Analyse extremistischer Bestrebungen in sozialen Netzwerken

Nils Böckler, Eva Groß, Mirko Allwinn, Günter Dörr, Christoph Igel, Stefan Jarolimek, Annika Pflug, Martin Steinebach, Jens Hoffmann, Kristin Weber, Kerstin Eppert, Viktoria Roth & Andreas Zick

Der Beitrag beschreibt den vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsverbund „Analyse extremistischer Bestrebungen in sozialen Netzwerken (X-SONAR)". Der Verbund erforscht extremistische Interaktions- und Eskalationsdynamiken in sozialen Onlinenetzwerken und deren Bedeutung für strafrechtlich relevante Radikalisierungsverläufe, wie beispielsweise in der Planung und für die Durchführung von extremistischen Gewalttaten. Ziel ist es unter anderem, ein Modell zur Risikoeinschätzung und Gewaltprävention abzuleiten sowie einen Demonstrator für ein softwaregestütztes Instrument zu entwickeln, das von Endnutzern/-innen aus Sicherheitsbehörden und Zivilgesellschaft zum anlassbezogenen Monitoring extremistischer Agitation in virtuellen Kontexten genutzt werden kann.

1. Aktueller gesellschaftlicher und politischer Bezug/ Kontextualisierung

Die Präsenz extremistischer und menschenfeindlicher Inhalte im virtuellen Raum hat innerhalb der letzten beiden Dekaden stetig zugenommen, wobei sich das Internet parallel von einem reinen Rezeptions- zu einem Interaktionsmedium entwickelt hat. Früher mussten extremistische Gruppen erhebliche Ressourcen mobilisieren, um Propagandaerfolge zu erzielen. Heute brauchen sie dazu nur wenige Klicks und kaum technische Kenntnisse, um Facebook, YouTube oder Twitter zu infiltrieren. Diese hochfrequentierten sozialen Onlinenetzwerke werden von einem Großteil der Kinder- und Jugendlichen für ihr alltägliches Informations-, Beziehungs- und Identitätsmanagement genutzt (Cortesi/Gasser 2015; Weimann 2015). Die Forschungsevidenz spricht für die These, dass das Web 2.0 es Menschen „leichter macht, im Internet auf radikale Milieus zu stoßen, in sie einzutauchen und so möglicherweise in eine gewalttätige Szene zu geraten" (Conway 2012, S. 293).

Aus sicherheitspolitischer Perspektive werden Fragen nach den Ursachen und Determinanten von Radikalisierungsprozessen im Internet spätestens dann relevant, wenn am Ende dieser Entwicklungen staatsschutzrelevante Delikte stehen. Dazu zählen unter anderem politisch motivierte Attentate durch Einzeltäter/-innen oder kleine Gruppen, die Ausreise junger Menschen nach Syrien bzw. in den Irak, Konfrontationsgewalttaten oder Brandanschläge auf Flüchtlingsheime. Die Logik sozialer Onlinenetzwerke harmoniert dabei mit dem Strategiewechsel einiger extremistischer Gruppierungen, die dazu übergegangen sind, Gewalttaten nicht mehr selbst bis ins Detail vorzubereiten, sondern vielmehr Individuen, die sich lose mit der Ideologie identifizieren, aus der Distanz zu eigenmächtigen Handlungen im Sinne der Gruppe zu bewegen (Böckler/Zick 2015). Derartige Kommunikationsprozesse konnten wiederkehrend in zeitlicher Nähe zu realweltlichen Gewalttaten beobachtet werden. Solche Täter/-innen scheinen sich zunehmend aus polizeilich nicht auffälligen Milieus zu rekrutieren.

