Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 1759

Sicherheit vs. Privatsphäre: Zur Akzeptanz von Überwachung in sozialen Medien im Kontext von Terrorkrisen

Christian Reuter[1], Gordian Geilen[2] und Robin Gellert[3]

Abstract: Nach den terroristischen Anschlägen in Paris 2015 und Brüssel 2016 wurde das Bedürfnis nach mehr Sicherheit und Überwachung im Internet laut. Als Folge der Enthüllungen der Überwachungs- und Spionagetechniken der National Security Agency (NSA) durch Edward Snowden 2013 konnte in der Bevölkerung aber auch ein Aufschrei nach erhöhtem Schutz der Privatsphäre im Internet wahrgenommen werden. Die geschilderten Ereignisse verdeutlichen die gegensätzlichen Wünsche nach Sicherheit und Überwachung im Internet sowie Schutz der Privatsphäre. Im ersten Teil dieses Beitrags stellen wir den Stand der Forschung im Bereich Terror, Sicherheit und Privatsphäre in sozialen Medien dar. Im zweiten Teil führen wir eine explorative Studie durch, um zu beleuchten, ob Bürgerinnen und Bürger in Krisenzeiten bereit wären, ihre Privatsphäre im Internet, vor allem in sozialen Netzwerken, zugunsten von Sicherheit zu reduzieren. Basierend auf qualitativen Daten zeigt diese Arbeit Meinungscluster und Tendenzen in Bezug auf das Nullsummenspiel „Sicherheit und Privatsphäre".

Keywords: Soziale Medien, Sicherheit, Privatsphäre, Notfallmanagement

1 Einleitung

Sicherheit oder Privatsphäre? Lassen sich diese beiden Maxime in Einklang miteinander bringen? Oder befinden sie sich in einem nicht kompromissfähigen Nullsummenspiel? Edward Snowden löste mit seinen Spionageaufdeckungen einen enormen Anstieg an dem Bedarf nach mehr Privatsphäre im Internet aus und stieß damit auf positiven Widerhall. Konträr dazu steht die Omnipräsenz des Terrorismus, sodass mittlerweile sogar von „Terrorkrisen" [We02] gesprochen wird. Der schwerwiegendste Angriff auf Europa war der Anschlag auf die Pariser Innenstadt im Dezember 2015, bei dem über 130 Menschen getötet wurden. Daraufhin wurden rapide neue Sicherheitskonzepte entworfen, um Anschläge wie diesen in Zukunft zu verhindern. Dabei war vor allem ein Detail von essentieller Bedeutung: Die Attentäter hatten sich vorab im Internet über ihren bevorstehenden Anschlag ausgetauscht.

Die beiden Leitgedanken „Sicherheit" und „Privatsphäre" haben beide großen Stellenwert. Doch wenn sie sich in einem augenscheinlichen Widerspruch befinden, ist

[1] Universität Siegen, Institut für Wirtschaftsinformatik, Kohlbettstr. 15, 57072 Siegen (alle Autoren), christian.reuter@uni-siegen.de
[2] gordian.geilen@student.uni-siegen.de
[3] robin.gellert@student.uni-siegen.de

dann deren Koexistenz überhaupt möglich? Im Zuge dieser Arbeit soll daher zunächst der Wunsch nach Privatsphäre der Bürger analysiert werden, um anschließend über das Potential zur Identifizierung und Überwachung von Terroristen im Internet zu diskutieren. Nach der Darlegung des Stands der Forschung werden der Fokus und die Ziele dieser Arbeit erläutert (Kap. 2). Anschließend werden die Methodik der empirischen Untersuchung sowie die erzielten Ergebnisse dargestellt (Kap. 3). Fortan folgt eine Diskussion über die Resultate (Kap. 4), um abschließend ein Fazit geben zu können (Kap. 5).

2 Stand der Forschung: Terror, Sicherheit und Privatsphäre in sozialen Medien

Terror, Sicherheit, Risiko, Vertrauen und Privatsphäre stehen in der Fachliteratur in einem nicht immer eindeutigen Verhältnis. Dies hängt teilweise mit der vagen und nicht eindeutigen Begriffsverwendung sogenannter „schillernder Begriffe“ [We07] zusammen, deren „wahre Bedeutung“ sind je nach Kontext und Disziplin unterscheidet. Selbst innerhalb des Systems von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) können terminologische Unterschiede attestiert werden [Re11].

[Wo12] zeigen, dass die norwegische Bevölkerung nach den Terroranschlägen im Juli 2011 ein erhöhtes interpersonelles und institutionelles Vertrauensgefühl gewann. Da Vertrauen und Angst als Gegensatzpaar verstanden werden kann, kann dies als Kontrast zu den Ergebnissen von [Gr09] stehen, wonach in der Bevölkerung die Angst vor terroristischen Anschlägen (gerade nach den Anschlägen auf das World Trade Center) relativ hoch ist, was sie auch auf die hohe mediale Präsenz des Themas zurückführen. Auch [Ja07] betont die Relevanz von Medien, vor allem die Fernsehberichterstattung, wenn es um die Angst der Bevölkerung nach Terroranschlägen geht. Doch nicht nur das Fernsehen, sondern gerade das Internet wird von terroristischen Gruppen zunehmend genutzt, um eine größere Zielgruppe zu erreichen [SeJa11], was beispielsweise durch Sharing-Plattformen wie YouTube oder soziale Netzwerke wie Facebook begünstigt wird.

Die Frage ist nun, ob die Bekämpfung dieser Angst und somit die Schaffung eines Gefühls der Sicherheit der Bevölkerung nur durch gravierende Einschnitte in die Privatsphäre erreichbar wäre. [DS04] untersuchten nach den Anschlägen am 11. September 2001 die Bereitschaft der amerikanischen Bevölkerung, Bürgerrechte gegen höhere persönliche Sicherheit einzutauschen und fanden heraus, dass sich diese Bereitschaft mit zunehmendem Gefühl nach Bedrohung verstärkt. Eine Studie, die diesen Zusammenhang in Europa untersuchte, konnte hingegen keine signifikante Korrelation erkennen [FR15]. [De02] diskutiert den Zusammenhang von Freiheit (und Privatsphäre gehört dazu) und Sicherheit im Kontext des Terrorismusbekämpfungsgesetz, schlussfolgert jedoch, dass dieses eher der Dialektik von Schutz und Angst folgt. Zur Abwägung von Sicherheit und Freiheit im Kontext von

Terror stellt [Le04] fest, dass Sicherheit auch keine abwägungsfähige Position darstellt, da sie sich nur negativ als Abwehr von Gefahren definieren lässt.

