Protokoll zum Fachworkshop:

Zur Relevanz des Web 2.0 in der Sicherheitsforschung: Neue Formen sozialer Kontrolle und Partizipation

- Situationsdarstellungen und Forschungsfragen -

Veranstalter: Fachdialog Sicherheitsforschung
Montag, 10. Oktober 2011
Le Méridien Parkhotel, Frankfurt am Main

Wie bereits mit der Etablierung des Internets werden mit seiner Entwicklung zum Web 2.0 Fragen der Sicherheit intensiv diskutiert. Viele dieser Diskussionen, der Skizzierung von neuen Gefährdungen, von neuen Formen sozialer Kontrolle, oder von neuen Möglichkeiten zu partizipativer Sicherheitsgestaltung mögen von der Art "alter Wein in neuen Schläuchen sein", manches tatsächlich neu – ausgelotet ist dies noch keinesfalls. Welche Auswirkungen des Web 2.0 auf die zivile Sicherheit – bezogen auf die Dimensionen Terrorismus, Kriminalität, Infrastruktursicherheit (Großunfälle) wie auch extreme Naturereignisse und Katastrophen – sind gegenwärtig zu beobachten? Welche Erwartungen oder Bewertungen werden von unterschiedlichen Akteuren zum Ausdruck gebracht? Mit Blick auf das Web 2.0 scheinen – neben spezifischen Fragen der IT-Sicherheit, die im Rahmen des Workshops nicht oder allenfalls am Rande diskutiert werden sollten – vor allem zwei Felder von Interesse: Erstens die Frage, ob und inwiefern ein Wandel von Gefährdungslagen, insbesondere im Bereich des Extremismus oder Terrorismus vorliegt, der in spezifischer Weise mit neuen Kommunikationsformen verbunden ist. Damit verknüpft ist das Problem, inwiefern neue Kontrolldesiderate und Kontrolloptionen nicht nur für polizeiliche und nachrichtendienstliche Organe sondern auch für nicht-staatliche Akteure – von privatwirtschaftlichen Sicherheitsdienstleistern über zivilgesellschaftliche Organisationen, bis hin zum Individuum – entstehen. Zweitens stellt sich für alle Dimensionen ziviler Sicherheit die Frage, wie soziale Medien für neue Formen der Kommunikation und Interaktion zwischen Behörden, Organisationen und Bürgerinnen und Bürgern genutzt werden können. Dazu gehört auch die Frage, inwiefern letztere durch Formen sozialer Vernetzung mittels Tools und Anwendungen des Web 2.0 für Aktivitäten in den Bereichen Prävention, Überwachung, Alarmierung oder auch Krisenmanagement und -bewältigung mobilisiert werden können und sollten und welche Aspekte es bei derartigen Ansätzen zu bedenken gilt.

Was bedeuten die Entwicklungen zum Web 2.0 für die zivile Sicherheitsforschung? Inwiefern handelt es sich hierbei um ein relevantes Untersuchungsthema? Welche Chancen, welche Risiken des Einsatzes von Web 2.0-Technologien/-Applikationen lassen sich identifizieren? Welche problematischen gesellschaftlichen und moralischen Konsequenzen können sich ergeben, wenn diese für neue Formen sozialer Kontrolle genutzt werden? An welcher Stelle, zu welchen Fragen und Problemen besteht Forschungsbedarf und welche Formen eignen sich, diesem zu begegnen? Diese und weitere Fragen wurden im Rahmen des interdisziplinären Fachworkshops „*Zur Relevanz des Web 2.0 in der Sicherheitsforschung – Neue Formen sozialer Kontrolle und Partizipation*“ der am 10. Oktober 2011 in Frankfurt am Main stattfand, adressiert. Für die vom Projektteam des Fachdialogs Sicherheitsforschung (http://www.bmbf.de/de/12655.php) konzipierte und organisierte Veranstaltung konnte eine Reihe anerkannter Referentinnen und

Referenten aus unterschiedlichen Disziplinen und Forschungsfeldern wie auch aus der polizeilichen Praxis gewonnen werden.

Nach den einleitenden Grußworten von **Peter Zoche** (Fachdialog Sicherheitsforschung) und **Reinhold Friedrich** (BMBF) stand zum Auftakt des ersten Themenblocks die „*Kommunikationswissenschaftliche Einordnung von Social Media im Rahmen der Sicherheitsforschung*“ im Mittelpunkt. **Christoph Neuberger** (München) skizzierte einleitend die Potentiale des „Konvergenzmedium“ Internets in der Sozial-, Zeit-, Raum- und Zeichendimension und ging auf dessen Weiterentwicklung vom „Web 1.0“ zum „Web 2.0“ und damit verbundene Implikationen auf unterschiedlichen Ebenen (Öffentlichkeit, Markt, Software, Hardware) ein. Empirische Daten zu Nutzungsformaten und -häufigkeiten belegten eine zunehmende Verlagerung von Aktivitäten ins Internet; allerdings spiele bis dato bei den meisten social media-Formaten die passive Nutzung eine erheblich größere Rolle als aktive Nutzungsformen. Die Entwicklung hin zum Web 2.0 führe zu wichtigen Veränderungen in drei zentralen Dimensionen – Partizipation, Transparenz und Koordination des Verhaltens – die für die Sicherheitsforschung allesamt relevant seien und jeweils sowohl Chancen als auch Risiken beinhalteten. Neuberger unterstrich die Notwendigkeit, die Potentiale sozialer Medien aus Perspektive unterschiedlicher Akteure (Bürgerinnen und Bürger, Ermittlungsbehörden, Straftäter etc.) in den Blick zu nehmen und sich mit den Formen und ambivalenten Folgen veränderter Kommunikation im Web 2.0 (Zwei-Wege-Kommunikation; Wegfall prüfender „Gatekeeper“ beim Zugang zur Medienöffentlichkeit; neue Formen behördlicher Kommunikation: clash of cultures?; Beobachtbarkeit; das Hinterlassen virtueller „Spuren“ etc.) zu beschäftigen. Der Journalismus könne auf Grundlage reicher Erfahrung und bewährten Regeln im Umgang mit der Validierung von Quellen (Augenzeugenberichte etc.) gerade in Krisensituationen oder beim Eintreten überraschender Ereignisse auch künftig eine wichtige Gatekeeper-Funktion erfüllen.

