindungen zu verwenden (Howlett, 1980; Sparrow, 1991). Relationale Verfahren eignen sich zudem, nicht auf die Enthüllung hierarchischer Strukturen mit

[1] *Kriminologie* ist die Lehre vom Verbrechen, während Verbrechensbekämpfung Gegenstand der *Kriminalistik* ist.

zentraler Führerschaft an deren Spitze hinzuarbeiten, sondern auf die Vereitelung kleinerer gesetzwidriger Aktivitäten mit exponentieller Resonanz oder brückenschlagender Wirkung (Chibelushi et al., 2006; Klerks, 2001). Insgesamt kann ein netzwerkorientiertes Vorgehen Analysten dabei unterstützen, ein umfassendes Verständnis von komplexen und dynamischen Systemen zu gewinnen.

Die tatsächliche Nutzung der Netzwerkanalyse durch Exekutivorgane ist für akademische Forscher in der Regel nicht einsehbar. Öffentlich bekannt ist aber, dass die Exekutivorgane verschiedener Länder und internationaler Bündnisse entsprechende Projekte ausgeschrieben und gefördert, Stellen geschaffen und Stipendien vergeben haben. In Rahmen dieser und anderer Initiativen wird die Netzwerkanalyse heute als ein integraler Bestandteil interdisziplinärer Ansätze zur Erforschung, Ermittlung und Prävention von Kriminalität angesehen - gemeinsam mit Ansätzen unter anderem aus der Informatik, Soziologie, und Rechtswissenschaft (Brantingham und Brantingham, 1993; Ressler, 2006).

1 Klassifizierung Methodischer Ansätze

In diesem Abschnitt fassen wir die verschiedenen methodischen Vorgehensweisen in der relationalen Analyse von Kriminalität in wesentliche Gruppen zusammen.

1.1 Relationales Denken und Netzwerkbeschreibungen

Die Kategorie „relationales Denken und Netzwerkbeschreibungen“ vereint Studien, die ursprünglich nicht netzwerkorientiert angelegt waren, die aber netzwerkrelevante Einsichten gewonnen haben, sowie theoretische und anekdotische Beschreibungen von Netzwerken, die den Wissensstand der Netzwerkforschung vorangebracht haben: Solche Studien haben gezeigt, dass das Knüpfen krimineller Verbindungen auf Vertrauen basiert (Erickson, 1981). Das liegt unter anderem daran, dass illegale Vereinbarungen im Falle von „Vertragsbruch“ nicht einklagbar sind, und dass Loyalität und Verschwiegenheit unabdingbar für die Geheimhaltung der gemeinsamen Sache sind (Ressler, 2006; Simmel, 1908; Waring, 2002). Erickson (1981) schließt aus der qualitativen Metaanalyse verschiedener Geheimbünde, dass die Netzwerkstruktur solcher Gruppen Funktion und Spiegel derjenigen Vertrauensbeziehungen ist, die bereits vor dem Entstehen der Gruppe zwischen ihren Mitgliedern bestanden haben. Untersuchungen in dieser Kategorie haben weiterhin dazu beigetragen, dass in der modernen Kriminalitätsforschung das Konzept der kriminellen Unterwelt, die parallel zur gesetzestreuen Welt existiert, ersetzt wurde durch ein Verständnis von Kriminalität, die ihre Anker und Berührungspunkte in der legalen Welt hat (Klerks, 2001; Sarnecki, 2001). Zudem haben zahlreiche Studien zu der mittlerweile von vielen anerkannten Einsicht geführt, dass kriminelle Gruppierungen von heute nicht als hierarchische Strukturen mit zentralen Führerschaft organisiert sind, sondern als lose verbundene Netze (Arquilla und Ronfeldt, 2001; Popp et al., 2004). Diese Netze setzen sich oft aus einer Vielzahl von Zellen zusammen, über deren Grenzen hinweg sich die Mitglieder kaum kennen. Die Partitionierung der Netze in voneinander weitestgehend unabhängige Cluster bietet den einzelnen Mitglieder wie auch dem Gesamtgefüge Schutz im Falle der Aufdeckung oder Schwächung einzelner Zellen. Abschließendes Beispiel für

Erkenntnisse aus Analysen in dieser Kategorie ist das Wissen darüber, dass Mitglieder heutiger illegaler Netze moderne Informations- und Kommunikationstechnologien (IKT) früh für sich adaptieren und kompetent und strategisch einsetzen, um sich über geographische und soziale Distanzen hinweg schnell, flexibel und zu niedrigen Kosten zu verlinken und zu koordinieren. Diese Art des Organisierens hat beispielsweise die Strategie des *Swarmings* ermöglicht, bei der mehrere Zellen ein oder mehrere Ziele aus unterschiedlichen Richtungen angreifen und in einem unregelmäßigen Pulsieren auftauchen und wieder verschwinden (Arquilla und Ronfeldt, 2001). Ein Beispiel für Swarming ist *the Battle of Seattle*, bei dem lose bis gar nicht organisierte Personengruppen mit vielfältigen Strategien, wie z.B. Blockaden von Straßen und Webseiten, versucht haben, das Treffen der Welthandelsorganisation in Seattle 1999 lahmzulegen. Natürlich ist nicht jede als Netz organisierte und organisierende Gruppierung auch kriminell: Auch einige staatliche Organe sowie zahlreiche nichtstaatliche Interessen- und Aktivistengruppen haben die Netzwerkform adaptiert. Ein Beispiel hierfür ist die „Internationale Kampagne für das Verbot von Landminen", die gemeinsam mit einer ihrer Organisatorinnen, Jody Williams, den Friedensnobelpreis im Jahre 1997 erhielt. Hauptunterschiede zwischen den Arten von Initiativen, für die der Battle of Seattle versus die Internationale Kampagne für das Verbot von Landminen stellvertretend stehen, sind deren Ziel und Einfluss: Temporäre Störung auf der einen Seite versus einer klar definierten und langfristigen politischen Agenda auf der anderen Seite (Denning, 2001).