[BR15, S.10] machen deutlich, dass seit der NSA-Affäre 2013 und den Enthüllungen durch Edward Snowden, die aufkommende Prämisse die Verschlüsselung der eigenen Daten im Internet und gerade in sozialen Netzwerken war. Jedoch gab es in der Bevölkerung auch vor Snowden schon den Wunsch nach mehr Privatsphäre [MD03]. [BR15, S.10] sprechen hier von einer erhöhten öffentlichen Besorgnis über persönliche Daten und Privatsphäre, wodurch sich ebenso der Einsatz von Verschlüsselungs-Tools, bspw. Programme wie „Tor“, bei Privatpersonen erhöhte. Doch auch die Betreiber sozialer Netzwerke selbst verwenden nun erhöhte Sicherheitsvorkehrungen, wenn es den Schutz der Privatsphäre betrifft. Eine weitere wichtige Erkenntnis als direkte Folge der Snowden-Enthüllungen ist die Etablierung sogenannter „Anti-Facebook“-Netzwerke (ebd.), welche vermehrt auf Privatsphäre der Nutzer achten und Software verwenden, die eben jene Privatsphäre schützen. Aus den bisherigen Ausführungen lässt sich konstatieren, dass zumindest ab Mitte 2013 Privatsphäre einen immensen Stellenwert innerhalb der Gemeinschaft der Internetnutzer und Mitglieder sozialer Netzwerke einnahm. Eine solche Entwicklung in der Etablierung von Domänen „unterhalb des Radars“ kann und wurde, wie die Pariser Anschläge verdeutlichen, jedoch auch von Terroristen verwendet, wie diverse Internetpräsenzen von Al-Qaida, der Taliban, FARC oder nicht zuletzt dem IS darlegen.

[Ch15] betont, dass erst durch die von Terroristen verfolgte Kommunikationsstrategie im Web 2.0 das Verbrechen zu einem terroristischen Akt wird. [Tu15] beschäftigt sich mit den generellen Maßnahmen und Strategien der Terrorbekämpfung, unter anderem auch mithilfe von Kommunikation. Mit der Ermittlung möglicher Methoden zur Identifizierung Terrorverdächtiger in sozialen Netzwerken haben sich Jeberson und Sharma [JS15] befasst. Diese sind jedoch nicht dazu geeignet, die terroristischen Zellen an sich ausfindig zu machen bzw. ihre Aktivitäten zu identifizieren, sondern beziehen sich auf jene Gruppen, die radikal handeln, aber die Grenze zum Terrorismus noch nicht überschritten haben, wie in Deutschland beispielsweise die Salafisten. Darüber hinaus besteht auch die Möglichkeit der Einbeziehung von öffentlich zugänglichen Nutzer-Postings zu Zwecken der Informationsgewinnung durch die Behörden in Krisensituationen. Sutton et al. [Su08] sprechen in diesem Kontext von sogenannten *Backchannels*, einer besonderen Form des Data Minings. Hierzu zählen Nutzerbeiträge, Videos, Geotags, Bewegungsprofile und dergleichen. Hinsichtlich der Früherkennung bzw. Überwachung terroristischer Aktivitäten im Netz können diese -Informationen in Kombination mit anderen Methoden als weiteres Überwachungsinstrument zum Einsatz kommen. [Re13] beschäftigt sich mit der Förderung der Entstehung von Communities in sozialen Medien, was [Lu16] mit Methoden der Nachvollziehbarkeit des Übergangs von Publics zu Communities aufgreift.

Eine generelle Grundlage zur Anwendung von Methoden zur Identifizierung und Überwachung potentieller terroristischer Aktivitäten ist die schon seit langem kontrovers diskutierte Vorratsdatenspeicherung, bei der es sich um ein Konzept zur kurzzeitigen

Aufbewahrung aller benutzergenerierten Daten handelt. Dies erlaubt ein Abbild der Kommunikation im (deutschsprachigen) Web, auf welche die Behörden durch die Kooperation mit IT-Dienstleistern Zugriff erhielten. Auf diese Weise ist zwar keine Überwachung in Echtzeit möglich, jedoch wird sich davon eine erhöhte Aufklärungsrate nach begangenen Straftaten versprochen. Dies stößt in der deutschen Bevölkerung bislang auf erheblichen Widerstand aufgrund der damit einhergehenden immensen Einschränkung der Privatsphäre der Internetnutzer [Ko16]. Beispielsweise haben die Politiker Burkhard Hirsch, Gerhart Baum und Sabine Leutheusser-Schnarrenberger in diesem Sinne eine Erklärung zur Vorratsdatenspeicherung abgegeben, um unbegründete Eingriffe in die Privatsphäre der Internetnutzer zu verhindern [Ku16]. Inwiefern dieses Instrument somit tatsächlich zur Anwendung kommen könnte, bleibt vorerst fraglich.

Zusammenfassend zeigt die Literaturrecherche, dass das Internet im Allgemeinen und die sozialen Netzwerke im Speziellen von allen beteiligten Akteuren (Nutzer, Behörden als auch terroristische Gruppierungen) aktiv genutzt werden. Zum anderen steht ebenso fest, dass es Methoden gibt, um Antiterrormaßnahmen im Internet zu etablieren, diese sich jedoch alle im bisherigen legalen Rahmen bewegen sollten und durch die Sensibilität in Folge der Spionageaffäre um Edward Snowden begrenzt zu sein scheinen. Der entscheidende Aspekt hierbei ist die Grenze zwischen der gewünschten Privatsphäre der Bevölkerung und deren Sicherheitsbedürfnis. Da in Mitteleuropa ein Anschlag stattfand und dieser über ein Netzwerk geplant worden war, stellt sich die Frage, ob eine Bereitschaft besteht, die bisherigen Methoden, wie von Jeberson und Sharma [JS15] erläutert, weiter auszubauen und die Privatsphäre der Nutzer sozialer Medien einzuschränken, um den Behörden einen größeren Handlungsspielraum innerhalb des Internets zu ermöglichen. Anhand der vorliegenden Literatur kann folgende Hypothese formuliert werden: Im Kontext der Terrorismuswahrnehmung sind trotz des Wunsches nach Privatsphäre die Nutzer sozialer Medien bereit, Teile ihrer Privatsphäre zugunsten erhöhter Sicherheit zumindest partiell und temporär aufzugeben. Es soll eruiert werden, ob für erweiterte Sicherheitsmaßnahmen (weltliche und digitale) Akzeptanz in der Bevölkerung besteht – gerade wenn ein gewisser Freiheitsverlust damit einherginge.