Nicht selten lässt sich nach Attentaten, egal ob aus dem rechtsextremen oder islamistischen Spektrum, die Genese von Fan- bzw. Sympathisant/-innengruppen im Internet beobachten (Böckler et al. 2013 a). Letzteres ist auch ein Beispiel dafür, wie mühelos sich Einzelpersonen in kürzester Zeit zu sog. Bottom-up-Hategroups vernetzen können. Auch Bewegungen wie PEGIDA und HoGeSa sind über das Internet ins Leben gerufen worden und nutzen es strategisch zur Rekrutierung und Mobilisierung ihrer Mitglieder, wobei die Erhaltung und Ausbildung einer virtuellen sozialen Identität durch eine effektive Organisation zu gelingen scheint. Das Internet ist der Kontext kollektiver Radikalisierung, in dem sich Menschen unabhängig von Ort und Zeit entsprechend gemeinsamer Interessen, Einstellungen und Bedürfnisse zusammenfinden, in dem sich Emotionen aufschaukeln und Meinungen polarisieren. Gleichzeitig werden diese Diskurse damit anfällig für die Unterwanderung durch extremistische Bewegungsakteure/-innen oder Gruppen.

2. Forschungsdesiderata

In Anbetracht der herausfordernden Fragen möchte X-SONAR einen Beitrag leisten durch:

1) grundlagenwissenschaftlich begründete Phasen- bzw. Eskalationsmodelle zur Verdichtung individueller bzw. kollektiver Radikalisierungsprozesse und daraus abgeleitete praxisrelevante Indikatoren zur (a) Früherkennung sowie zur (b) dynamischen Risikoeinschätzung von Radikalisierungsprozessen im virtuellen Raum;
2) ein softwaregestütztes Instrumentarium zur (a) ressourcensparenden Analyse staatsschutz-relevanter Netzwerkstrukturen und Diskurse sowie zur (b) strukturierten Einschätzung und zum Management von individuellen wie kollektiven Radikalisierungsdynamiken;

3) die Entwicklung von Maßnahmen und Sicherheitsstrategien für (a) die Polizei wie auch für (b) zivilgesellschaftliche Akteure (bspw. durch das gezielte Setzen von Gegennarrativen im virtuellen Raum, aber auch Interventionsmaßnahmen vor Ort), um alle präventiven und interventiven Akteure besser in die Lage zu versetzen, den erkannten Radikalisierungsprozessen früh zu begegnen;
4) die Entwicklung einer Infrastruktur, um die erarbeiteten Erkenntnisse, methodischen Verfahren und Instrumente sowohl für die Fort- und Weiterbildung von Sicherheitsbehörden (LKÄ und BKA) zu nutzen als auch zivilgesellschaftlichen Endnutzern/-innen (Jugendmedienschutz, Medienunternehmen, Berufspädagogen/-innen und Schulpsychologen/-innen) zu vermitteln.

3. Ansatzpunkte des Projektes

Die automatisierte Suche und Klassifizierung von öffentlich zugänglichen Inhalten in einem dezentralen Netz wie dem Internet ist nicht nur das zentrale Geschäftsmodell zahlreicher Suchmaschinen, sondern bietet bspw. in der Forensik auch die Möglichkeit, Seiten im Internet zu sichern, zu einem späteren Zeitpunkt zu sichten, auszuwerten oder Veränderungen zu dokumentieren. Webcrawler nutzen hierzu Hyperlinks, um Webseiten nach bestimmten Inhalten durchzusuchen und Indizes für einzelne Themenbereiche zu erstellen. Sie wählen bestimmte URLs nach Themengebieten aus und laden den Inhalt der Webseite herunter. Danach wird die Webseite weiter analysiert, die Ergebnisse der Analyse werden abschließend in einem Index gespeichert und können von dort abgerufen werden. Zur Steigerung der Effizienz können die Such-, Download- und Indexierungsprozesse parallel abgearbeitet werden oder das Webcrawling kann sich auf bestimmte Themen – wie das Auffinden von islamistischer oder rechtsradikaler Propaganda – konzentrieren. Erste Ansätze, wie dies bezogen auf extremistische Inhalte geschehen kann, wurden beispielsweise von der Arbeitsgruppe um Chen (2012) aufgezeigt.