1.2 Link Analyse

Die Link Analyse wird seit den 1970er Jahren in der Kriminalitätsprävention und der Strafverfolgung eingesetzt, um illegale Strukturen systematisch zu erfassen und auszuwerten. Bei dem Verfahren werden relationale Daten via Reduktion und Abstraktion aus großen Mengen von Daten aus verschiedenen Quellen extrahiert, in einer Assoziationsmatrix repräsentiert und als Netzwerkvisualisierung, auch Anacapa Diagramm genannt, dargestellt (Harper und Harris, 1975). Die Methode wurde anfangs manuell durchgeführt, bald aber durch Softwareprogramme wie *Analyst's Notebook* oder *NetMap* unterstützt. Knotentypen in Anacapa Diagrammen sind unter anderem Personen, Organisationen, Telefonnummern, Adressen, Autokennzeichen, Informationen, und Produkte. Kanten können die Existenz, Stärke, Wahrscheinlichkeit und Art von Kontakten repräsentieren (Howlett, 1980). Ein Anacapa Diagramm ist lediglich ein Bild. Daher bedarf es der Kompetenz und Erfahrung der Mitarbeiter der Exekutivorgane, um mittels induktiver Logik aus Anacapa Diagrammen Hypothesen abzuleiten, die nachfolgend geprüft werden (Davis, 1981). Die Interpretation der Netze kann den Behörden unter anderem zur Identifikation von Personen dienen, die hinsichtlich ihres Wissens oder Könnens eine Alleinstellung im Netzwerk aufweisen, sowie zur Erkennung von Akteuren, die aus bestimmten Netzwerkpositionen heraus das Geschehen maßgeblich beeinflussen. Zudem kann mit Hilfe der Link Analyse abgeschätzt werden, wie stark einzelne Personen in konspirative Ereignisse involviert sind, über welche Menge und Qualität von Informationen sie verfügen und welche Erwartungen an sie in Abhängigkeit ihrer Position oder Rolle im Netzwerk gestellt werden können (ebd.). Harper und Harris (1975) haben gezeigt, dass Polizisten ohne technische Ausbildung die Methode der Link Analyse leicht erlernen

können. Dabei leiteten die untersuchten Polizisten starke Kanten (strong ties) zuverlässig aus harten Fakten ab, entnahmen aber schwache Kanten (weak ties) aus impliziten Hinweisen mit geringer Genauigkeit (ebd.).

1.3 Analyse Sozialer Netzwerke

Die Analyse sozialer Netzwerke (ASN) erweitert die Link Analyse um analytische Fähigkeiten, wie z.B. dem Berechnen graphentheoretischer Maßzahlen oder dem Partitionieren von Netzen in homogene Subgruppen, auch Cluster genannt. Einige Maße aus der ASN sind in der Kriminalitätsforschung besonders relevant: Die Betweenness Zentralität kann helfen, „kriminelle Kontaktmakler" zu identifizieren – also unauffällige Personen, die zur richtigen Zeit am richtigen Ort auftauchen, um Kontakte zu vermitteln (Klerks, 2001). Schwache Kanten (Granovetter, 1973) sind von tragender Bedeutung bei der Koordinierung zwischen Zellen oder Gruppen und dienen zudem als Brücken zu sozial wie geographisch entfernten Quellen für Informationen, Warnungen, Spezialisten und Ressourcen (Sarnecki, 2001; Williams, 2001). Knoten mit niedriger struktureller oder regulärer Äquivalenz können schwer ersetzbare Personen oder Objekte repräsentieren (Krebs, 2002). Relevant sind zudem *cut points*, also Knoten oder Sets von Knoten, deren Schwächung oder Eliminierung zum Zerfall (von Teilen) des Netzes in unverbundene Gruppen führen würde (Carley et al., 2001; Rodríguez, 2004). Für den Typ der zellulären Netze wurde jedoch gezeigt, dass die Beseitigung einzelner Zellen keine nachhaltige Schwächung des Gesamtnetzes bewirkt (Carley et al., 2001).

Die Anwendung der ASN bei der Untersuchung von Kriminalität birgt eine Reihe von Schwierigkeiten. Wir gehen hier vor allem auf Probleme hinsichtlich der Gewinnung, Qualität und Aussagekraft von Daten ein: Da Straftäter in der Regel Fragebögen nicht oder nicht korrekt ausfüllen, entfällt ein klassischer Ansatz zur Erhebung von Netzwerkdaten. Bei alternativen Verfahren zur Erhebung oder Fusion von Datensätzen kann oft nicht von vornherein unterschieden werden, wer potenziell oder tatsächlich straffällig ist und wer nicht (Pehl 2008). Daher sind die in Betracht gezogenen Datensätze häufig groß, hinsichtlich relevanter Verbindungen zwischen kriminellen Personen aber mager. Weiterhin reduzieren unscharfe Netzwerkgrenzen die Aussagekraft von Maßen wie Dichte, Durchmesser, Degree und Closeness Zentralität und euklidischer Distanz (Brantingham und Brantingham, 1993; Sparrow, 1991). Zudem besteht die Gefahr, diejenigen Personen als zentral zu identifizieren, über die den staatlichen Organen die meisten Informationen vorliegen, die aber nicht zwangsläufig die tatsächlich bedeutsamsten Akteure sind (Klerks, 2001). Darüber hinaus sind Lücken und Fehler in Daten in dieser Domäne häufig nicht zufällig- oder normalverteilt, wie man das sonst oft bei fehlenden Daten zu einer Population annimmt, sondern systematisch verteilt. Das liegt unter anderem daran, dass Befragte in Ermittlungen die Angaben zu ihrer Person absichtlich und nach bekannten Mustern variieren (Sparrow, 1991; Wang et al., 2004). Überdies wurden die meisten Methoden, Maße und Softwareprogramme in der ASN zur retrospektiven sozialwissenschaftlichen Analyse von Netzen mit wenigen Knoten- und Kantentypen entwickelt (Krebs, 2002). Für Exekutivorgane spielen jedoch die Früherkennung und Vermeidung von Gefahren sowie die Echtzeitanalyse von Daten oft keine geringere Rolle als Fahndung und Ermittlung (Chibelushi et al., 2006).