Die Forschungsfrage lautet: *Welche Auswirkungen haben terroristische Aktivitäten auf das Sicherheitsempfinden und inwieweit ist die Bevölkerung bereit, auf Freiheiten zu Gunsten von erhöhter Sicherheit zu verzichten?*

3 Empirische Studie

Um die dargestellten Fragestellungen und Ziele dieser Arbeit zu erreichen, wurde eine mehrheitlich quantitative, jedoch dennoch explorative, Umfrage durchgeführt, welche sowohl das Sicherheitsempfinden der Bevölkerung als auch deren Wünsche erfassen soll. Der Fokus dieser Umfrage lag auf der Erschließung der Frage, ob die Probanden für das Versprechen nach mehr Sicherheit auf Teile ihrer Privatsphäre verzichten würden. Die quantitativen Fragen enthielten sowohl nominales als auch ordinales Skalenniveau.

Ersteres bezog sich vor allem auf Fragen der Wünsche oder bisheriger Erfahrungen der Probanden, letzteres auf von uns gestellte Aussagen, welche die Probanden bewerten sollten. Dadurch konnte nicht nur ein Cluster an individuellen Erfahrungen und Meinungen erstellt, sondern auch, im Falle der persönlichen Meinungen der Probanden zu utopischen Aussagen, ein Stimmungs- bzw. Prioritätencluster angelegt werden.

1. Nutzen Sie soziale Netzwerke?
2. Welche sozialen Medien nutzen Sie am häufigsten?
3. Weshalb nutzen Sie soziale Medien?
4. Ich habe auch schon einmal in sozialen Netzwerken beobachtet, dass radikale Gruppen oder Einzelpersonen dort Präsenz zeigen.
5. In welcher Form haben Sie bereits Extremismus bzw. Radikalismus in sozialen Medien erlebt?
6. Um welchen Inhalt ging es dabei?
7. Wie reagieren Sie, wenn Sie Kommentare und Postings solcher Gruppen oder Personen lesen?
8. Nach den Anschlägen von Paris: Wie sicher fühlen Sie sich in Deutschland?
9. Wie empfinden Sie die vorhandenen Sicherheitsmaßnahmen gegen Terrorismus (z. B. Polizei und Grenzschutz) in Deutschland?
10. Welche der folgenden Sicherheitsmaßnahmen würden Ihr Sicherheitsgefühl verstärken?
11. Wenn es der Aufspürung von Terroristen diente, würde ich auf Bereiche meiner Privatsphäre in sozialen Netzwerken verzichten (z. B. durch generelles Erfassen privater Nachrichten).
12. In welchen Bereichen sind Sie dazu bereit, auf Teile Ihrer Privatsphäre in sozialen Netzwerken zu verzichten?
13. Geschlecht
14. Wie alt sind Sie?
15. Welchen Schulabschluss haben Sie erlangt?
16. Welcher Tätigkeit gehen Sie nach?

Tabelle 1: Fragen

Auf die mithilfe von Google Forms erstellte Online-Umfrage, welche von uns über soziale Medien, E-Mail-Verteiler und persönliche Ansprache an die Teilnehmer der Studie verteilt wurde, erhielten wir Antworten von 61 Probanden aus Deutschland ab 18 Jahren. Der größte Anteil der Probanden lag in der Altersgruppe zwischen 18 und 30 Jahren (67%), mit einem ausgewogenen Verhältnis beim Geschlecht der Teilnehmer (49% weiblich, 51% männlich). Mit etwa der Hälfte der Probanden machten Studierende (49%) den Großteil der Teilnehmer aus (Abb. 1).

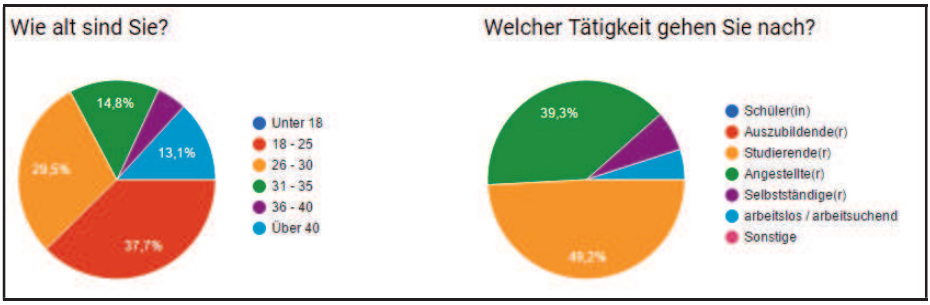

Abb. 1: Angaben der Probanden auf die Fragen nach ihrem Alter und der Tätigkeit (n = 61).

Die Teilnehmer können selbstverständlich weder von der Anzahl noch von der Verteilung als repräsentativ angesehen werden, was den explorativen Charakter unserer Studie erklärt. Es geht uns hierbei weniger darum, vorher definierte Hypothesen

repräsentativ zu bestätigen oder zu widerlegen, sondern eine erste empirische Basis für diese Fragestellung in diesem speziellen Kontext zu schaffen. Aus diesem Grund wurden neben geschlossenen auch offene Fragen gestellt. Der Rücklauf bei der qualitativen (offenen) Antwortmöglichkeit betrug knapp 56% (n = 34). Das ist hinsichtlich der überschaubaren Anzahl an Teilnehmern als relativ hohe Rücklaufquote zu bewerten (mehr als die Hälfte) und gewährleistet ein präziseres Clustering der Probanden.

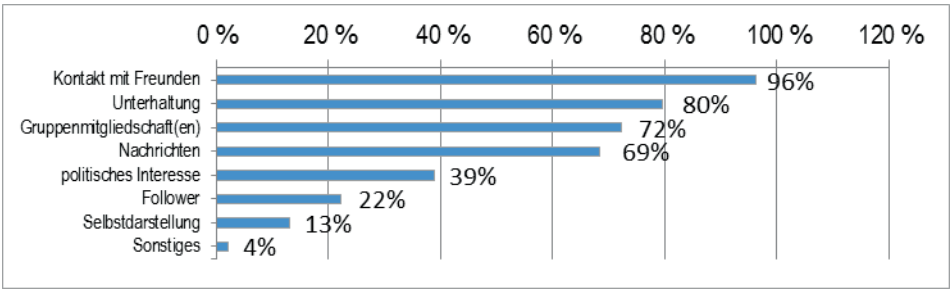

Abb. 2: Gründe für die Nutzung sozialer Medien. Mehrfachnennung möglich (n = 54).

Im Folgenden werden wir zuerst die wichtigsten Erkenntnisse der Auswertung der erhobenen Daten zusammenfassen. Anschließend folgt ein Clustering der Ergebnisse, um kausale Wirkungszusammenhänge zwischen den gegebenen Antworten zu eruieren.