Gerhard Vowe (Düsseldorf) konstatierte in seinem Vortrag zu Sicherheitskommunikation und Sicherheitsforschung in der Online-Welt einen rasanten Übergang in die digitale Welt, für den es kein „Navigationssystem“ gebe. Mit dem Web 2.0 bilde sich eine qualitativ neue Infrastruktur für gesellschaftliche Kommunikation heraus, die neue Formen der Integration von Individual-, Gruppen- und Massenkommunikation und eine zunehmende Konvergenz von Information, Kommunikation und Transaktion ermögliche – was eine Fülle von Chancen aber auch Risiken berge. Vowe verwies auf strukturelle Veränderungen gesellschaftlicher Kommunikation in sachlicher (größere Divergenz der Inhalte), zeitlicher, räumlicher und sozialer Hinsicht. Bisherige Grenzziehungen für gesellschaftliche Kommunikation, die Sicherheitswahrnehmungen und/oder Sicherheitsmaßnahmen in unterschiedlichen Dimensionen von Öffentlichkeit berührten (publizistisch relevant – publizistisch irrelevant; geheim – bekannt; privat – offen; proprietär – allgemein zugänglich; riskant – sicher), würden zunehmend in Frage gestellt und müssten neu ausgehandelt werden. Analytisch gelte es dabei, nach Kontinuitäten aber auch nach qualitativen Veränderungen und Brüchen zu fragen. Abschließend plädierte Vowe dafür, sowohl die substantiellen Chancen und Risiken des Web 2.0 als auch die damit verknüpften Chancen und Risiken für die (Sicherheits-)Forschung – in theoretischer, methodischer und organisatorischer Hinsicht – künftig stärker in den Blick zu nehmen.

In der Diskussion wurde betont, dass sich gesellschaftliche Kommunikation und Öffentlichkeit über die bereits genannten Punkte hinaus nicht zuletzt durch eine immens erweiterte und beschleunigte Zugänglichkeit und Bereitstellung von Information für und durch neue Akteure mit heterogenen Interessen verändere. Wichtig sei zudem, das Internet nicht allein als Kommunikationsmedium sondern als Handlungsmedium zu begreifen und zu analysieren. Die Divergenz der Themen und des Wissens sei an sich nicht neu, zudem ließen sich auch gegenläufige

Trends, eigene Formen der Konvergenzbildung im Netz beobachten; die These einer Fragmentierung der Öffentlichkeit werde von empirischen Analysen nicht bestätigt. Neben Prozessen der kommunikativen Öffnung und Streuung (Veränderung von Kommunikations- und Diffusionswegen, Pluralisierung von Diskussionsorten und Partizipationsmöglichkeiten etc.) gelte es deshalb auch Prozesse der Konzentration und Schließung, Macht- und Exklusionseffekte in den Blick zu nehmen (Stichworte: „Filterblase"; Internet als private Infrastruktur ohne Recht auf Zugang; Marktmacht von Anbietern). Grundsätzlich seien Prozesse der Neustrukturierung gesellschaftlicher Kommunikation, der Nutzung neuer Technologien und Medien durch unterschiedliche Akteure nicht prognostizierbar und kaum kontrollierbar oder steuerbar. Dies könne Verunsicherung hervorrufen aber auch Raum für Innovation, kreative Aneignungs- und Nutzungsweisen „bottom-up" schaffen (Bsp. Mapping-Projekte). Kontrovers diskutiert wurde auch die Frage sicherheitsrelevanter Grenzziehungen: Welche Rolle spielt das Web 2.0 innerhalb dieses Prozesses? Welche Phänomene und Entwicklungen die mit dem Web 2.0 in Verbindung gebracht werden sind tatsächlich neu? Welche relevanten Fragen zum Thema Grenzziehungen und Aushandlungsprozesse wären über die genannten hinaus zu adressieren? Und sei nicht die zentrale gesellschaftliche Herausforderung in Gegenwart und Zukunft der Umgang mit permanentem (technologiegetriebenem) Wandel? Alles sei so fluide geworden, dass die Frage nach dem Umbruch hin zu einem wie auch immer gearteten neuen Zustand oder stabilen Grenzziehungen in dieser Form im Grunde gar nicht mehr gegeben sei. Es gelte vor allem Dynamiken und Interaktionen, beschleunigte Prozesse der kontinuierlichen Öffnung und Schließung zu analysieren. Auch deshalb sollte die Forschung sich nicht allein auf Massenphänomene konzentrieren; wichtiger noch sei es, den Fokus auf die – heterogene und mit unterschiedlichen Zielsetzungen agierende – „digitale Avantgarde" zu richten.