1.4 Rechnergestützte Modellierung und Simulation

Rechnergestützte Modellierung und Simulation dienen unter anderem der Exploration möglicher Szenarien (was wäre wenn?), der Untersuchung von Grenz- und Extremwerten, und der Durchführung systematischer Experimente zu Entstehung und Verhalten komplexer und dynamischer Systeme. Komplexität bedeutet hier das Entstehen nichtlinearen Verhaltens durch das Zusammenwirken einfacher Prinzipien und Aktivitäten, wie z.B. exponentiellem positivem und negativem Wachstum (Gilbert und Troitzsch, 2005; Sterman 2000). Die Beschreibung der dabei entstehenden Systeme erfordert Konzepte, die nicht zur Beschreibung der zugrundeliegenden Systemkomponenten nötig sind. Angewandt auf den Bereich der Kriminalität heißt das, dass die exakte Kenntnis über die Merkmale und das Verhalten einzelner Personen keinen zwangsläufigen Schluss auf das Verhalten einer kriminellen Gruppe zulässt. Überdies argumentieren Brantingham et al. (1993), dass Kriminalität nicht in diskrete Elemente oder Beziehungen zerlegbar ist und zudem eine hohe Anzahl sich gegenseitig beeinflussender Faktoren involviert. Daher eignen sich parametrische statistische Verfahren nicht als Analysemethode. Zudem folgen Netzwerkformierungen nicht der Normalverteilung, so dass Zufallsstichproben und darauf basierende statistische Verfahren wie die multivariate Regression ebenfalls ungeeignet sind (Malm et al., 2008). Modellierung und Simulation schaffen hier Abhilfe, da sie es ermöglichen, die nichtlineare Natur komplexer Systeme systematisch zu untersuchen.

Short et al. (2008) präsentieren ein Modell für die Entstehung und Dynamik von *hot spots*, also Orten, an denen Einbrüche und Diebstähle verübt werden, und in deren Nähe oft Wiederholungstaten stattfinden. Die Analyse des Verhaltens des Modells über die Zeit, kurz Simulation, gibt Einblick in die Wechselwirkungen zwischen den Variablen und die dabei entstehenden Kriminalitätsmuster. Enders und Su (2007) modellieren, wie sich Terroristen an Anti-Terror-Maßnahmen anpassen: Nach den Terroranschlägen vom 11. September 2001 in den USA (9/11) änderte die US-Regierung ihre Strategien zur Fahndung nach Terroristen. Daraufhin wich al-Qaida auf weniger koordinierte und ausgeklügelte Angriffe aus, wie z.B. die Bombenanschläge auf die Madrider S-Bahn im März 2004. Ein abschließendes Beispiel für diese Methodengruppe sind von der US-amerikanischen Steuerbehörde geförderte Simulationen, mit denen die Diffusion von Steuerbetrugsmustern in der Bevölkerung nachvollzogen werden soll (Carley und Maxwell, 2006).

Die in diesem Beitrag vorgestellten Familien von Methoden werden zunehmend um Verfahren aus der Statistik, der künstlichen Intelligenz, und dem maschinellen Lernen erweitert (siehe dazu z.B. Popp und Yen 2006; Skillicorn 2009). Solche Verfahren dienen im Bereich der Kriminalitätsforschung unter anderem bereits als Grundlage des Data Minings, und werden als eine von mehreren Komponenten in der ASN und der Modellierung und Simulation eingesetzt (National Research Council, 2008).

2 Unterbereichen von Kriminalität aus dem Blickwinkel der Netzwerkanalyse

Der folgende Abschnitt gibt einen netzwerkorientierten Überblick über einige Unterbereiche von Kriminalität. In der Realität können sich diese Bereiche überschneiden,

wie z.B. die Wirtschaftskriminalität mit der grenzüberschreitenden Kriminalität. Die Nutzung moderner Informations- und Kommunikationstechnologien für gesetzwidrige Zwecke, kurz Cyber-Kriminalität, wird hier nicht als ein eigener Bereich aufgeführt, sondern als integraler Bestandteil vieler Kriminalitätsarten verstanden. Die Rechtslage zu dieser und anderen neueren Formen von Kriminalität ist teilweise noch unklar und der Forschungsstand dünn. Ein Beispiel hierfür ist das *Trolling*, bei dem Verfasser von thematisch abweichenden Kommentaren in Internetforen die Normen und Werte anderer Personen herausfordern („for the lulz") (Schwartz, 2008). Die daraus resultierenden Auseinandersetzungen werden mitunter in die „reale" Welt getragen. So z.B. bei den Protesten vor Scientology Einrichtungen in verschiedenen Ländern in 2008, deren Planung durch *Anonymous* ursprünglich mit dem Bilderboard *4chan* in Verbindung stand.

2.1 Gangs und Gemeinsames Begehen von Straftaten (Co-offending)

Organisierte Kriminalität kann mit verschiedenen Organisationsformen von Gruppen in Verbindung stehen. Eine dieser Formen ist das uneinheitlich definierte Konzept der *Gang*. Eine verbreitete Definition von Gangs sind lose, nicht-hierarchisch organisierte Gruppen von verschiedener Größe, die in einem bestimmten Gebiet ein breites Spektrum von Delikten und Straftaten begehen, mindestens ein Jahr lang bestehen und eine gruppenspezifische Art von Kommunikation und Symbolik benutzen (Reiss, 1988; Sarnecki, 2001). Der innere Zusammenhalt von Gangs ist niedrig. Das liegt unter anderem an der hohen Fluktuationsrate in der Mitgliederbasis, dem sehr kleinen Set an Gruppennormen, und dem Fehlen einer klaren Führerschaft (ebd.). Gangs werden hauptsächlich durch externen Druck zusammengehalten, wie z.B. Konflikte mit anderen Gangs oder sozioökonomische Zwänge. Daher scheint die nachhaltige Schwächung von Gangs durch das Eindämmen dieser externen Kräfte sinnvoll (Klein und Crawford, 1967). Ein mehrfach beobachtetes Merkmal großer Gangs (200 und mehr Mitglieder) ist ein kleiner Kern aktiver Mitglieder (30 bis 40 Personen), die sich wiederum in kleineren Cliquen von fünf bis zehn Mitgliedern organisieren (Klein und Crawford, 1967; Sarnecki, 2001). Ist die Identität von Gangmitgliedern bekannt, können Interventionen in Abhängigkeit der Netzwerkposition erfolgreich sein (McGloin, 2005): Cut points eignen sich beispielsweise, um abschreckende Nachrichten effektiv unter den Mitgliedern zu verbreiten. Die hier genannten Merkmale und Definition von Gangs greifen nicht für alle Gangs – beispielsweise nicht für straffer organisierte Street Gangs in Los Angeles, auf die hier aber nicht näher eingegangen wird.