3.1 Ergebnisse I: Nutzerverhalten und Umgang mit Missbrauch

Die Mehrheit der Probanden (89%) hat bereits Missbrauch in sozialen Medien (durch radikale Gruppen oder Einzelpersonen) persönlich erfahren, ob im direkten Umfeld oder über geteilte Inhalte. Auch wenn dies nicht immer im Kontext des Terrorismus erfolgt ist, erschließt sich hieraus, dass es sich bei radikalem oder extremistischem Missbrauch sozialer Medien kaum um eine Randerscheinung handeln kann. Dies ist bereits eine wichtige Erkenntnis im Hinblick auf eine potentiell positive Einstellung der Probanden zu verschärften Überwachungsmaßnahmen in sozialen Medien, denn persönliches Erleben und eigene Betroffenheit fördern im Allgemeinen die Bereitschaft zur Änderung des Status quo. Von den Probanden, die angegeben haben, schon einmal mit Extremismus oder Radikalismus in sozialen Netzwerken in Berührung gekommen zu sein (Abb. 3), geben rund 94% an, dies in Form von Kommentaren, Likes oder Shares erfahren zu haben, gefolgt von eindeutigem Bild- oder Videomaterial (69%), privaten oder öffentlichen Profilseiten (60%) sowie innerhalb von Gruppen in sozialen Medien (42%).

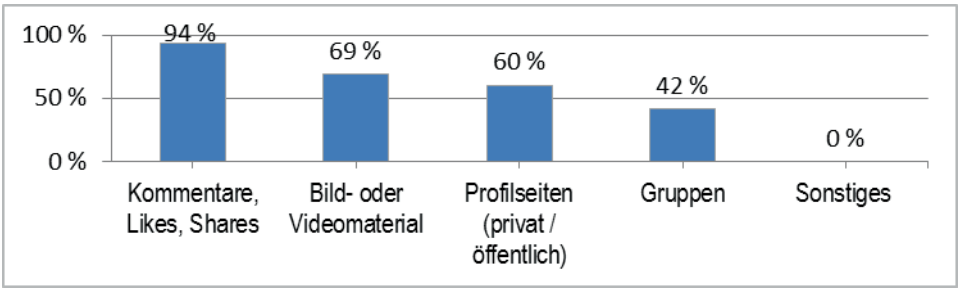

Abb. 3: Bereits erlebte Formen von Extremismus bzw. Radikalismus in sozialen Netzwerken. Mehrfachnennung möglich (n = 48).

Als interessant erweisen sich dabei auch die Antworten auf die Folgefrage nach den erlebten extremistischen bzw. radikalen Inhalten (Abb. 4). Die beiden Topantworten mit jeweils rund 94% bzw. 90% der Probanden sind erlebte Ausländerfeindlichkeit und Rassismus, gefolgt von Hetze gegen ethnische Minderheiten (56%) und gegen Homosexuelle (29%). Eine weitere wichtige Erkenntnis an dieser Stelle ist der erlebte Aufruf zur Radikalisierung in sozialen Medien durch Gruppierungen wie die Salafisten oder gar den IS von immerhin einem Viertel der Befragten (25%), die zuvor angegeben hatten, Hetze oder Extremismus erlebt zu haben. Dies ist als ein Indiz für eine aktive Präsenz solch radikaler Gruppierungen in sozialen Medien anzusehen.

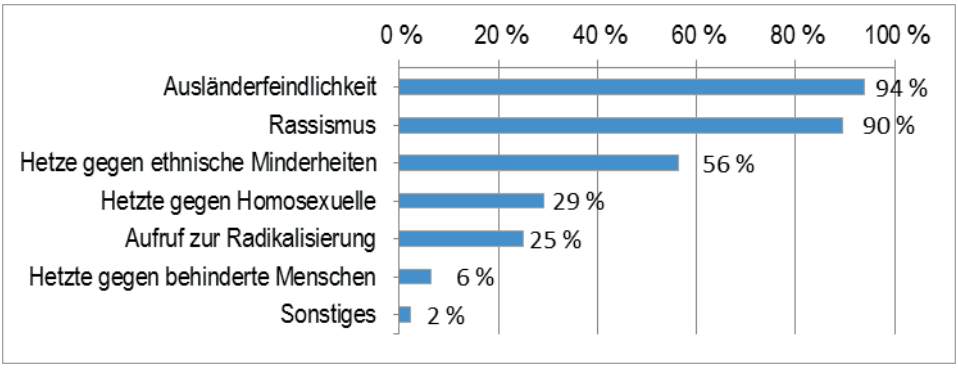

Abb. 4: Antworten auf die Frage nach bereits erlebten Inhalten von Extremismus bzw. Radikalismus in sozialen Netzwerken. Mehrfachnennung möglich (n = 48).

3.2 Ergebnisse II: Sicherheitsempfinden und Maßnahmen

Der nächste Themenblock befasste sich damit, wie die Probanden die aktuelle Sicherheitslage in Deutschland bewerten. Wir stellten fest, dass sich trotz der Anschläge von Paris knapp 49% der Probanden in Deutschland derzeit sicher fühlen, wohingegen sich 28% gegenteilig äußern, sicherlich auch von der Berichterstattung beeinflusst.

Damit einhergehend sollten die Probanden weiter die aktuellen Sicherheitsmaßnahmen in Deutschland bewerten. Auffällig ist hier, dass keiner der Probanden mit der Ausprägung „5“ (optimal) geantwortet hat und es somit keinen einzigen Probanden gibt, der die Sicherheitsmaßnahmen als optimal bezeichnen würde. Rund 33% der Probanden beurteilten diese jedoch mit einer „4“ (gut), während weitere 30% diese als ausreichend ansehen würden. Fassen wir diese beiden Gruppen zusammen, erhalten wir knapp 62% der beteiligten Probanden, welche die Sicherheitsmaßnahmen als mindestens ausreichend betrachten würden. Etwa 32% und damit die zweithäufigste gewählte Antwort auf diese Frage stellt die Ausprägung „2“ (schlecht) dar, während weitere 7% die Sicherheitsmaßnamen als sehr mangelhaft bezeichnen würden. Das Ergebnis dieser Frage ist demnach sehr ambivalent. Die beiden Topantworten stellen dabei zwei gegensätzliche Pole der Einschätzung von Sicherheitsmaßnahmen dar. Erst mit Zunahme jener Probanden, die die Sicherheitsmaßnahmen als ausreichend bezeichnen, kann festgestellt werden, dass der Großteil der Probanden (62%) die aktuellen Sicherheitsmaßnahmen als mindestens ausreichend bezeichnen würde.

Wir konnten ein Cluster darüber erstellen, welche Wünsche die Probanden bezüglich Sicherheitsmaßnahmen haben (Abb. 5). Dabei antworteten die Meisten (60%), sie wünschten sich verstärkte Polizeipräsenz, gefolgt von einer naheliegenden Schlussfolgerung, nämlich einer besseren Ausrüstung der Polizei (58%). An dieser Stelle folgt der Wunsch nach stärkerer Überwachung der Online-Kommunikation (48%).