Den am Konsortium beteiligten sowie assoziierten Partnern/-innen und Endnutzern/-innen erscheint es vielversprechend, diese Ansätze weiterzuentwickeln und sie erstmalig mit dem Ansatz der Bedrohungsanalyse zu verbinden. Bedrohungsanalyse und -management fokussieren praxisnah das Erkennen risikobehafteter Verhaltensmuster und -verläufe mit dem Ziel, mögliche Bedrohungen durch Einzelpersonen und Kleingruppen zu erkennen, um dann gegebenenfalls gewaltpräventiv tätig zu werden (Meloy & Hoffmann 2014). Berufsgruppen, die bisher schon bedrohungsanalytisches Wissen in der Praxis nutzen, sind bspw. Pädagogen/-innen, Vertreter/-innen von Sicherheitsbehörden und Sozialberufen sowie Psychiater/-innen und Psychologen/-innen. Klassische thematische Anwendungsfelder des Bedrohungsmanagements (BM) sind etwa häusliche Gewalt und Stalking (Mullen et al. 2009), schwere Gewalt am Arbeitsplatz (Hoffmann/Dölitzsch 2015; White 2014), in Universitäten (Hoffmann/Timmel Zamboni 2014) und an Schulen (Böckler et al. 2013 b). In jüngsten Studien hat sich gezeigt, dass das Internet als sozialer Raum eine zunehmend bedeutsame Rolle bei der Detektion von Warnverhalten spielt. Es liegen bereits erste wissenschaftliche Ergebnisse vor, die auch zum Verständnis terroristischer Aktivitäten genutzt werden können (Borum 2015; Monahan 2012; Meloy/Yakeley 2014). In diesem Zusammenhang wurden bspw. Vorschläge für eine strukturierte Risikoanalyse formuliert, die gegenwärtig empirisch geprüft werden (Meloy et al. 2015). Zudem offenbarte sich in Studien, dass Täter vor Anschlägen markante Verhaltensauffälligkeiten im Internet zeigten (Böckler, Hoffmann & Zick 2015; Gill 2015). Erste Untersuchungen setzen dabei auf das Erkennen von Warnverhalten im digitalen Raum.

Warnverhaltensweisen beschreiben dynamische Risikofaktoren, die zu verschiedenen Zeitpunkten und in unterschiedlichen Konstellationen im Vorfeld einer schweren Gewalttat auftreten können (Hoffmann/Roshdi 2015). Als in sozialen Onlinenetzwerken auftretendes individuelles Warnverhalten wurden bislang die direkten und indirekten Andeutungen einer Straftat (Leakage), die Identifizierung mit Gewalttätern und die Fixierung auf bestimmte Themen, Konflikte und Personen benannt, die potenziell auch für automatisierte Textanalysen im Internet genutzt werden könnten (Brynielsson et al. 2013; Cohen et al. 2014). Dies sind erste Hypothesen, die umfassendere und tiefer gehende Forschungsarbeiten benötigen. Im Bereich der Radikalisierung und insbesondere der Onlineradikalisierung laufen disziplinäre Forschungsprojekte (etwa im Bereich Informatik, Soziologie, Bedrohungsmanagement) bislang isoliert nebeneinander her. Darüber hinaus finden die Forschungsbemühungen von staatlichen Behörden und universitären Einrichtungen weitestgehend getrennt voneinander statt. Die Forschung geht nur unzureichend auf die Bedürfnisse der Praxis ein und

andersherum werden die vielfältigen und grundlegenden Einsichten aus der Praxis in der Forschung nur selten zur Kenntnis genommen. Diesen Entwicklungen steuert X-SONAR entgegen, indem a) der Forschungsverbund aus interdisziplinär ausführenden Experten/-innen zusammengesetzt ist und b) die Endnutzer/-innen sowohl als Kooperationspartner/-innen als auch im Experten/-innenkreis assoziierter Partner/-innen von Projektbeginn an vertreten sind. Um die Praxisrelevanz der Projektergebnisse zu gewährleisten, ist es unabdingbar, dass ein komplexer Verbund wie X-SONAR im Rahmen seiner Arbeit zunächst den deutschen Raum fokussiert, da sowohl das Phänomen der Onlineradikalisierung als auch die Möglichkeiten, auf dieses zu reagieren, von spezifischen gesellschaftlichen Stimmungen, politischen Strukturen, rechtlichen Rahmenbedingungen und ethischen Grundsätzen abhängt. Das Projekt sieht sich daher mit komplexen Dynamiken konfrontiert, die zunächst nur konstruktiv auf nationaler Ebene bewältigt werden können. Die Projektpartner/-innen stehen jedoch im kollegialen Austausch mit Wissenschaftlern/-innen, die auf EU-Ebene zu diesem Thema forschen, und tauschen sich mit diesen aus (etwa mit dem EU-Verbund VOXPOL).