Die Mehrzahl der an Gruppendelikten beteiligten Personen sind nicht in Gangs organisiert (Sarnecki, 2001). Weit üblicher als Gangs sind ephemere Verbindungen von zwei bis vier Tätern (*co-offender*), die Netzwerke als Organisationsform wie auch Form des Handelns wählen (Waring, 2002). Analysen polizeilicher Daten haben gezeigt, dass weniger als 20% der registrierten Täter stets oder nie alleine handeln, während etwa zwei Drittel der Täter mal in Gruppen und mal allein Straftaten verüben (Reiss, 1988; Sarnecki, 2001). „Co-offending" Beziehungen überdauern oft nicht mehr als eine Straftat und spiegeln somit den Fakt wider, dass generell rund drei Viertel aller Täter nicht mehr als einmal straffällig werden (Sarnecki, 2001). Größe und Struktur von co-offending Netzwerken sind abhängig vom Beobachtungszeitraum: Sarneckis Netzwerkanalyse aller

co-offending Beziehungen, die die Stockholmer Polizei über einen Zeitraum von fünf Jahren in den 1990ern registriert hatte, zeigte eine core-periphery Struktur. In deren Kern fanden sich lediglich 20% aller Knoten, aber 83% aller Kanten, 39% aller Straftaten und 95% der am schwersten Kriminellen wieder. Das gemeinsame Ausführen von Straftaten hat Einfluss auf das persönliche Kriminalitätsverhalten: Gemeinschaftstäter begehen mehr und schwerere Verbrechen als Einzeltäter und beginnen ihre kriminelle Laufbahn früher. Aus den genannten Gründen sind Maßnahmen der Exekutivorgane, die auf Abschreckung Einzelner zielen, nur dann effektiv, wenn es sich um permanente Einzeltäter handelt, oder um co-offender, auf die das „Anwerber" Profil passt (Reiss, 1988; Sarnecki, 2001). Diese Anwerber sind Schwerkriminelle, die eine Vielzahl von Straftaten gemeinsam mit einer Vielzahl von verschiedenen jüngeren Partnern ausüben. Die Forschung zu gemeinsamer Täterschaft hat weiterhin gezeigt, dass mit Ausnahme des Wehrdienstes die Verlagerung von Tätern an andere Orte nicht zwangsläufig die Chance auf weitere Straftaten reduziert, da co-offender an neuen Orten ihren Pool an möglichen Mittätern erweitern können. Soziale Mobilität hingegen, wie z.B. in Form von Ausbildung, Arbeitsstelle und Familiengründung, ließen viele Täter von weiteren Verbrechen absehen (Reiss, 1988; Sarnecki, 2001). Einen ähnlichen Zusammenhang zwischen der Stärkung sozialer Mobilität und der Reduktion von Kriminalität beobachtete Ianni (1972) auch für Mafias in den USA: Italienische Immigranten mit niedrigem sozioökonomischem Status organisierten sich zunächst in Mafias und verdienten durch illegale Geschäfte ein (Neben-)Einkommen (Ianni und Reuss-Ianni, 1972). Als ihre Nachkommen aufgrund regulärer Ausbildung besser bezahlte und einflussreichere Stellen in der legalen Welt als in der Mafia bekommen konnten, verließen sie mitunter die Mafia und gliederten sich in die amerikanische Gesellschaft ein. Ihre illegalen Tätigkeiten wurden häufig von Gruppen mit niedrigerem sozioökonomischem Status übernommen; oft Latein- und Afro-Amerikanern. Ianni stellte zudem fest, dass Mafias in den USA zumeist keine großen, national und hierarchisch organisierten Gruppen sind, und dass Autoritätsverhältnisse und Netzwerkpositionen in der Mafia die Familien- und Verwandtschaftsbeziehungen der Mitglieder widerspiegeln. Insgesamt generalisieren Forscher im Bereich der Gangs und co-offending Netzwerke auf Grund empirischer Befunde, dass die generelle Form solcher kriminellen Gruppierungen über verschiedene Zeiträume und Orte hinweg relativ stabil bleibt, die Identität von Knoten und Kanten jedoch häufig und schnell wechselt.

2.2 Umfeldkriminologie (Environmental criminology)

Ausgehend von der empirischen Beobachtung, dass Gesetzeswidrigkeiten oft räumliche und zeitliche Muster aufweisen, untersucht die Umfeldkriminologie den Zusammenhang zwischen Tat, Täter und physischer Umwelt (Brantingham und Brantingham, 1993). Der Begriff *Umfeldkriminologie* ist nicht etabliert; wir führen ihn hier in Anlehnung an den englischen Begriff *environmental criminology* ein. Übertragen in Netzwerkkonzepte werden in der Umfeldkriminologie die Täter, Opfer und Angriffsziele als Knoten repräsentiert, und die Wege der Täter zu und zwischen diesen Punkten als Kanten. Malm et al. (2008) zeigen, wie netzwerkanalytische Zentralitätsmaße zur Erklärung der Distanz der zurückgelegten Wege zwischen den Beteiligten in einem Drogenproduktions- und Absatznetzwerk in Vancouver, Kanada, genutzt werden können. Im Gegensatz dazu boten

soziodemographische Angaben zu den Komplizen keinen solchen Erklärungsgehalt. Die Autoren der Studie schlagen vor, wie Exekutivorgane aus solchen Forschungsergebnissen Informationen zu den beteiligten Akteuren entnehmen können: Personen von zentraler Bedeutung legen die längsten Wege zu ihren Komplizen zurück. Das liegt daran, dass die Drogenproduktionsstätten und die Wohnungen der meisten Beteiligten nahe beieinander liegen, sich beide aber weit entfernt befinden von den Aufenthaltsorte der zentralen Akteure, die zudem in vergleichsweise wohlhabenderen Stadtteilen lokalisiert sind.

Die Umfeldkriminologie nutzt netzwerkanalytische Ansätze noch selten. Dominierende Methoden zur Erforschung zeitlicher und räumlicher Muster von Straftaten sind die Analyse von Umfeldvariablen sowie Simulationen (Brantingham und Brantingham, 1993; Short et al., 2008): Verkürzend gesagt geschieht eine Straftat dann, wenn eine zu einer Straftat bereite Person innerhalb ihres alltäglichen und vertrauten Aktionsraumes ein geeignetes Angriffsziel, aber keine Überwachungsmaßnahmen vorfindet. Die meisten der daraus resultierenden Verbrechen sind hochgradig opportunistisch. Diese können nach Meinung der Umfeldkriminologen durch städtebauliche Maßnahmen eingeschränkt werden, wie z.B. der Verhinderung starker sozioökonomischer Differentiale zwischen Stadtvierteln, das Umwandeln von Durchfahrtsstraßen in Sackgassen, unregelmäßige statt gitterförmige Straßennetze, und Überwachungsmechanismen wie Kameras und nachbarschaftliche Organisationen in Wohngebieten.