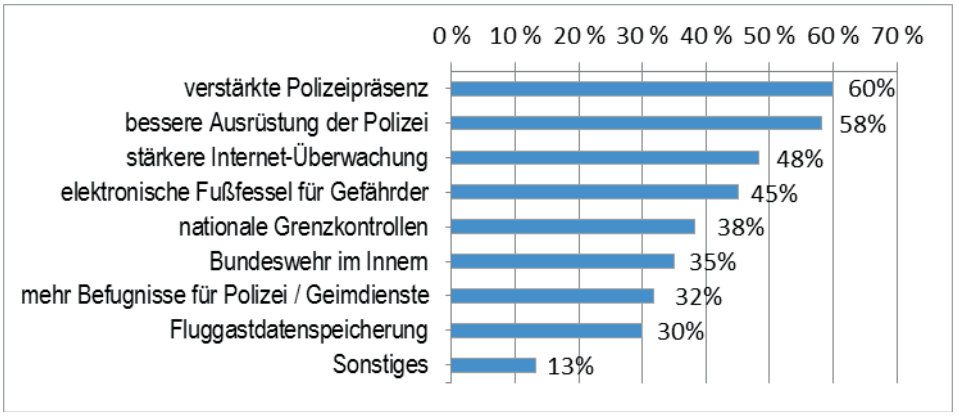

Abb. 5: Antworten der Probanden auf die Frage nach gewünschten Sicherheitsmaßnahmen gegen terroristische Aktivitäten und Bedrohungen. Mehrfachnennung möglich (n = 60).

Alleine die Betrachtung der am meisten genannten Antworten lässt darauf schließen, dass die Probanden weniger Maßnahmen im Netz als im weltlichen Raum fordern, was natürlich auch durch die Fragestellung nach radikalem Verhalten beeinflusst sein kann. Der Wunsch nach körperlicher Unversehrtheit durch erhöhte Polizeipräsenz ist dabei der Primus der genannten Antworten. Dies zeigt, dass sinnlich und körperlich erfahrbare Maßnahmen, in diesem Fall die verstärkte physische Präsenz der Exekutive, von der Bevölkerung eher begrüßt würde als beispielsweise die Überwachung von sozialen

Netzwerken, wobei es möglich ist, dass sich die Probanden digitale Maßnahmen schlechter vorstellen können, wie weltliche. Warum genau die Probanden sich durch Polizeipräsenz sicherer fühlen, kann durch die Umfrage nicht beantwortet werden. Hypothetisch könnte darauf geschlossen werden, dass die Polizei eine direktere und repressivere Maßnahme gegen Terrorismus darstellt als digitale Aufklärungsmaßnahmen, also das Sammeln und Auswerten von Daten. Dies würde sich auch mit dem Wunsch nach einer besseren Ausrüstung für die Einsatzkräfte decken.

Um jedoch weitere Meinungen und Wünsche bezüglich möglicher Sicherheitsmaßnahmen zu erfassen, die nicht zur Auswahl standen, wurde eine Option für freie Antwortmöglichkeiten gegeben. Generell können zwei Meinungscluster erstellt werden: (1) *Repressive Maßnahmen:* Der Großteil der Probanden wünscht sich repressive Maßnahmen wie verstärkte Polizeipräsenz oder deren verbesserte Ausrüstung. (2) *Präventive Maßnahmen:* Die Probanden wünschten sowohl stärkere Überwachung im Internet als auch elektronische Fußfesseln für sogenannte potentielle Gefährder. Bei diesen beiden Clustern sollte jedoch beachtet werden, dass die Grenzen zwischen repressiven und präventiven Maßnahmen fließend sind. So kann Polizeipräsenz in dem Sinne einen präventiven Charakter besitzen, indem sie mögliche Straftäter vor Gewalttaten abschreckt.

3.3 Ergebnisse III: Sicherheit vs. Privatsphäre

Auf die Frage, ob die Probanden bereit seien, auf Teile ihrer Privatsphäre in sozialen Netzwerken zu verzichten und im Gegenzug gewährleistet wäre, dass dieser Verzicht die Aufspürung von terroristischen Organisationen und ihren Anhängern begünstigt, antworteten die Probanden sehr unterschiedlich, jedoch mit leichter Tendenz. Rund 44% der Befragten wären bereit, zumindest Teile der Privatsphäre aufzugeben, während rund 36% dies verneint. Bisher muss also festgehalten werden, dass die Probanden geteilter Meinung bezüglich des Verlusts ihrer Privatsphäre im Netz zu Gunsten verbesserter Terrorbekämpfung sind. Erst mit der Ergänzung der folgenden, offenen Frage kann ein präziseres Meinungs-Cluster erstellt werden. Vor allem die Meinungen jener Probanden, die sich bei dieser Frage unschlüssig waren, also die eine „3“ auf der Skala angegeben haben, können damit näher untersucht werden (Abb. 6).

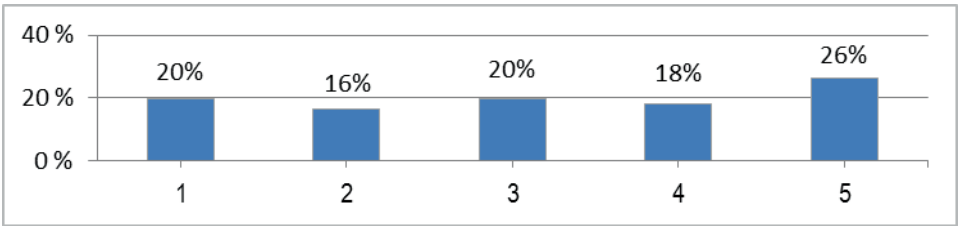

Abb. 6: Antworten auf die Frage nach der Bereitschaft zum Verzicht auf Privatsphäre zu Gunsten erhöhter Sicherheit (n = 61). Skala: 1 (stimme gar nicht zu) bis 5 (stimme vollkommen zu).

Nach der Analyse beider Fragen konnten in Bezug auf den *Verzicht auf Privatsphäre zugunsten von Sicherheit* drei Meinungscluster erstellt werden, welche im Folgenden erläutert werden sollen:

Starke Zuneigung (44%): Diese Gruppe, welche bei der Frage nach der Bereitschaft zum Verzicht auf Privatsphäre zu Gunsten erhöhter Sicherheit mit Ausprägung „4" oder „5" geantwortet haben, betrachten soziale Medien als öffentlichen Raum und argumentieren, dass jeder selbst entscheiden müsse, welche Informationen er in diesem öffentlichen Raum zulässt *(„[…] wer soziale Netzwerke nutzt, sollte sich im Klaren sein, was er dort postet*", P41). Sollte es der Aufspürung von Terroristen dienen, wären jene Probanden bereit, ihre Privatsphäre aufzugeben (*„Komplette Kommunikation über soziale Netzwerke sollte für Behörden einsehbar sein"; „Facebook und WhatsApp sollten vollkommen überwacht werden")*, da sie diese in den sozialen Medien entweder als nicht gegeben betrachten oder bereit sind, einzelne Teilaspekte komplett offenzulegen (*„Gerne können FÜR SOLCHE ZWECKE sogar auch meine Nachrichten gelesen werden")*. Dazu zählen Gruppenzugehörigkeit oder private Nachrichten.