Die Polizei, betonte **Axel Henrichs** (Landespolizeischule Rheinland-Pfalz) in seinem Vortrag zum Auftakt des zweiten Themenblocks *„Polizeiliche Kontrolle in sozialen Netzwerken: Erwartungen, Bedarf, Analysemöglichkeiten"* müsse und wolle sich mit dem Phänomen Internet „ganzheitlich" beschäftigen. Um den beiden verfassungsrechtlichen Aufträgen – Gefahrenabwehr und Repression – genüge tun zu können, müsse die Polizei notfalls in Grundrechte eingreifen dürfen. Jede im und über das Internet zugängliche Erkenntnisquelle müsse genutzt und die „digitale Forensik" massiv ausgebaut werden. Eine Kultivierung und Regulierung des polizeilichen Handelns im Netz durch die Schaffung klarer rechtlicher Rahmensetzungen und Ermächtigungsgrundlagen, sowie eine verbesserte Schulung von Polizeibeamten zur Verringerung allgegenwärtiger Wissensdefizite, seien hierbei von zentraler Bedeutung. Innerhalb des für polizeiliche Maßnahmen wichtigen Dreiecks Technik – Taktik – Recht fungiere die Technik zunehmend als „Schrittmacher" und gebe ein Tempo vor, mit dem das Recht nicht Schritt halten könne. Weitere Probleme entstünden durch unklare Zuständigkeiten von Aufsichtsbehörden, fehlende Rechtsgrundlagen für ein „virtuelles Betretungsrecht" in der Strafprozessordnung und durch unklare Begriffsdefinitionen („allgemeine Zugänglichkeit"; „Privatheit"; „(Teil-)Öffentlichkeit"). Präzisierungen seien hier dringend notwendig. Grundsätzlich stelle sich die Frage, ob und inwieweit Regelungen für die „reale" auf die „virtuelle Welt" übertragbar seien. Daneben werfe die Bindung an nationales Recht im Umgang mit Phänomenen wie „cloud computing"; „cloud storage" oder auch international vernetzter Kriminalität erhebliche Probleme auf. Entscheidend sei, dass Handlungsbedarfe, die sich aus der polizeilichen Praxis ergäben, an verantwortlicher Stelle erkannt und aufgegriffen würden (Rechtsgrundlagen, Ressourcenausstattung usw.). Als Forschungsdesiderat nannte Henrichs darüber hinaus Untersuchungen zur Wirkung des neuen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Nach der Pause standen Überlegungen zur bürgerschaftlichen Partizipation und Interessenslage im Zentrum des Vortrags „FutureICT and the Need of a Trustable Web“ von **Dirk Helbing** (Zürich), seine Ausführungen fokussierten auf die Schaffung eines zukünftigen „trustable web“. Wenn es gelinge, die richtigen technologisch-regulatorischen Voraussetzungen zu schaffen, biete der im Zuge informations- und kommunikationstechnischer Entwicklungen stattfindende Prozess der Umgestaltung sozialer Systeme ungeachtet aller Ambivalenzen große Potentiale – auch im Sinne von mehr Demokratie und mehr Partizipation. Im Umgang mit Problemen die das Internet aufwerfe (surveillance etc.) komme es zu – an sich nicht neuen – Kollisionen zwischen top-down (Politik) und bottom-up-Prinzipien (Markt). Faktisch könne das Internet nicht top-down kontrolliert werden, gleiches gelte für gegenwärtige Versuche der Finanzmarktregulierung. Deshalb bedürfe es neuer regulatorischer Lösungsansätze, einer Koordinierung heterogener Interessen auf Grundlage des Prinzips der „demokratischen Delegation, was Effizienz schaffe aber auch Kompromisse erzwinge und voraussetzungsvoll sei (Vertrauen; gesellschaftliche Anpassungsfähigkeit an beschleunigten Wandel; Privatsphäre; geschützter Raum für Minoritäten). Helbing unterstrich, dass die Ursache für vielfältige Destabilisierungen unserer Zeit v.a. in der Schaffung starker Kopplungen, weltweiter Vernetzungen und interdependenter Systeme zu suchen sei – ein Zuviel an Vernetzung führe langfristig zu Verwundbarkeit, Destabilisierung von innen, zur Häufung von extremen Ereignissen und zum Zusammenbruch von Kooperation. Die gesellschaftlichen Implikationen dieser veränderten Welt seien – auch wissenschaftlich – kaum verstanden. Wissenstechniken wie computerbasierte Modellierung und Simulation von gesellschaftlichen Prozessen und Dynamiken auf Grundlage der Verfügbarkeit von neuen Daten könnten hier wichtige Erkenntnisse liefern. Notwendig sei eine veränderte, interaktions- statt komponentenorientierte Sichtweise: eine Wissenschaft der komplexen Systeme, in deren Fokus Dynamiken und Interaktionen, Fragen der Kooperation und Prozesse der Selbstorganisation (bottom-up) stehen. Damit letztere zu gesellschaftlich erwünschten Ergebnissen führen, sei die Schaffung eines Regulatoriums für Interaktionen (top-down) notwendig. Das *FuturICT flagship project* ziele u.a. auf die Schaffung „eines „planetaren Nervensystems“, vergleichbar dem menschlichen Immunsystem, für dessen Funktionieren bottom-up-Mechanismen wie etwa Reputationsmechanismen eine zentrale Rolle spielen sollen. Als offene, transparente Plattform bzw. sich selbst regulierendes, nachhaltiges „Informationsökosystem“ setze das „trustable web“ eine verantwortungsvolle Nutzung und die Entstehung eines kollektiven Bewusstseins voraus. Zudem müssten die Nutzer Besitzer ihrer Daten sein und diese selbst kontrollieren können.