Für opportunistische Gruppendelikte wurde die in der ASN weit verbreitete Annahme der homophily („gleich und gleich gesellt sich gern“, McPherson et al., 2001) mehrfach empirisch bestätigt: Täter ähneln sich untereinander oft hinsichtlich ihres Wohnortes, Geschlechts, Alters, und kriminellen Erfahrungsgrades, und in Europa weniger als in Nordamerika auch in ihrem ethnischen Hintergrund (Sarnecki, 2001). Je geplanter eine Tat jedoch ist, wie z.B. Raubüberfälle und Beschaffungskriminalität, umso unterschiedlicher können Mittäter hinsichtlich ihrer persönlichen Merkmale sein: Malm et al. (2008) können die homophily Annahme für ein Drogenproduktionsnetz weder hinsichtlich des Geschlechts noch des ethnischen Hintergrundes der Beteiligten bestätigen. Die merkmalsbasierte Ähnlichkeit von Gemeinschaftstätern, die zudem eine geringe graphentheoretischer Distanz ausweisen, kann somit Exekutivorganen einen Hinweis auf die Art der Organisation einer Tat geben.

2.3 Grenzüberschreitende Kriminalität

Frei zugängliche, netzwerkorientierte Publikationen zu grenzüberschreitender Kriminalität gehören hauptsächlich zur Methodengruppe der Netzwerkbeschreibungen. Ziele internationaler Kriminalität sind vorwiegend Profit sowie sozialer und politischer Einfluss (Jamieson, 2001). Die Entwicklung illegaler Strukturen hin zu verstärkt transnationalen, deregulierten und geographisch verstreuten Netzwerken von verschiedenster Form, Größe, Stabilität und Konzentration wurde seit den 1990er Jahren unter anderem durch folgende Faktoren begünstigt: Genauso wie legale Organisationen auch, profitieren illegale Netze von der Öffnung, Globalisierung und Privatisierung der Märkte, der Standardisierung von Produkten und Prozessen und der freien Verfügbarkeit von Vernetzung und technologischen Innovationen, wie z.B. in der Kryptographie und *Steganographie*, also

dem Verstecken von Informationen z.B. in Bildern (Williams, 2001). Diese Faktoren fördern eine Atmosphäre der Anonymität, schnelle und flexible Transaktionen und das Ausnutzen unterschiedlicher Rechtssysteme (Curtis und Karacan, 2002). Illegale Strukturen sind darüber hinaus durch das Einsparen versunkener Kosten wie Firmenzentralen schneller anpassungsfähig und mobiler als viele legale Organisationen.
Eine neue globale Dynamik in der grenzüberschreitenden Kriminalität ergab sich weiterhin durch die politische Wende, die 1989 in Osteuropa und Russland einsetzte (Berry et al., 2003; Jamieson, 2001): Große Bestände an Waffen, vor allem aus der ehemaligen Sowjetunion und Jugoslawien, wurden teilweise ohne strikte staatliche Überwachung und Zollkontrollen umverteilt. Ehemals staatlich finanzierte Krimnelle suchten sich neue Auftraggeber und Kunden. Nationale Gesetze gegen Kriminalität und Korruption wurden nicht in allen Ländern gleichstark durchgesetzt.

Eine besondere Herausforderung für Exekutivorgane sind strategische Allianzen zwischen mehreren kriminellen Gruppen, wodurch Risiken breiter verteilt werden, sowie zwischen kriminellen und legalen Organisationen, was zur Reduktion von Risiken führen kann. So zahlt beispielsweise die kolumbianische FARC für die Waffen, die sie von der nordirischen IRA und der spanischen ETA erhalten, in Drogen, welche wiederum von Drogenkartellen gegen Waffen aus Osteuropa oder Diamanten aus Afrika gehandelt werden (Curtis und Karacan, 2002). Effektive Maßnahmen zur Verhinderung international operierender krimineller Netze sind z.B. die gezielte Bekämpfung von Korruption auf allen Ebenen der Gesellschaft, strenge Kontrollen an Grenzen, Häfen und Flughäfen, effiziente Koordination zwischen Exekutivorganen über Landesgrenzen hinweg, und die moderate Umgestaltung der klassisch-hierarchischen Organisationsform von Exekutivorganen hin zu mehr netzwerkähnlicheren Strukturen (Arquilla und Ronfeldt, 2001; Jamieson, 2001).

2.4 Wirtschaftskriminalität

Netzwerkanalysen konnten Aufschluss darüber gegeben, wie die Art und der Rang der Position, die Mitarbeiter in einer Firmen innehaben, mit deren Rolle in Fällen von Wirtschaftskriminalität zusammenhängen (Baker und Faulkner, 1993; Diesner et al., 2005). Im Gegensatz zu legalen Firmenaktivitäten bedarf illegales Wirtschaften der optimalen Mischung aus Effizienz und Verschleierung. Diese Mischung kann unter anderem erreicht werden durch das Ersetzen persönlicher Treffen mit mittelbarer Kommunikation, die Minimierung des Kommunikationsvolumens und von Redundanz, der Dezentralisierung und gegenseitigen Abschottung der involvierten Akteure und der personellen Trennung von Planung und Ausführung. Baker und Faulkner (1993) stellten bei die Analyse eidesstattlicher Zeugenaussagen, die im Zuge von Prozessen gegen Preisabsprachen in der elektrotechnischen Industrie in den USA in den 1950er Jahren erfasst wurden, fest, dass die Konspiration im Falle von preisgünstiger und standardisierter Massenware zu schwach verlinkten, dezentralen Strukturen führte. Unter diesen Umständen trafen sich die Führungskräfte der involvierten Firmen nur selten und nur dann, wenn sie koordinierte Entscheidungen treffen mussten, deren Implementierung sie dann an Mitarbeiter in niedrigeren Positionen delegierten. Die resultierende Dezentralisierung schützte zunächst kriminelle Entscheider. Kam es aber zum Prozess, wurde die Mehrzahl von ihnen schuldig gesprochen und erhielt höhere Strafen als Beteiligte in niedrigeren Positionen. Im

Gegensatz dazu scheint bei Preisabsprachen zu teuren Einzelanfertigungen das Bedürfnis nach Effizienz größer als das nach Verschleierung: In diesem Fall führten häufige Kommunikation und enge Koordinierung zu einem zentralisierten Netz mit einem kleinen, dichten Kern. Unter diesen Umständen wurde ein prozentual geringerer Anteil von Personen für schuldig befunden, diese aber unabhängig von ihrer Position gleichhoch bestraft.