Starke Abneigung (36%): Ein etwas geringerer Anteil steht dem konträr gegenüber und ist strikt gegen eine Überwachung sozialer Medien und nicht dazu bereit, Teile seiner Privatsphäre aufzugeben (*„Auf keinen Fall. Ich habe nichts mit Terrorismus zu tun"; „In keinem Bereich")*. Sehr interessant ist dabei die Antwort eines Probanden, welche sich auch mit denen der restlichen „Gegner" des Verzichts auf Privatsphäre deckt: „*Privatsphäre gegen Sicherheit einzutauschen, erscheint mir generell nicht fair: Sicherheit kann nicht zu 100% gewährleistet werden. Darum wäre ich nicht bereit, auf Privatsphäre zu verzichten*" (P14). Dieses Stimmungsbild durchzieht dieses Cluster in seiner Gesamtheit und zeigt, dass jene Probanden nicht an eine vermehrte Sicherheit durch die Überwachung sozialer Medien glauben, gar deren Missbrauch fürchtet (*„Generell dient die Überwachung zum größten Teil der Marktforschung oder der Kontrolle der Bürger")*, den Behörden nicht vertraut (*„Weg vom Überwachungsstaat!!!!")* und somit auch nicht bereit sind, Teile seiner oder ihrer Privatsphäre aufzugeben.

Kompromissbereitschaft (20%): Zu denjenigen, die auf der Skala mit einer „3" geantwortet haben, kann durch die Hinzunahme der offenen Antwort ein Stimmungsbarometer hinzugefügt werden. Diese Personen würden ohne triftigen Grund seitens der Behörden nicht auf ihre Privatsphäre verzichten, würden aber im Gegenzug zur Verhinderung von Straftaten und dergleichen einen Kompromiss eingehen und „Hilfe anbieten" (*„Sollte es dazu dienen, eine Auflösung/Aufklärung von beispielsweise Straftaten oder Verdachte jeglicher Art zu unterstützen, ließe ich mich allerdings auf Kompromisse ein und würde meine Unterstützung anbieten"; „Wenn dadurch ein Terroranschlag verhindert wird, in allen Bereichen")*.

Nicht zu unterschätzen sind nach dieser Cluster-Bildung zwei Sachverhalte. Zunächst zeigt sich, dass das Cluster „Starke Zuneigung" die größte Gruppe darstellt. Ebenso erkennt man anhand der offenen Antworten, dass der Verzicht der Privatsphäre in

sozialen Räumen kein Novum für diese Gruppe darstellt *(„[…] soziale Netzwerke sind ja quasi ein öffentlicher Raum“)*. Der zweite Sachverhalt betrifft die Synergie zwischen den Clustern „Starke Zuneigung“ und „Kompromissbereitschaft“. Letzteres Cluster ist ebenso bereit, Teile ihrer Privatsphäre zumindest partiell oder temporär aufzugeben (*„Öffentliche Beiträge/Profile, da diese ein breites Publikum betreffen und beeinflussen können. KEIN Mitlesen privater Nachrichten“)*. Betrachten wir beide Gruppen als Einheit, erkennen wir den Trend, dass der Verzicht der Privatsphäre tatsächlich eine Möglichkeit für den Großteil der Befragten, nämlich knapp 64%, darstellt.

4 Diskussion: Sicherheit und/oder Privatsphäre

Die anfänglichen Überlegungen hinsichtlich der Auswirkungen der NSA-Spähaffäre um Edward Snowden auf das Bedürfnis nach Privatsphäre in der Bevölkerung scheinen im starken Kontrast zu stehen zum gleichzeitigen Bedürfnis nach Sicherheit – gerade nach den terroristischen Anschlägen von Paris und Brüssel. Bei Betrachtung der Erkenntnisse aus unserer Studie in Bezug auf repressive und präventive Maßnahmen sowie die Meinungscluster starke Zuneigung, starke Abneigung und Kompromissbereitschaft gegenüber dem Verzicht auf Privatsphäre zu Gunsten erhöhter Sicherheit lässt sich zunächst festhalten, dass es scheinbar keine allgemeingültigen Lösungsansätze geben kann, die alle zufriedenstellen. Dies deckt sich auch mit den nicht konsistenten Forschungsergebnissen zu jenem Thema [DS04, FR15].

Greifbar an dieser Stelle ist jedoch eine Tendenz zur Zuneigung respektive Kompromissbereitschaft der Probanden hinsichtlich des (zumindest teilweisen) Verzichts auf Privatsphäre für ein verstärktes Sicherheitsempfinden. Immerhin ist das Gros der Teilnehmer (64%) dieser Auffassung. Somit ergeben sich hier zumindest Chancen für den Staat bzw. Behörden und Organisationen mit Sicherheitsaufgaben (BOS), neue respektive, bislang verwehrte Antiterrormaßnahmen zu etablieren.

An dieser Stelle möchten wir auf eine Studie der R+V Versicherung [RV15] zurückgreifen, die sich als Langzeitstudie seit Mitte der 1990er mit den Ängsten der Deutschen befasst. Die Erkenntnisse dieser Studie korrelieren mit unseren Umfrageergebnissen. Insbesondere seit den Anschlägen vom 11. September 2001 in den USA ist ein signifikanter Anstieg der Furcht vor terroristischen Anschlägen zu verzeichnen. Seither hat sich die Sorge davor in der deutschen Bevölkerung verdoppelt. Zwar sind Schwankungen bei der Angabe von Terrorangst in den letzten 15 Jahren zu beobachten, doch mit durchschnittlich 46% in den Jahren ab 2001 liegt das „Angstniveau“ der Deutschen fast doppelt so hoch wie noch in den 1990er-Jahren. Hier wäre darüber hinaus die Frage zu stellen, welche Einflussfaktoren (neben den Attentaten selbst) dazu geführt haben. Zu den Variablen zählen unter anderem die Medienberichterstattung durch die Presse (insbesondere die Art und Weise der Darstellung) und die damit verbundene Wahrnehmung durch die Rezipienten, die zeitlichen Abstände von Anschlägen (Aktualität) oder die direkte bzw. indirekte

Betroffenheit. Diese Studie führt die Angst der Deutschen vor Terrorismus auf dem zweiten Platz (52%), gefolgt von der Sorge vor Naturkatastrophen (53%).