Hans-Jörg Albrecht (Freiburg) plädierte in seinem Kommentar dafür, vergangene Erfahrungen im Umgang mit neuen Technologien, neuen Formen von Interaktion und damit verknüpft der Entwicklung veränderter Einstellungen, Wahrnehmungen (Gefahren, Risiken, Tolerierung) und Handlungsweisen in den Blick zu nehmen. Es lohne sich zu fragen, ob und inwieweit man sowohl in theoretischer Hinsicht als auch mit Blick auf das Verständnis des Umgangs mit Veränderungen aus der Geschichte lernen und verallgemeinerungsfähige Annahmen ableiten könne. Im Fokus gegenwärtiger Vorstellungen über Sicherheit, Bedrohung und Risiko stünden extreme Ereignisse unterschiedlichster Form; die Zusammenhänge zwischen Phänomenen wie Mobbing, sexuellem Missbrauch, Amokläufen, Extremismus oder Radikalisierungsprozessen und kommunikativen Entwicklungen seien indes unklar. Albrecht unterstrich, dass Vorstellungen, die hinter der Wahrnehmung von und dem Umgang mit Risiken steckten, in besonderem Maße der Analyse und Diskussion bedürften und verwies auf sechs gegenwärtig prägende Konzepte: Furcht vor „Ansteckung“; das Verderben von unschuldigen Menschen; „Spurensuche“; der Umgang mit Anonymität im Netz; die Erhöhung von „Verletzlichkeit“ und problematische Vorstellungen über die Prognostizierbarkeit von extremen Ereignissen, Entwicklungen aus von Akteuren im Netz produzierten Informationen, mit dem Ziel, das Auftreten von Schaden zu verhin-

dern. Mit Blick auf die polizeiliche Praxis im Netz unterstrich Albrecht die Notwendigkeit einer rechtlichen Anpassung (Polizeigesetz und Strafprozessordnung) an technologische Entwicklungen. Bestehende Regelungen für Zwangsmaßnahmen (Zugang, verdeckte Ermittlungen usw.) ließen sich nicht einfach auf die virtuelle Welt übertragen. Zudem müsse die Tendenz, Potentiale des Web 2.0 nicht allein für die Aufklärung und Verfolgung von Straftaten sondern zunehmend auch für proaktive Maßnahmen zu nutzen, kritisch hinterfragt werden. Studien in den USA belegten, dass verdeckte Ermittlungen und das Aufstellen von „honeypots“ höchst problematische Effekte hervorbringen könnten.

In der Diskussion wurde nochmals unterstrichen, dass – auch aufgrund verfassungsrechtlicher Vorgaben für informationelle Eingriffe – bestehende rechtliche Vorschriften nicht einfach auf den virtuellen Raum übertragbar seien. Entsprechende Regelungen und Instrumentarien müssten grundsätzlicher ansetzen und komplexer gestaltet sein; nicht zuletzt auch, um die Gefährdungen, die mit polizeilichen Eingriffen verbunden seien, kontrollierbar(er) zu machen (Protokollierung/ Überwachung von Zugriffen, technische Sicherheit von Zugriffsmechanismen etc.). Allerdings fehle es Juristen häufig an Wissen darüber, was technisch möglich sei, zugleich fehlten Anreize für die Technikentwicklung, technisch gestützte Lösungen zu schaffen die es erlauben, Entwicklungen in Richtung immer umfassenderer Datenerfassung, -verknüpfung und -auswertung wieder in den Griff zu bekommen. Die Bearbeitung dieser Fragen und die Entwicklung angemessener Lösungsansätze erfordere eine intensive Zusammenarbeit von Technikern, Sozialwissenschaftlern und Juristen im Rahmen integrierter Forschung. Als weiteres Forschungsdesiderat wurde die Erforschung sozialer Wirkungen von (Überwachungs-)Technologien genannt; hierzu existierten im Wesentlichen Alltagstheorien aber nahezu kein empirisch fundiertes Wissen. Ähnliches gelte für gesellschaftliche (Un-)Sicherheitswahrnehmungen und für Diskurse über „Sicherheit“, auf die sich polizeiliche Arbeit berufe; auch hier werde häufig auf Grundlage von Annahmen operiert, ohne ausreichendes Wissen darüber, wie der normative Begriff von Sicherheit zustande komme und was im Einzelnen dahinter stecke. Wünschenswert sei eine stärkere Öffnung und Kooperationsbereitschaft von Polizei und Sicherheitsbehörden für gemeinsame Forschung, von der die Behörden selbst profitieren könnten. Der geforderte „ganzheitliche“ Umgang mit dem Web 2.0 verweise auch auf Fragen der polizeilichen Organisation(skultur): Was bedeuten technische Entwicklungen, neue Ermittlungstätigkeiten jenseits technischer Anwendungsfragen für die formale Organisation, für Einsatztaktiken oder für das Selbstverständnis der Polizei? Welche heterogenen Handlungsoptionen ergeben sich jeweils in Abhängigkeit davon, wie neue Technologien genutzt werden (bottom-up vs. top-down; reaktiv vs. proaktiv) und welche Implikationen dieser Nutzungsweisen gilt es zu bedenken? Zudem gelte es das generell für technische Entwicklungen beobachtbare Problem des „function creep" im Blick zu behalten. Erste empirische Studien zur Aneignung des Internet in Polizeiorganisationen zeigten, dass faktisch ein fortlaufendes Wechselspiel von auf Bedürfnisse der Praxis gegründeten Einzelinitiativen, lokalen Software-Entwicklungen (bottom-up) und Versuchen der Zentralisierung und Vereinheitlichung (top-down) stattfinde.