Diesner et al. (2005) zeigten mit der Netzwerkanalyse der Emails, die im Zuge der staatlichen Ermittlungen gegen den Enron Konzern veröffentlicht wurden, wie jobspezifische, interpersonelle und firmenweite Kommunikationsmuster mit der Entwicklung der Firmenkrise zusammenhingen. Die Autoren fanden weiterhin, dass sich die aus Emailköpfen gewonnen sozialen Netze und die aus Emailtexten extrahierten semantischen Netze in ihrer Dynamik mitunter gegenläufig verhielten und Aufschluss über verschiedene Aspekte von unlauteren Aktivitäten geben können. Diesner et al. (2005) empfehlen daher, explizite Angaben zu Relationen zwischen Einheiten mit zusätzlichen Informationen zu Netzwerken, die explizit oder implizit in unstrukturierten Textdaten enthalten sind, anzureichern.

2.5 Terrorismus

Seit 9/11 ist die Zahl der Publikationen zu Terroristennetzwerken sprunghaft angestiegen. Ziel der Terroristen ist heute nicht mehr nur das kurzfristige Erregen breiter Aufmerksamkeit, sondern auch das langfristige Verbreiten des Memes[2] Angst (Enders und Su, 2007; Ressler, 2006). Terrorgruppen von heute sind, wie z.B. al-Qaida, als dezentrale, disperse Netze von geringer Dichte strukturiert, oder als Hybrid aus Hierarchie und Netz, wie z.B. Hamas. Dadurch sind sie flexibel, anpassungsfähig und strukturbedingt belastbar. Weiterhin nutzen diese Gruppen moderne IKT professionell zur Organisation, Kommunikation, Verschleierung und Rekrutierung von Mitgliedern, Öffentlichkeitsarbeit, und Planung und Ausführung von Attacken (Popp et al., 2004; Zanini und Edwards, 2001). Ihre zentralen Führer sind, wenn es diese überhaupt gibt, weniger ein strategisches Ziel der Gegenwehr als Personen, die hinsichtlich ihres Wissens, Könnens oder Leitens von relevanten Informationen eine Einzelstellung innehaben. Terroristen formen möglichst wenige Verbindungen in legale Kreise hinein und nutzen schwache Kanten so selten, dass diese nahezu inexistent scheinen (Krebs, 2002). Starke Verbindungen zwischen den Zellen werden möglichst selten und über ungewöhnlich lange Wege aktiviert, so dass diese von Außenseitern als schwache Kanten fehlinterpretiert werden können. Die Ausführer einer Attacke sind in schwach verlinkten Zellen organisiert, welche von einem größeren, darunterliegenden Netzwerk stets neu formiert und aktiviert werden können (Rodríguez, 2004).

Die zeitgemäße Analyse von Terrornetzen bedarf einer Kombination von mehreren Methoden (Carley et al., 2007; Chen et al., 2008; Popp et al., 2004; Skillicorn, 2008): Große Mengen von Rohdaten aus verschiedenen Quellen liegen verschiedenen Behörden meist in Textform vor. Diese Daten müssen zunächst konsolidiert, übersetzt und nach relevanten Dokumenten und Angaben gefiltert werden. Dann gilt es, relevante Knoten zu identifizieren, disambiguieren, klassifizieren, extrahieren, und schließlich zu verlinken. Es

[2] Meme sind ein Stück Kultur dass in der Gesellschaft generiert und reproduziert wird (Dawkins 1976).

folgt die Analyse der relationalen Daten. Visualisierungen dienen dabei der heuristischen Exploration der Daten. Anschließende Simulationen können helfen, mögliche Zukunftsszenarien zu explorieren. Die gesammelten Daten können zudem als Input für maschinelle Lernverfahren dienen. Schließlich gilt es, die gewonnenen Einsichten kompetent zu evaluieren, interpretieren und als eine mögliche Entscheidungshilfe zu nutzen.

Es wurde vielfach argumentiert, dass es den Exekutivorganen im Vorfeld von 9/11 nicht an relevanten Informationen mangelte, sondern an der qualifizierten und auch netzwerkanalytischen Auswertung der Daten (Arquilla und Ronfeldt, 2001; Xu und Chen, 2005). Popp et al. (2004) generalisieren weiter, dass Exekutivorgane zuviel Zeit mit dem Suchen nach und Aufbereiten von Informationen sowie dem Anfertigen von Berichten zubringen. Daher bleibt ihnen zuwenig Zeit zur Analyse der Daten und zur Zusammenarbeit mit in- und ausländischen Kollegen. In der Behebung dieser Diskrepanz könnte der informierte Einsatz moderner Analysemethoden und entsprechender Technologien eine entscheidende Rolle spielen (ebd.).

3 Sicherheit versus dem Schutz persönlicher Daten

Die Prävention von Kriminalität ist ein zweischneidiges Schwert: Ziel der Exekutivorgane und Wunsch der Bürger ist es, möglichst viele Anschläge bzw. β–Fehler sowie das fälschliche Verdächtigen Unschuldiger bzw. α–Fehler zu vermeiden. Das Recht von Privatpersonen schließt, je nach Staat, beispielsweise das Recht auf informationelle Selbstbestimmung, freie Meinungsäußerung und den Schutz vor staatlicher Überwachung ein. Da von vornherein oft unklar ist, wer kriminell ist und wer nicht, gilt es, den Pool an Personen, zu denen Daten erfasst werden, sowie beide Arten von Fehlern mittels rechtlicher, methodischer und technischer Lösungen zu minimieren. Solche Lösungen sind z.B. das Anonymisieren von Rohdaten (Sweeney, 2002), das Beschränken unspezifischer Suchen auf anonymisierte Daten und die klare Trennung von Datenanalyse und Strafahndung (Taipale, 2003). Zudem sind klare Gesetze sowie Prüf- und Kontrollmechanismen für das Auslösen einer Suche in personenbezogenen Daten, das schrittweise Zusammenführen von Daten aus unterschiedlichen Quellen wie z.B. Bank- und Polizeidaten und das Verbinden von Verhaltensdaten mit der Identität von Personen unabdingbar (ebd.)