Wie bereits Gethmann [Ge96] festgestellt hat, ist die Angst jedoch kein guter Ratgeber. Dies ist insbesondere für Behörden und Politik von großer Bedeutung: Kurzfristige, übereilte Reaktionen auf terroristische Bedrohungen sind daher gewissermaßen als ambivalent zu betrachten. Einerseits können schnelle, zeitnahe Antiterrormaßnahmen der Bevölkerung ein Gefühl von Sicherheit im Sinne von Handlungsfähigkeit und Entschlossenheit der Regierung vermitteln. Andererseits – und dies ist ein nicht zu unterschätzendes Risiko – können übereilte Maßnahmen als Kurzschlussreaktion auf Bedrohungen oder Attentate (un-)absehbare, negative Auswirkungen auf die Freiheit und Privatsphäre der Bevölkerung haben. Eine extreme Ausprägung dieser Art wäre beispielsweise die Charakteristik eines Polizeistaats, zu der die totale Überwachung zählt und somit der Freiheit und Privatsphäre entgegenwirkt. Auch der nicht selten geäußerte Wunsch unserer Probanden nach dem Einsatz der Bundeswehr im Innern (Abb. 5) kann als intuitiver „Schnellschuss“ interpretiert werden.

Aus diesem Grund empfiehlt sich stets eine mittel- bis langfristige Evaluierung einer Bedrohung und entsprechender Gegenmaßnahmen sowie deren Konsequenzen für die Bevölkerung, bevor endgültige Entscheidungen gefällt werden. In Anlehnung an das *Time-lag*-Prinzip aus den Wirtschaftswissenschaften oder die *Cultural Lag*-Theorie nach Ogburn [Og57] ist es im übertragenen Sinne empfehlenswert, stets einen zeitlichen Verzögerungseffekt bei Entscheidungsfindungen zu beachten. Denn das Abwarten der Effekte terroristischer Anschläge kann von Vorteil sein, bevor politische Entscheidungen im Hinblick auf den Einsatz der genannten Methoden gefällt werden. Hierdurch kann gewährleistet werden, dass keine voreiligen Entscheidungen zu ungewollten Konsequenzen führen wie z. B. ein nicht-intendierter Freiheitsverlust seitens der Bevölkerung.

5 Fazit: Keine klare Tendenz, aber Kompromissbereitschaft

Privatsphäre und Sicherheit stehen in einem Spannungsfeld. Der 2013 ausgelöste NSA-Skandal durch Edward Snowden und der daraus resultierende „Privatsphäre-Boom“ scheinen noch aktuell zu sein. Viele der Probanden unserer Studie, welche dem zweiten Cluster „Starke Abneigung“ zugeordnet werden konnten, argumentieren damit, dass eine Überwachung aufgrund nie erreichter absoluter Sicherheit nur der Spionage der eigenen Bevölkerung aufgrund von Marktforschung bzw. Kontrolle diene. Auf der anderen Seite, dem ersten Cluster „Starke Zuneigung“, wünschen sich gerade diese Probanden eine Überwachung des Internets und betrachten dieses als öffentlichen Raum. Diese beiden Cluster, da ungefähr gleich groß in ihrer Anzahl an Probanden, zeigen die zwei Extreme, welches dieses Thema hervorruft. Interessant ist dabei das dritte Cluster derjenigen, die eine „Kompromissbereitschaft“ zeigen. In diesem Fall zeigt sich, dass jene Probanden zwar auf ihre Privatsphäre achten, in dringenden Verdachtsfällen aber zumindest auf

Teile ihrer Privatsphäre verzichten würden.

Ein Trend (Privatsphäre oder Sicherheit) kann nach unserer Umfrage nicht ausgemacht werden, wenn nur die einzelnen Cluster betrachtet werden. Zwar besteht die Kompromissbereitschaft zur Aufgabe der Privatsphäre, jedoch nur im Gegenzug des Versprechens einer Prävention oder Aufspürung der Verursacher terroristischer Attacken. In diesem Fall bleibt festzuhalten, dass der Wunsch nach Privatsphäre immer noch gegeben ist, in unserer Studie jedoch auffiel, dass sich das Bewusstsein gegenüber sozialen Netzwerken als öffentlicher Raum geändert hat und eine generelle Kompromissbereitschaft besteht, Teile der Privatsphäre in sozialen Netzwerken aufzugeben. Erst wenn wir aufgrund ihrer inhaltlichen Übereinstimmung die Cluster „Starke Zuneigung“ und „Kompromissbereitschaft“ als eine Einheit betrachten, kann jener Trend, soziale Netzwerke als öffentliche Räume mit eingeschränkter Privatsphäre zu begreifen, die bei Bedarf wie in der Realität, durch exekutive Organe interveniert werden können, aufgezeigt werden.

Die Kompromissbereitschaft bzw. die starke Zuneigung zu einer Überwachung von Teilen der sozialen Netzwerke kann aus einer anderen Feststellung erfolgen, nämlich der, dass etwa 89% aller Probanden bereits Auftritte radikaler Vereinigungen bzw. Zeuge von radikalen und extremistischen Äußerungen in sozialen Netzwerken wurden. Zieht man noch hinzu, dass in den Nachrichten durch den Vormarsch des IS, das Erstarken rechtspopulistischer Parteien und der Flüchtlingsdebatte, die Diskussion über den Umgang mit diesen Themen im Vordergrund steht, so kann man davon ausgehen, dass einige der Probanden, die zu den Clustern „Starke Zuneigung“ und „Kompromissbereitschaft“ gehören, mit einer anderen Sichtweise auf diese Parteien, Gruppierungen und extremistisches Gedankengut reagieren bzw. dieses öfter oder in einer kritischeren Form in den sozialen Medien erlebt haben. Um diese Querverweise jedoch fundiert zu eruieren, benötigt es einer weiteren Studie, die sich genauer mit der Erfahrung extremistischen Gedankenguts in sozialen Medien beschäftigt. Darüber hinaus ist eine Untersuchung notwendig, welche soziokulturellen und -ökonomischen Merkmale die Probanden der einzelnen Cluster aufweisen.

Als Fazit kann und muss nach dieser Studie jedoch weiterhin davon ausgegangen werden, dass Sicherheitsmaßnahmen auf Kosten von Privatsphäre im öffentlichen Raum zwiespältig betrachtet werden. Die Enthüllungen durch Snowden haben möglicherweise immer noch Einfluss auf die Sensibilisierung der Privatsphäre in sozialen Netzwerken, die Anschläge des IS hingegen zeigen, dass Kompromissbereitschaft existiert, ihre Privatsphäre in diesen Medien einzuschränken. Eine generelle Tendenz hin zur bedingungslosen Bereitschaft, die Privatsphäre zugunsten von Sicherheit aufzugeben, konnte nicht gezeigt werden.