Mit Blick auf Ansätze wie Modellierung und Simulation wurde auf die Notwendigkeit eines angemessenen Umgangs mit Simulationen und Prognosen, eines Bewusstsein für deren begrenzte Aussagefähigkeit und starke Bindung an ein spezifisches Referenzsystem verwiesen. Reales Handeln von Personen unterliege dagegen immer mehreren Referenzsystemen und sei durch situationsbezogene Entscheidungen darüber gekennzeichnet, welchem Referenzsystem jeweils eine bestimmte Priorität gegeben werde. Erfahrungen in anderen Bereichen verwiesen auf Grenzen von Versuchen, Interaktions- und Kooperationsprozesse ex ante zu regulieren. Wichtiger sei die Fähigkeit von Personen, in nicht vorab definierten Situationen zu entscheiden; im Fokus sollten deshalb primär Fragen der Kompetenzentwicklung in Richtung Handeln und Ent-

scheiden unter Bedingungen von Komplexität und Ungewissheit (Vertrauensbildung, Sicherheit schaffen etc.) stehen. Ob neue IT-gestützte Instrumentarien in einem positiven Sinne verhaltensregulierend wirken können, wurde ebenso kontrovers diskutiert wie die Frage, ob angesichts von Prozessen wie Selbstorganisation und Kooperation ein übergeordneter technologisch-regulierender Rahmen überhaupt notwendig sei. Das zentrale Problem – der Umgang mit selbst geschaffener Komplexität – könne nicht durch top-down-Richtlinien allein geregelt werden. Notwendig sei ein integrierter Ansatz, der Partizipation und Mitgestaltung ermögliche und damit auch Vertrauen in die neu zu schaffenden Strukturen entstehen lasse. Ein dringend zu adressierendes Problem sei darüber hinaus der Missbrauch von Daten durch Firmen, hier gelte es rechtliche Regelungen zu schaffen, die es Bürgern und Institutionen ermöglichen, ihre Rechte einzufordern, nur so könne Vertrauen erhalten werden. Die technische Verfügbarkeit von Daten schaffe eine qualitativ veränderte Situation; eine Auseinandersetzung mit deren Implikationen wie auch dem gesellschaftlichen Umgang mit diesen Veränderungen sei dringend erforderlich, möglicherweise auch im Rahmen einer öffentlichen ethischen Debatte. Zugleich sollte untersucht werden, welche Mechanismen jenseits von Vertrauen für die Stabilisierung und das Funktionieren von sozialen Netzwerken eine Rolle spielen und wie diese auch im Hinblick auf zukünftige Entwicklungen genutzt werden könnten.

Zu Beginn des dritten Themenblocks *„Behörden und Bürger – Praxis aus Polizei und Katastrophenschutz“* schilderte **Ralf Hövelmann** (Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen) zentrale Schritte, Herausforderungen und Ziele der Polizei NRW auf dem Weg „Von der Idee zur erfolgreichen App“, die auf der CeBIT in Hannover vorgestellt wurde. Ein zentrales Moment sei die Suche nach neuen Wegen der Bürgerkommunikation: Mobile Anwendungen ermöglichten veränderte, aktive und direkte Formen der Kommunikation zwischen Polizei und Bürgerinnen und Bürgern. Zu den notwendigen Voraussetzungen zählten der Aufbau einer Online-Plattform, die Schaffung von Organisationsstrukturen/ technischen Infrastrukturen, die Schulung von Personal, die Klärung von Datenschutzfragen etc.. Vor dem Hintergrund von Reichweitenanalysen und Erwartungen, dass bis zum Jahr 2013 eine Mehrheit der Menschen über mobile Endgeräte ins Internet gehen werde, böten mobile Anwendungen eine wichtige Chance für die Polizei, Menschen auf der Straße, insbesondere auch jüngere Zielgruppen, zu erreichen und zu informieren. Ziel sei es, eine möglichst hohe Verbreitung und einen möglichst hohen Nutzwert durch kontinuierliche Weiterentwicklung von Nutzungsmöglichkeiten zu erreichen (Serviceinformationen, Fahndungsaufrufe, "Use and Push"-Funktion, Personalisierung, Notruf 110, Online-Anzeigen etc.). Polizeitaktisch ermögliche die App nicht allein neue Formen der Presse- und Öffentlichkeitsarbeit, sondern vielfältige Potentiale, etwa im Bereich Krisenkommunikation (z.B. regionalisierte, georeferenzierte Informationen), die künftig auch einsatztaktisch stärker genutzt werden könnten. Die App stoße bundesweit – ähnlich wie das Pilotprojekt "Facebook Fahndung" der PD Hannover – bei Nutzern wie auch in Behördenkreisen auf großes Interesse; langfristiges Ziel sei die Entwicklung einer Polizei Deutschland-App mit regionalen Strukturen.