4. Konsortium und Teilvorhaben

X-SONAR wird im Forschungsverbund der folgenden sechs Institute und Einrichtungen gemeinsam umgesetzt.

Universität Bielefeld, Institut für interdisziplinäre Konflikt- und Gewaltforschung

Das Institut für interdisziplinäre Konflikt- und Gewaltforschung (IKG) koordiniert den Forschungsverbund X-SONAR. Als eine der führenden deutschen Forschungseinrichtungen im Bereich Konflikt- und Gewaltforschung bietet das IKG eine umfassende Struktur für interdisziplinäre Theorieentwicklung und empirische Forschung zu politisch und gesellschaftlich relevanten Phänomenen um Konflikte und Gewalt.

Innerhalb des Forschungsverbundes erforscht das IKG kollektive, islamistisch-dschihadistische Radikalisierung in sozialen Onlinenetzwerken sowie individueller Radikalisierungsverläufe aus soziologischer und sozialpsychologischer Perspektive. Dies geschieht in engem Austausch mit dem Teilvorhaben des LKA Niedersachsen, das den Bereich Rechtsextremismus abdeckt. Für beide Bereiche setzt das **Institut Psychologie und Bedrohungsmanagement (I:P:Bm)** als Unterauftragnehmer eine Verhaltensanalyse in Radikalisierungsverläufen um, die der Ableitung praxisrelevanter Indikatoren zur Früherkennung Vorschub leisten soll und in ein softwaregestütztes Instrument zu Risikoanalyse und Bedrohungsmanagement einfließen wird.
Verbundkoordination/Leitung:
Prof. Dr. Andreas Zick, Kerstin Eppert
(Kontakt: x-sonar@uni-bielefeld.de)
Wissenschaftliche Mitarbeit:
Viktoria Roth, Annika Hamachers, Dorian Tsolak
I:P:Bm: Dr. Jens Hoffmann, Mirko Allwinn, Nils Böckler

Landeskriminalamt Niedersachen – Kriminologische Forschung und Statistik

Der Bereich Kriminologische Forschung und Statistik (KFS) ist ein Fachstab der Behördenleitung des LKA Niedersachsen. Die Aufgaben bestehen darin, praxisbezogene kriminologische Forschung zu betreiben und wissenschaftliche Beratung aller Ebenen der Landespolizei bei kriminologischen Fragestellungen zu gewährleisten. Sie fungiert als Schnittstelle zwischen polizeilicher und gesamtgesellschaftlicher Kriminalprävention in unterschiedlichen Handlungsfeldern. Zu ihren Kernaufgaben gehören neben der Erarbeitung der polizeilichen Kriminalstatistik und anderer strategischer Lageanalysen auch die periodische Dunkelfeldstudie sowie die Durchführung von drittmittelgeförderten Forschungsprojekten.

Seit Februar 2017 forscht das Team der KFS im Rahmen des Verbundprojektes X-SONAR zu Radikalisierungsprozessen und Eskalationsdynamiken in sozialen Onlinenetzwerken. Das Teilvorhaben des LKA Niedersachsen erforscht aus sozialwissenschaftlicher Perspektive und in enger Kooperation mit dem IKG individuelle und kollektive rechtsextremistische Radikalisierung, die zu staatsschutzrelevanten Delikten führen können.
Leitung: Hartmut Pfeiffer, Dr. Eva Groß
Wissenschaftliche Mitarbeit:
Lisa Borchardt, Julia Gundlach