Danksagung: Die Forschungsarbeiten wurden im Rahmen des BMBF-Projekts „KOKOS“ (Fö.-Kz. 13N13559) sowie im Rahmen des EU-FP7-Projekts „EmerGent“ (Fö.-Kz. 608352) gefördert. Die Fragestellung und kompakte Eindrücke basieren auf [Re16].

Literaturverzeichnis

[BR15] Bartlett, Jamie; Reynolds, Louis: State of the art 2015: a literature review of social media intelligence capabilities for counter-terrorism, Demos (2015)

[Ch15] Christoph, Stefan: Funktionslogik terroristischer Propaganda im bewegten Bild. In: Journal for Deradicalization Bd. Fall/15 (2015), Nr. 4, S. 145–205

[DS04] Davis, Darren W.; Silver, Brian D.: Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America. In: American Journal of Political Science Bd. 48 (2004), Nr. 1, S. 28–46

[De02] Denninger, E: Freiheit durch Sicherheit? Anmerkungen zum Terrorismusbekämpfungsgesetz. In: Aus Politik und Zeitgeschichte Bd. 10/11 (2002), S. 22–30

[Fr15] Friedewald, Michael; Lieshout, Marc van; Rung, Sven; Ooms, Merel; Ypma, Jelmer: Privacy and Security Perceptions of European Citizens: A Test of the Trade-off Model. In: IFIP Advances in Information and Communication Technology Bd. 457 (2015), S. 54–70

[Ge96] Gethmann, Carl Friedrich: Ist die Angst ein schlechter Ratgeber? In: 5. Essener Forum für psychosoziale Versorgung, 1996

[Gr09] Grimm, A.; Hulse, L.; Schmidt, S.: Risikowahrnehmung und psychologische Reaktionen in öffentlichen Krisensituationen am Beispiel von Terrorattentaten. In: Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz Bd. 52 (2009), Nr. 12, S. 1129–1140

[Ja07] Jackob, Nikolaus: Die Diffusion von Terrormeldungen, die Wirkung von Anschlägen auf die öffentliche Meinung und die Folgen für das Vertrauen in der Demokratie. In: Glaab, S. (Hrsg.): Medien und Terrorismus - auf den Spuren einer symbiotischen Beziehung.. Band 3. Aufl. Berlin : Berliner Wissenschafts-Verlag, 2007 — ISBN 978-3-8305-1435-0, S. 155–174

[Je15] Jeberson, W; Sharma, Lucky: Survey on counter Web Terrorism. In: COMPUSOFT, An international journal of advanced computer technology Bd. 4 (2015), Nr. 5, S. 1744–1747

[Ko16] Koshan, Mansoor: Vorratsdatenspeicherung – verfassungsrechtliche Rahmenbedingungen und rechtspolitische Verortung. In: Datenschutz und Datensicherheit - DuD Bd. 40 (2016), Nr. 3, S. 167–171

[Ku16] Kurz, Constanze: Erklärung zur Vorratsdatenspeicherung: „Eingriff in die Privatsphäre von Millionen Menschen“. . — netzpolitik.org

[Le04] Lepsius, Oliver: Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland. In: Leviathan Bd. 32 (2004), Nr. 1

[Lu16] Ludwig, Thomas; Reuter, Christian; Pipek, Volkmar: From Publics to Communities: Tracing the Path of Shared Issues through ICT. In: Computer Supported Cooperative Work: The Journal of Collaborative Computing (JCSCW) Bd. 25 (2016), Nr. 2-3, S. 193–225

[MD03] Metzger, Miriam J.; Docter, Sharon: Public Opinion and Policy Initiatives for Online Privacy Protection. In: Journal of Broadcasting & Electronic Media Bd. 47 (2003), Nr. 3, S. 350–374

[Og57] Ogburn, William F.: Cultural lag as theory. In: Sociology and Social Research Bd. 41 (1957), Nr. 3, S. 167–174

[Re16] Reuter, Christian; Gellert, Robin; Geilen, Gordian: Reception of Terror in Germany – Security, Privacy and Social Media. In: Adjunct Proceedings of 30th EnviroInfo Conference. Berlin, 2016

[Re13] Reuter, Christian; Heger, Oliver; Pipek, Volkmar: Combining Real and Virtual Volunteers through Social Media. In: Comes, T.; Fiedrich, F.; Fortier, S.; Geldermann, J.; Müller, T. (Hrsg.): Proceedings of the Information Systems for Crisis Response and Management (ISCRAM). Baden-Baden, Germany, 2013, S. 780–790

[Re11] Reuter, Christian; Pohl, Patrik; Pipek, Volkmar: Umgang mit Terminologien in inter-organisationaler Krisenkooperation - eine explorative Empirie. In: Eibl, M. (Hrsg.): Mensch & Computer 2011: Übermedien Übermorgen. München, Germany : Oldenbourg-Verlag, 2011.

[Rv15] R+V Versicherung: R+V Studie – Die Ängste der Deutschen. URL https://www.ruv.de/presse/aengste-der-deutschen

[SJ11] Seib, Philip; Janbek, Dana M.: Global Terrorism and New Media: The post-Al Qaeda Generation. New York : Routledge, 2011

[Su08] Sutton, Jeannette; Palen, Leysia; Shklovski, Irina: Backchannels on the Front Lines: Emergent Uses of Social Media in the 2007 Southern California Wildfires. In: Friedrich, F.; Van de Walle, B. (Hrsg.): Proceedings of the Information Systems for Crisis Response and Management (ISCRAM). Washington D.C., USA, 2008.

[Tu15] Turk, Austin T.: Terrorism and Counterterrorism. In: Goode, E. (Hrsg.): The Handbook of Deviance. Hoboken, NJ : John Wiley & Sons, Inc, 2015, S. 537–548

[We02] Werthes, Sascha; Conrad, C; Kim, R: Die Terrorkrise als Medienereignis? Internationale Krisenkommunikation - Eine Herausforderung im 21. Jahrhundert. In: Schicha, C.; Brosda, C. (Hrsg.): Medien und Terrorismus. Münster : Lit-Verlag, 2002 — ISBN 3-8258-5923-1

[We07] Weichhart, Peter: Risiko - Vorschläge zum umgang mit einem schillernden Begriff. In: Berichte zur Deutschen Landeskunde Bd. 81 (2007), Nr. 3, S. 201–214

[Wo12] Wollebæk, Dag; Enjolras, Bernard; Steen-Johnsen, Kari; Ødegård, Guro: After Utøya: How a High-Trust Society Reacts to Terror—Trust and Civic Engagement in the Aftermath of July 22. In: PS: Political Science & Politics Bd. 45 (2012), Nr. 01, S. 32–37