Die Frage, ob soziale Medien in Krisenfällen eine Rolle spielen, betonte **Volkmar Pipek** (Siegen), stelle sich im Grunde nicht – sie seien einfach da. Entscheidend sei es, in eine Gestaltungsposition zu kommen: Wie müssen soziale Netze aussehen, damit sie bestimmte Zwecke und Funktionen für uns erfüllen? Gerade weil es dabei sowohl Chancen als auch Risken gebe, sollte man verschiedene Konzepte entwickeln und testen, um vorhandene Potentiale tatsächlich nutzen zu können. Prinzipiell seien bestimmte Phänomene des sozialen Verhaltens online, die im Zusammenhang mit Web 2.0 diskutiert würden, nicht neu und begleiteten das Internet seit seinen Anfängen. Dieses biete nicht allein in technischer Hinsicht sondern v.a. als relevante gesellschaftliche Kommunikationsinfrastruktur eine Fülle neuer Möglichkeiten, auch und gerade

für das Krisenmanagement. Konkrete Interaktionserfahrungen mit Polizei, Feuerwehr und Krisenmanagern im Rahmen des Projekts *InfoStrom* (BMBF) zeigten, dass es extrem wichtig sei, zum einen die Praktiker auf lokaler Ebene, vor Ort an der Entwicklung zu beteiligen und zum anderen zu versuchen, eine soziotechnische Perspektive zu etablieren. Prozesse der integrierten Technikgestaltung erforderten eine enge Zusammenarbeit von Informatik und Sozial-/Geisteswissenschaften und sollten darüber hinaus eine Einbeziehung der Nutzer ermöglichen. Soziale Medien, neue Interaktionsmöglichkeiten würden zunehmend auch von Organisationen/ Akteuren des Krisenmanagements genutzt; sie führten zum Entstehen ganz eigener Kommunikationskulturen und böten vielfältige Nutzungspotentiale. Als Stärken sozialer Medien nannte Pipek die große Diversität von Medien, die Möglichkeit zur Anbindung an klassische Informationswege, zum Posten von Masseninformationen wie auch der relativ gezielten Adressierung, Möglichkeiten der kontextuellen Anreicherung von Mitteilungen über Tags (Codewörter) und Geo-Tags (ortsbezogene Informationen) sowie der Verstärkung von Meldungen über Retweets. Zentrale Herausforderungen seien zum einen die Qualität und Zuverlässigkeit der Informationen, zum anderen die Bewältigung, Strukturierung und Verarbeitung großer Mengen von Information. Der analytisch-gestalterische Ansatz von *InfoStrom* sei es, die Bürger als Krisenmanager ihrer eigenen Krise aufzufassen und unterschiedliche Kommunikationswege/-muster im Hinblick darauf zu untersuchen, wie soziale Medien gestaltet werden müssten, damit sie in der jeweiligen Situation und Konstellation einen Nutzen entwickeln können: Krisenkommunikation (Behörden – Bürger); Selbsthilfe-Netzwerke (Kommunikation von Menschen untereinander ohne Beteiligung institutionalisierter Akteure); Integration bürgergenierter Inhalte (Bürger – Behörden/Organisationen); interorganisationale Kommunikation/ interorganisationales Krisenmanagement.

Mit Blick auf die Polizei-NRW-App wurden in der Diskussion sowohl (künftige) Potentiale als auch Probleme und Risiken thematisiert (Online-Anzeigeerstattung; Umgang mit Zeugen, Beweismaterial wie Fotos, Videos etc.; Falschinformationen und Manipulationsmöglichkeiten; Datensicherheit etc.) und auf die Notwendigkeit kontinuierlicher erfahrungsbasierter Lernprozesse verwiesen. Eine weitere Frage, die der Evaluation bedürfe, sei der tatsächliche Mehrwert der App (Anzeigeverhalten, Aufklärung von Straftaten, Kontakt mit schwer erreichbaren Zielgruppen). Generell bestehe zu Fragen wie Nutzungsweise (aktiv/passiv), Nutzungsmotiven (Nutzwert, Infotainment, Voyeurismus) und Nutzererwartungen/-bedarfen (Funktionalität, Information) erheblicher empirischer Forschungsbedarf. Weiterhin wurde angemerkt, dass Verlauf und Erfolg von Versuchen, social media für neue Formen der Bürgerkommunikation zu nutzen, stark davon abhänge, ob entsprechende Ansätze eher bottom-up oder top-down (Entwicklung von Richtlinien etc.) geprägt seien; dies zeige der europäische Vergleich. Wenn die Polizei sich öffne und ihren Beamten erlaube, eine eigene Stimme in sozialen Netzwerken zu haben, so zeigten Erfahrungen im Kontext der Riots in Großbritannien, könne dies auch zur Entstehung von Vertrauen und zum Verständnis für Fehler beitragen. Zu fragen wäre hierbei, wie Vertrauen gemessen wird und ob und inwieweit sich das in Deutschland offensichtlich sehr stabile vertikale Vertrauen in die Polizei mit und durch Kommunikation im Web 2.0 tatsächlich verändere. Generell zeige die empirische Forschung, dass Behörden/ Institutionen in Krisensituationen zunächst ein Vertrauensvorschuss gegeben werde, den man nicht zerstören dürfe. Wenn diese in sozialen Medien präsent seien, sei es wichtig, nicht allein (krisenrelevante) Informationen bereitzustellen, sondern in Interaktion zu treten, auf Bedürfnisse, Fragen, Kritik etc. zu reagieren. Dynamiken und Interaktionen (Eskalation vs. Deeskalation), die durch und mit social media entstehen, sollten intensiver erforscht werden: Welche Rolle können social media im Hinblick darauf spielen, gesellschaftliche Prozesse (z.B. Proteste) in eine bestimmte Richtung zu lenken, in bestimmten Bahnen zu halten?