Deutsche Hochschule der Polizei, Fachgebiet Kommunikationswissenschaft

Die Deutsche Hochschule der Polizei (DHPOL) ist eine universitäre Spezialhochschule mit Sitz in Münster. Sie ist zuständig für die Aus- und Fortbildung des höheren Dienstes der Polizeien des Bundes und der Länder. Dabei wird besonders die Vernetzung und Verflechtung zwischen Wissenschaft und Praxis in den Fokus genommen. Neben Lehre und Fortbildung bildet die Forschung die dritte zentrale Säule der Deutschen Hochschule der Polizei. Das Fachgebiet Kommunikationswissenschaft beschäftigt sich mit der medial vermittelten bzw. öffentlichen Kommunikation mit Fokus auf den Themenbereich Polizei und Innere Sicherheit. Innerhalb des Forschungsverbundes erstellt die DHPOL eine Bestandsaufnahme und Bedarfsanalyse in den 16 Landeskriminalämtern sowie dem BKA anhand von Experteninterviews. Des Weiteren wird eine Analyse von Propaganda und Rekrutierungsmaterial aus dem islamistischen Spektrum und Fallstudien zu Dschihadreisenden (Syrien, Irak) durchgeführt sowie eine repräsentative, mehrstufige Onlinebefragung zu Regulationsmechanismen und dem öffentlichen Umgang mit Onlinepropaganda erstellt.
Leitung:
Univ.-Prof. Dr. Stefan Jarolimek
Wissenschaftliche Mitarbeit:
Kristin Weber, Jonathan Widmann

Fraunhofer-Institut für Sichere Informationstechnologie

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) hat mit seinen über 150 Mitarbeitern/-innen eine umfassende Kompetenz besonders im Umfeld der Internetsicherheit gewonnen. Bereits vor über zehn Jahren hat die Abteilung Multimediasicherheit Studien zur Verfolgbarkeit von Urheberrechtsverletzungen im Internet durchgeführt und hier unter anderem die Verfolgbarkeit von IP-Adressen diskutiert. Später wurde auf Basis dieser Kompetenzen ein öffentliches Gutachten für den Börsenverein des Deutschen Buchhandels erstellt. Die Suche im Internet wurde somit ein Kernthema der Aktivitäten, was 2010 zu der Ausgründung der CoSee GmbH führte, welche sich auf Suchdienstleistungen im Internet in Bezug auf Urheberrechtsverletzungen spezialisiert

und gemeinsam mit SIT ein umfassendes Framework zum automatisierten Zugriff auf heterogene Interneträume erstellt hat.

Im Forschungsverbund arbeitet das Fraunhofer SIT an spezifischen Webcrawlern und Instrumenten zur Risikoanalyse in Onlineinhalten sowie an der Entwicklung und Testung eines Demonstrators, der Endnutzer/-innen dabei unterstützen soll, strafrechtlich relevante rechtsradikale und islamistisch-dschihadistische Inhalte aus sozialen Onlinenetzwerken zu bewerten.
Leitung: Prof. Dr. Martin Steinebach
Wissenschaftliche Mitarbeit:
Oren Halvani, Felix Mayer, Inna Vogel, York Yannikos

Landesinstitut für Präventives Handeln (Saarland)

Das Landesinstitut für Präventives Handeln (LPH) wurde 2009 als zentrale Anlaufstelle für Präventionsfragen in der saarländischen Landesregierung gegründet. Sein Aufgabengebiet liegt in der Entwicklung und Umsetzung von Präventionsprogrammen im Bereich der Pädagogischen Prävention, der Kriminalprävention sowie der Gesundheitsförderung. Darüber hinaus beschäftigt sich das LPH intensiv mit der Erforschung von nachhaltiger Wirksamkeit verschiedenster Präventionsmaßnahmen. Durch die interdisziplinäre Ausrichtung und ressortübergreifende Vernetzung des LPH können Kompetenzen im Präventionssektor optimal gebündelt und vielfältigen Akteuren sowohl innerhalb der Landesgrenzen als auch weit darüber hinaus bedarfsgerecht zur Verfügung gestellt werden.