Überdies ist es unerlässlich, Methoden und Programme, die im Einsatz sind oder deren Einsatz geplant ist, regelmäßig und systematisch zu evaluieren (Harper und Harris, 1975). Data Mining Techniken, die ursprünglich für den kommerziellen Sektor entwickelt wurden und erfolgreich im Marketing eingesetzt werden, können nicht ohne weiteres auf die Erforschung von Kriminalität übertragen werden, und auf die Untersuchung von Terrorismus möglicherweise gar nicht (National Research Council, 2008). Das liegt unter anderem daran, dass Daten zu Kriminalität oft unvollständiger und fehlerhafter sind als Daten für kommerzielle Anwendungen. Zudem liegen nicht immer präzise und empirisch bestätigte Angaben zur Robustheit der Methode gegenüber Schwankungen in der Datenqualität vor. Schließlich weisen Kriminalitätsforscher darauf hin, dass bei der Analyse von personenbezogenen Daten klar zwischen erforschenden versus beweisenden

Verfahren zu unterscheiden ist, Konfidenzintervalle korrekt zu interpretieren sind, und probabilistische Ergebnisse keine deterministische Deutung zulassen.

4 Ausblick

Zusammenfassend zum Einsatz der Netzwerkanalyse in der Kriminalitätsforschung schlagen wir vor, die Aussage "Countering terrorism, at its core, is about managing information" (Golbeck et al. 2006: 125) zu verallgemeinern: Die Untersuchung und Verhinderung von Kriminalität sind in ihrem Kern Aufgaben im Bereich des Informationsmanagements; inklusive entsprechender Methoden, Technologien und Evaluationen. Wir schließen mit einem Zitat, dass Simmel (1908: 260) ursprünglich in Bezug auf Geheimbünde äußerte, dass aber auch die zeitlose Bedeutsamkeit der exakten Analyse kriminalitätsrelevanter Phänomene sowie die Überprüfung und Veröffentlichung entsprechender Ergebnisse betont: „In viel weiterem Umfange, als man sich klar zu machen pflegt, ruht unsre moderne Existenz von der Wirtschaft, die immer mehr Kreditwirtschaft wird, bis zum Wissenschaftsbetrieb, in dem die Mehrheit der Forscher unzählige, ihnen gar nicht nachprüfbare Resultate anderer verwenden muss, auf dem Glauben an die Ehrlichkeit des andern."

5 Literaturverzeichnis

Arquilla, John und *David F. Ronfeldt*, 2001: The Advent of Netwar (Revisited). S. 1-25 in: *John Arquilla* und *David F. Ronfeldt* (Hg.), Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: RAND.

Baker, Wayne E. und *Robert F. Faulkner*, 1993: The Social Organization of Conspiracy: Illegal Networks in the Heavy Electrical Equipment Industry. American Sociological Review 58(6): 837-860.

Berry, Laverle, Glenn E. Curtis, John N. Gibbs, Rex A. Hudson, T. Karacan, N. Kollars und *R. Miro*, 2003: Nations Hospitable to Organized Crime and Terrorism. Washington D.C.: Library of Congress.

Brantingham, Patricia L. und *Paul J. Brantingham*, 1993: Nodes, Paths and Edges: Considerations on the Complexity of Crime and the Physical Environment. Journal of Environmental Psychology 13(1): 3-28.

Carley, Kathleen M., Jana Diesner, Jeffrey Reminga und *Maksim Tsvetovat*, 2007: Toward an interoperable dynamic network analysis toolkit. Decision Support Systems. 43(4): 1324-1347.

Carley, Kathleen M., Ju Sung Lee und *David Krackhardt*, 2001: Destabilizing networks. Connections 24(3): 31-34.

Carley, Kathleen M. und *Dan T. Maxwell*, 2006: Understanding taxpayer behavior and assessing potential IRS interventions using multiagent dynamic-network simulations. Proc. of Internal Revenue Service (IRS) Research Conference, Washington D.C..

Chen, Hsinchun, Wingyan Chung, Jialun Qin, Edna Reid, Marc Sageman und Gabriel Weimann, 2008: Uncovering the Dark Web: A case study of Jihad on the Web. Journal of the American Society for Information Science and Technology 59(8): 1347-1359.

Chibelushi, Caroline, Bernadette Sharp und *Hanifa Shah*, 2006: ASKARI: A Crime Text Mining Approach. S. 155-174 in: *Panagiotis Kanellis*, *Evangelos Kiountouzis, Nicholas Kolokotronis* und *Drakoulis Martakos* (Hg.), Digital Crime and Forensic Science in Cyberspace. Hershey, PA: Idea Group.

Curtis, Glenn E. und *Tara Karacan*, 2002: The Nexus among Terrorists, Narcotics Traffickers, Weapons Proliferators, and Organized Crime Networks in Western Europe. Washington, D.C.: Library of Congress.

Davis, Roger H., 1981: Social network analysis: An aid in conspiracy investigations. FBI Law Enforcement Bulletin 50(12): 11-19.

Dawkins, Richard, 2006: The selfish gene. Oxford: Oxford University Press.

Denning, Dorothy E., 2001: Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. S. 239-288 in: *John Arquilla* and *David F. Ronfeldt* (Hg.), Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: RAND.

Diesner, Jana, Terrill Frantz, und *Kathleen M. Carley, 2005*: Communication Networks from the Enron Email Corpus "It's Always About the People. Enron is no Different". Journal of Computational and Mathematical Organization Theory, 11(3): 201-228.

Enders, Walter und *Xuejuan Su*, 2007: Rational Terrorists and Optimal Network Structure. Journal of Conflict Resolution 51(1): 33-57.

Erickson, Bonnie H., 1981: Secret Societies and Social Structure. Social Forces 60: 188-210.

Gilbert Nigel und *Klaus G. Troitzsch*, 2005: Simulation for the Social Scientist. Maidenhead: Open University Press.

Golbeck, Jennifer, Aaron Mannes und *James Hendler*, 2006: Semantic Web Technologies for Terrorist Network Analysis. S. 125-137 in: *Robert L. Popp* und *John Yen* (Hg.), Emergent Information Technologies and Enabling Policies for Counter-Terrorism. Wiley-IEEE Press.