Ein wichtiges Moment des Krisenmanagements sei die emotionale Bewältigung einer Krisensituation; hier böten soziale Medien (Bsp. Loveparade) große Potentiale. Bislang ebenfalls unterschätzt seien Formen der bottom-up-Organisation, der Beteiligung der Bürger und der Koordination von Hilfe in Krisensituationen über social media (lokale, zeitnahe Bedarfs-/Angebotsartikulationen; Personensuche; detailliertere Lagebilder, zielgerichtete Verteilung von Ressourcen). Entsprechende Forschung finde bisher v.a. im amerikanischen Raum statt, wo bspw. an Verfahren zur automatisierten Auswertung von Twitter-Kommunikation gearbeitet werde (Forschungsgruppe "*ConnectivITy Lab*", Leysia Palen, http://www.cs.colorado.edu/~palen/Home/Connectivity_Lab.html). Social media könnten gerade im Bereich Katastrophenschutz sinnvoll eingesetzt werden (Monitoring; neue Informationskanäle für Krisenstäbe; beschleunigte Informationen an die Bevölkerung; zentral koordinierte behördliche Kriseninformation); allerdings gebe es auch Gefahren und Probleme, derer man sich bewusst werden müsse. Generell sollte im Blick behalten werden, dass Versuche eine neue Medienkonfiguration herzustellen Gewinner aber auch Verlierer kenne (digital divide). Einerseits könnten Web 2.0-Medien/-applikationen als redundant ausgelegte Kanäle im Krisenfall andere Kommunikationswege entlasten, andererseits müsse man sich darüber im Klaren sein, dass man sich mit der Nutzung von sozialen Medien einer spezifischen Logik preisgebe: Soziale Medien im Internet funktionierten nach einer privatwirtschaftlichen nicht einer staatlichen/öffentlichen Logik. Bisher gebe es keine Verpflichtung, kein „must care“ für private Unternehmen, Informationen im Krisenfall durchzulassen; hier gelte es, vergleichbar zu anderen Infrastrukturen, die teilweise öffentlichen Zwecken zugeführt würden, in Zusammenarbeit mit privaten Unternehmern, Anbietern entsprechende Konfigurationen auch bei sozialen Medien zu schaffen; ggf. seien auch Vorgaben des Gesetzgebers, rechtliche Rahmensetzungen erforderlich. Weiterhin wurde unterstrichen, dass jede (weitere) Infrastruktur auch neue Verletzlichkeiten, Ausfallgefahren biete. Die Vorbereitung auf einen möglichen Ausfall von Infrastrukturen, das Nachdenken über Rückfallstrategien sollte deshalb integraler Bestandteil bereits der Konzeptentwicklung und der Gestaltung von Infrastrukturen sein. Inwieweit könnten Informationen aus social media auch dazu genutzt werden, um drohende Gefahren abzuwenden und gewissermaßen „vor die Lage“ zu kommen (modell-/simulationsbasierte Entscheidungsunterstützung etc.)? Prinzipiell sollten diesbezügliche Erwartungen nicht zu hoch gesteckt werden; vorstellbar seien aber Ansätze, in Krisensituationen relevante fehlende Informationen gezielter anzufragen, um Entscheidungen von Krisenstäben (Priorisierung von Maßnahmen etc.) zu unterstützen. Entsprechende Ansätze sollten als interaktiver, praxisnaher Prozess gestaltet werden und könnten bspw. auch die Ausbildung von Scouts beinhalten, die im Krisenfall u.U. verlässlichere Informationen von vor Ort liefern könnten als ungeschulte Personen. Der Aufbau eigener soziale Netzwerke-Infrastrukturen speziell für das (interorganisationale) Krisenmanagement erfordere strategische Diskussionen und Kommunikationen, die zwar über soziale Medien geführt werden könnten jedoch in irgendeiner Form geschützt sein sollten. Es sei deshalb sinnvoll, nicht ausschließlich auf vorhandenen Strukturen (z.B. Facebook) aufsetzen, sondern aus Anforderungen der Praxis zu lernen und bewusst eigene Strukturen und Netzwerke aufzubauen und zu gestalten. In diesem Zusammenhang wurde die Frage nach Möglichkeiten der Evaluation und Erfolgsbemessung einzelner Anwendungen im Hinblick auf jeweils gesteckte (Einsatz-)Ziele aufgeworfen. Dies sei im Krisenfall faktisch sehr schwierig, vorstellbar seien aber Debriefing-Prozesse, retrospektive Analyse und Aufarbeitung der Abläufe, ex-post-Identifikation von Lern- und Verbesserungsmöglichkeiten etc. Die erfolgreiche Nutzung sozialer Medien hänge nicht zuletzt von der Entwicklung und Etablierung entsprechender Nutzungskulturen ab; erst dann werde der Nutzwert sichtbar und bewertbar. Ein zentrales Moment sei die Notwendigkeit einer sinnvollen Strukturierung von (nutzergenerierten) Inhalten und Informationen, als Voraussetzung dafür, diese im Krisenmanagement tatsächlich sinnvoll nutzen zu können. Die Potentiale

von social media sollten in einem kreativen, partizipativen Prozess des Ausprobierens ausgelotet werden: "Man muss den Mut zum Experiment haben."