Im Forschungsverbund X-SONAR verantwortet das LPH – in Kooperation mit dem Deutschen Forschungszentrum für Künstliche Intelligenz (DFKI) – die Dissemination und nachhaltige Nutzung der Forschungsergebnisse. Daher wird eine umfassende deutschlandweite berufliche Weiterbildung für Fachpersonal (Sicherheitsbehörden und Zivilgesellschaft) entwickelt. Ziel des Qualifizierungsprogramms ist die Stärkung der Handlungskompetenz in der Früherkennung, Risikoeinschätzung und Gefahrenabwehr extremistischer Gewalttaten.
Leitung: Prof. Dr. Günter Dörr
Wissenschaftliche Mitarbeit:
Sonja Possinger

Deutsches Forschungszentrum für Künstliche Intelligenz GmbH, Educational Technology Lab

Das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI) mit den Standorten Kaiserslautern, Saarbrücken, Bremen, Osnabrück und Berlin ist auf dem Gebiet innovativer Softwaretechnologien die führende Forschungseinrichtung in Deutschland. In der internationalen Wissenschaftswelt zählt es zu den wichtigsten „Centers of Excellence" und ist, gemessen an Mitarbeiterzahl und Drittmittelvolumen, das weltweit größte Forschungszentrum auf dem Gebiet der Künstlichen Intelligenz und deren Anwendungen.

Im Forschungsverbund X-SONAR fokussiert das Teilvorhaben des DFKI die Unterstützung von Trainings-, Qualifizierungs- und Bildungsprozessen der schulischen, akademischen und beruflichen Aus-, Fort- und Weiterbildung durch Künstliche Intelligenz und innovative Softwaretechnologien. In Forschung, Entwicklung, Innovation und Transformation kommt der Emergenz von Technologie, Bildung und Organisation in vernetzten, digitalisierten Welten besondere Bedeutung zu. Die Wissenschaftlerinnen und Wissenschaftler kooperieren mit Partnern aus Forschung und Wissenschaft, Digital- und Bildungswirtschaft sowie mit Spin-offs, EdTec Start-ups und jungen Unternehmen im E-Learning und in der digitalen Bildung.
Leitung: Prof. Dr. habil. Christoph Igel

5. Assoziierte Partner/-innen

Dem Forschungsverbund gehören acht assoziierte Partner/-innen an, die mit ihrer Fachkompetenz eine beratende und unterstützende Funktion wahrnehmen und zur erfolgreichen Umsetzung des Gesamtvorhabens beitragen. Dazu gehören: Behörde für Schule und Berufsbildung, Beratungsstelle Gewaltprävention Hamburg (Dr. Christian Böhm), Fachhochschule der Polizei des Landes Brandenburg (Prof. Dr. phil. Frank J. Robertz), Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V. (FSM), jugendschutz.net, Institut für Rechts- und Kriminalsoziologie Wien (IRKS) (Dr. Hemma Mayrhofer), Landeskriminalamt Schleswig-Holstein (Marco Jäger), Stiftung Deutsches Forum für Kriminalprävention (DFK) (Wolfgang Kahl) und Universität Hamburg (Prof. Dr. Sighard Neckel).

Literatur

Böckler, N., & Zick, A. (2015). *Wie gestalten sich Radikalisierungsprozesse im Vorfeld jihadistisch-terroristischer Gewalt? Perspektiven aus der Forschung.* Handlungsempfehlungen zur Auseinandersetzung mit islamistischem Extremismus und Islamfeindlichkeit. Berlin Forum. Friedrich-Ebert-Stiftung.

Böckler, N., Hoffmann, J. & Zick, A. (2015). The Frankfurt Airport Attack: A Case Study on the Radicalization of a Lone-Actor-Terrorist. *Journal of Threat Assessment and Management.* Vol. 2: 3–4, S. 153–163.

Böckler, N., Seeger, T., Sitzer, P. & Heitmeyer, W. (2013 a). *School shootings: Conceptual framework and international empirical trends.* In: N. Böckler, T. Seeger, P. Sitzer, et al. (Hrsg.). School Shootings: International Research Case Studies and Concepts for Prevention. Springer-Verlag, New York, S. 1–26.