Granovetter, Mark S., 1973: The Strength of Weak Ties. American Journal of Sociology 78(6): 1360-1380.

Harper, Walter R. und *Douglas H. Harris*, 1975: The application of link analysis to police intelligence. Human Factors 17(2): 157-164.

Howlett, James B., 1980: Analytical Investigative Techniques: Tools for Complex Criminal Investigations. Police Chief 47: 42-45.

Ianni, Francis und *Elizabeth Reuss-Ianni*, 1972: A Family Business: Kinship and Social Control in Organized Crime. New York, NY: Russell Sage Foundation.

Jamieson, Alison, 2001: Transnational Organized Crime: A European Perspective. Studies in Conflict and Terrorism 24(5): 377-387.

Klein, Malcolm W. und Lois Y. Crawford, 1967: Groups, Gangs, and Cohesiveness. Journal of Research in Crime and Delinquency 4(1): 63-75.

Klerks, Peter, 2001: The network paradigm applied to criminal organizations: theoretical nitpicking or a relevant doctrine for investigators. Connections 24(3): 53-65.

Krebs, Valdis, 2002: Mapping networks of terrorist cells. Connections 24(3): 43-52.

Malm, Aili, Brian Kinney und *Nahanni Pollard*, 2008: Social Network and Distance Correlates of Criminal Associates Involved in Illicit Drug Production. Security Journal 21(1-2): 77-94.

McGloin, Jean M., 2005: Street Gangs and Interventions: Innovative Problem Solving with Network Analysis. Washington, D.C.: US Department of Justice, Office of Community Oriented Policing Services.

McPherson, Miller, Lynn S. Lovin und *James M. Cook*, 2001: Birds of a Feather: Homophily in Social Networks. Annual Review of Sociology 27: 415-444.

National Research Council, 2008: Protecting Individual Privacy in the Struggle Against Terrorists. Washington, D.C.: The National Academies Press.

Pehl, Dirk, 2008: Die Implementation der Rasterfahndung: Eine Empirische Untersuchung zur Anwendung, Umsetzung und Wirkung der Gesetzlichen Regelungen zur Operativen Informationserhebung durch Rasterfahndung. Berlin: Max-Planck-Institut.

Popp, Robert L., Thomas Armour, Ted Senator und *Kristen Numrych*, 2004: Countering terrorism through information technology. Communications of the ACM 47(3): 36-43.

Popp, Robert L. und *John Yen* (Hg.) (2006), Emergent Information Technologies and Enabling Policies for Counter-Terrorism. Wiley-IEEE Press.

Reiss, Albert J., 1988: Co-offending and Criminal Careers. Crime and Justice 10: 117-170.

Ressler, Steve, 2006: Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research. Homeland Security Affairs 2(2).

Rodríguez, Jose A., 2004: The March 11th Terrorist Network. Paper presented at VIII Congreso Español de Sociología, September 2004, Alicante, Spanien.

Sarnecki, Jerzy, 2001: Delinquent Networks: Youth Co-Offending in Stockholm. Cambridge, UK: Cambridge University Press.

Schwartz, Matthias, 2008: The Trolls Among Us. The New York Times, August 03, 2008, S. MM24.

Short, Martin B., Maria R. D'Orsogna, Virginia B. Pasour, George E. Tita, Paul J. Brantingham, Andrea L. Bertozzi und *Lincoln B. Chayes*, 2008: A Statistical Model of Criminal Behavior. Mathematical Models and Methods in Applied Science 18: 1249-1267.

Simmel, Georg, 1908: Das Geheimnis und die geheime Gesellschaft. S. 256-304 in: *Georg Simmel*, Soziologie. Untersuchungen über die Formen der Vergesellschaftung, Leipzig, Berlin: Duncker & Humblot.

Skillicorn, David, 2008: Knowledge Discovery for Counterterrorism and Law Enforcement. Boca Raton und andere: CRC Press.

Sparrow, Malcolm K., 1991: The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects. Social Networks 13(3): 251-274.

Sterman, John, 2000: Business Dynamics: Systems Thinking and Modeling for a Complex World. Homewood, IL: Irwin/ McGraw-Hill.

Sweeney, Latanya, 2002: k-Anonymity: A Model for Protecting Privacy. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems 10(5): 557-570.

Taipale, Kim A., 2003: Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data. Columbia Science and Technology Law Review 5(2): 1-83.

Wang, Gang, Hsinchun Chen und *Homa Atabakhsh*, 2004: Automatically detecting deceptive criminal identities. Communications of the ACM 47(3):70-76.

Waring, Elin, 2002: Co-Offending as a Network Form of Social Organization. S. 31-47 in: *Elin Waring* und *David Weisburd* (Hg.), Crime & Social Organization, New Brunswick, NJ: Transactions Publishers.

Williams, Phil, 2001: Transnational Criminal Networks. S. 61-97 in: *John Arquilla* und *David F. Ronfeldt* (Hg.), Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: RAND.

Xu, Jennifer und *Hsinchun Chen*, 2005: Criminal network analysis and visualization. Communications of the ACM 48(6): 100-107.

Zanini, Michelle und *Sean Edwards*, 2001: The Networking of Terror in the Information Age. S. 29-60 in: *John Arquilla* und *David F. Ronfeldt* (Hg.), Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica, CA: RAND.

Software:

Analyst's Notebook (http://www.i2.co.uk/products/analysts_notebook)
NetMap (http://www.altaanalytics.com)

Danksagung:

Diese Publikation wurde teilweise gefördert durch die National Science Foundation (DGE-9972762), das Office of Naval Research (N00014-06-1-0921, ONR N00014-06-1-0104), das U.S. Air Force Office of Scientific Research (FA9550-05-1-0388), das Army Research Institute (W91WAW07C0063) und das Army Research Lab (20002504, DAAD19-01-2-0009). Zusätzliche Unterstützung wurde bereitgestellt vom Center for Computational Analysis of Social and Organizational Systems (CASOS), Carnegie Mellon University, Pittsburgh, PA. Die hierin

enthaltenen Ansichten und Schlussfolgerungen sind die der Autoren und sollten weder explizit noch implizit als repräsentativ für offizielle Grundsätze und Richtlinien der Sponsoren und der U.S. Regierung interpretiert werden.