Social Media und Web 2.0, so bleibt als ein zentrales Ergebnis des Workshops festzuhalten, sind Phänomenbereiche, die ohne Zweifel auch für die zivile Sicherheitsforschung in ihren unterschiedlichen Dimensionen Relevanz besitzen. Die Vorträge der Referenten wie auch die Plenumsdiskussionen trugen dazu bei, das sehr breite Thema Web 2.0 und Sicherheitsforschung aus theoretischer wie auch praxisorientierter Perspektive in all seiner Ambivalenz zu beleuchten. Der Workshop lieferte eine große Bandbreite an wichtigen Hinweisen auf offene Fragen und (inter-)disziplinäre Forschungsbedarfe und machte deutlich, dass eine angemessene Beschäftigung mit dem Thema Web 2.0 in der zivilen Sicherheitsforschung bedeuten sollte, Chancen und (Gestaltungs-)Potentiale auszuloten, zugleich aber auch Herausforderungen, Probleme und Risiken neuer Medien, neuer Kommunikations- und Interaktionsformen, neuer Formen der sozialen Kontrolle und Partizipation zu diskutieren und zu analysieren.

Referenten- und Teilnehmerverzeichnis

1.	Prof. Dr. Dr. Hans-Jörg **Albrecht**	Max-Planck-Institut für ausländisches und internationales Strafrecht Freiburg i. Br.
2.	Harald Arnold	Max-Planck-Institut für ausländisches und internationales Strafrecht Abteilung Kriminologie Freiburg i. Br.
3.	Sabine Blum M.A.	Albert-Ludwigs-Universität Institut für Soziologie Freiburg i. Br.
4.	Sebastian Denef	Fraunhofer-Institut für Angewandte Informationstechnik FIT St. Augustin bei Bonn
5.	RD Reinhold Friedrich	Bundesministerium für Bildung und Forschung BMBF Referat 522 Sicherheitsforschung Bonn
6.	Prof. Dr. Dirk **Helbing**	ETH Zürich Lehrstuhl für Soziologie, insb. Modellierung und Simulation Zürich
7.	Dr. Axel **Henrichs**	Landespolizeischule Rheinland-Pfalz Fachhochschule für öffentliche Verwaltung, Fachbereich Polizei Hahn-Flughafen
8.	Sven Hermann	Bundesministerium für Bildung und Forschung BMBF Referat 525: Kommunikationssysteme; IT-Sicherheit Bonn
9.	Ralf **Hövelmann**	Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen Düsseldorf

10.	Dr. Martin Kahl	Universität Hamburg Institut für Friedensforschung und Sicherheitspolitik Hamburg
11.	Dr. Catarina Christina Katzer	Cyberpsychologie, Medienethik und Jugendforschung / Europäisches Netzwerk für Cybermobbing Köln
12.	PD Dr. Stefan Kaufmann	Albert-Ludwigs-Universität Freiburg Institut für Soziologie Freiburg i. Br.
13.	Dr. Daniel Jeffrey Koch	Fraunhofer-Institut für System- und Innovationsforschung ISI Karlsruhe
14.	Dr. Benedikt Köhler	Arbeitsgemeinschaft Social Media e.V. Ethority GmbH München
15.	Prof. Dr. Nicole Krämer	Universität Duisburg-Essen Fachgebiet Sozialpsychologie: Medien und Kommunikation Fakultät für Ingenieurwissenschaften Duisburg
16.	Dr. Matthias Künzel	VDI/VDE Innovation + Technik GmbH Berlin
17.	Prof. Dr. Christoph **Neuberger**	Ludwig-Maximilians-Universität München Institut für Kommunikationswissenschaft und Medienforschung München
18.	Prof. Dr. Sabine Pfeiffer	Hochschule München Professur für Innovation und kreative Entwicklung / ISF München Institut für Sozialwissenschaftliche Forschung e.V. München

19.	Prof. Dr. Volkmar **Pipek**	Universität Siegen Juniorprofessur für CSCW in Organisationen, Institut für Wirtschaftsinformatik Siegen
20.	Prof. Dr. Ralf Poscher	Albert-Ludwigs-Universität Freiburg Institut für Staatswissenschaft und Rechtsphilosophie Freiburg i. Br.
21.	Prof. Dr. Jo Reichertz	Universität Duisburg-Essen Institut für Kommunikationswissenschaft Essen
22.	Prof. Dr. Gerhard **Vowe**	Heinrich-Heine Universität Düsseldorf Lehrstuhl für Kommunikations- und Medienwissenschaft
23.	Prof. Dr. Nils Zurawski	Universität Hamburg Vertretungsprofessur für Sicherheit, soziale Konflikte und Regulation Institut für Kriminologische Forschung Hamburg
24.	Peter Zoche M.A.	Fraunhofer-Institut für System- und Innovationsforschung ISI Projektleitung Fachdialog Sicherheitsforschung Karlsruhe