Böckler, N., Seeger, T., Sitzer, P. & Heitmeyer, W. (2013 b). *School Shootings. International Research, Case Studies, and Concepts for Prevention.* Springer-Verlag, New York.

Borum, R. (2015). Assessing Risk for Terrorism Involvement. *Journal of Threat Assessment and Management.* Vol. 2: 2, S. 63–87.

Brynielsson, J., Horndahl, A., Johansson, F., Kaati, L., Martenson, C. & Svenson, P. (2013). Harvesting and analysis of weak signals for detecting lone wolf terrorists. *Security Informatics.* Vol. 2: 11, S. 1–15.

Chen, H. (2011). Dark web: Exploring and data mining the dark side of the web. Springer Science & Business Media. Springer-Verlag, New York.

Cohen, K., Johansson, F., Kaati, L. & Mork, J. (2014). Detecting linguistic markers for radical violence in social media. *Terrorism & Political Violence.* Vol. 26, S. 246–256.

Conway, M. (2012). *Von al-Zarqawi bis al-Awlaki: Das Internet als neue Form des radikalen Milieus.* In: Malthaner, S. & Waldmann, P. (Hrsg.). Radikale Milieus: Das soziale Umfeld terroristischer Gruppen. Campus, Frankfurt und New York, S. 279–303.

Cortesi, S. & Gasser, U. (2015). *Digitally Connected: Global Perspectives on Youth and Digital Media*, Berkman Center for Internet and Society, Harvard University. Research Publication 2015–6 (April 2015). Verfügbar unter http://ssrn.com/abstract=2585686.

Gill, P. (2015). *Lone-Actor Terrorists. A behavioural analysis.* Routledge: New York.

Hoffmann, J. & Dölitzsch, C. (2015). *Schwere Gewalt am Arbeitsplatz.* In: Hoffmann J. & Roshdi, K. (Hrsg.). Amok und andere Formen schwerer Gewalt: Risikoanalyse – Bedrohungsmanagement – Präventionskonzepte. Schattauer Verlag, Stuttgart, S. 90–110.

Hoffmann, J. & Roshdi, K. (2015). *Bedrohungsmanagement.* In: Hoffmann, J. & Roshdi, K. (Hrsg.). Amok und andere Formen schwerer Gewalt: Risikoanalyse – Bedrohungsmanagement – Präventionskonzepte. Schattauer Verlag, Stuttgart, S. 266–296.

Hoffmann J. & Timmel Zamboni K. (2014). *Building up a Threat Assessment Process at Universities: Experiences from Europe.* In: Meloy, J. R. & Hoffmann, J. (Hrsg). International Handbook of Threat Assessment. Oxford University Press, New York, S. 351–359.

Meloy, J. R., Hoffmann, J., Roshdi, K. & Guldimann, A. (2014). Some Warning Behaviors Discriminate between School Shooters and Other Students of Concern. *Journal of Threat Assessment and Management.* Vol. 1: 3, S. 203–211.

Meloy, J. R. & Hoffmann, J. (2014). *International Handbook of Threat Assessment.* New York: Oxford University Press.

Meloy, J. R. & Yakeley, J. (2014). The violent true believer as "lone wolf:" Psychoanalytic perspectives on terrorism. *Behavioral Sciences and the Law.* Published in Wiley Online Library, DOI: 10.1002/bsl.2109.

Meloy, J. R., Roshdi, K., Glaz-Ocik, J. & Hoffmann, J. (2015). Investigating the individual terrorist in Europe. *Journal of Threat Assessment and Management*, 2: 3–4, S. 140–152.

Monahan, J. (2012). The individual risk of terrorism. *Psychology, Public Policy, and Law.* Vol. 18: 2, S. 167–205.

Mullen, P. E., Pathé, M. & Purcell, R. (2009). *Stalkers and their Victims.* Cambridge University Press. (2nd edition).

Weimann, G. (2015). *Terrorism in cyberspace: the next generation.* Columbia University Press.

White, S. G. (2014). *Workplace Targeted Violence.* In: Meloy, J. R. & Hoffmann, J. (Hrsg). International Handbook of Threat Assessment. Oxford University Press, New York. S. 83–105.