

## Terrorabwehr im Internet

*Terror überschattet zunehmend den Alltag, auch in Europa, gefährdet jeden Einzelnen. Konspiration hinterlässt im digitalen Zeitalter besonders viele Spuren. Nicht nur Politiker kommen immer häufiger auf die Idee, Digitalisierung zur Bekämpfung und Verhinderung gewalttätiger Aktionen einzusetzen. OBJEKTSpektrum fragte beim ersten Internetsoziologen Deutschlands, Dr. Stephan Humer, der als Gründungsvorsitzender über 500 Wissenschaftler und andere Experten in einem Netzwerk zu dieser Thematik zusammenbringt, nach.*

### „Gegenrede halte ich für eine der vielversprechendsten Lösungen“: Interview mit dem Internetsoziologen Dr. Stephan Humer

**OBJEKTSpektrum:** Herr Dr. Humer, Ihr Schwerpunkt als Vorsitzender des Vereins Netzwerk Terrorismusforschung e. V. sind die Verwebungen von Digitalisierung und Terrorismus. Eine Sprecherin des Al-Kaida-Monitoring-Teams, das im Auftrag des UNO-Sicherheitsrates die Internetnutzung von Individuen und mehr als 75 Terrorgruppen überwacht, bezeichnete das Internet als „Schweizer Taschenmesser für Terroristen“. Und sie sorgte sich über „böse Anwendungen des Internets [...] wie Verschlüsselung.“ – Sind Hintertüren gut und Verschlüsselung böse im Kampf gegen IS und Co.?

*Stephan Humer: Nein, denn das wichtigste Ziel sollte immer sein, die Gründe für Terrorismus zu beseitigen. Das ist natürlich schwierig bis unmöglich – es wird immer entsprechende Bestrebungen geben –, aber trotzdem sollte man bei jeder repressiven Maßnahme die Verhältnismäßigkeit bedenken. Leider ist auch über 20 Jahre nach Beginn der Massenverbreitung des Internets immer noch kein ausreichendes ganzheitliches Bewusstsein bei vielen Verantwortlichen zu beobachten: Die Politik ist schnell mit sinnlosen Maßnahmen, die ganz und gar unverhältnismäßig sind, aber zumindest nach Handlungsfähigkeit aussehen und damit Sinnhaftigkeit nur vorgaukeln. Auf Dauer schadet das aber sowohl der Politik als auch der Gesellschaft. Ich plädiere deshalb seit jeher für die Berücksichtigung der Eigengesetzlichkeiten von Digitalisierung und ihrer gesellschaftsverändernden Potenziale. Nur dann können digitale Anti-Terror-Maßnahmen sinnvoll sein. Verschlüsselung pauschal zu verdammen, ignoriert diesen Aspekt und ist damit in letzter Konsequenz Unsinn.*

*Die US-Regierung hat die großen Konzerne des Silicon Valleys wie Apple, Facebook, Twitter und Microsoft eingeladen, um zu beraten, wie sich die Digitalisierung für den Kampf gegen den Terrorismus nutzen lässt. Nach dem Motto: Wer traditionelle Unternehmensbranchen auseinandernehmen kann, schafft das auch mit terroristischen Vereinigungen. Ist eine solche Instrumentalisierung der IT eine Chance?*

*Die IT-Branche muss natürlich ihren Teil beitragen, denn sie ist Teil der Gesellschaft, die von Terrorismus betroffen ist. Trotzdem muss man auch hier klar sagen: Verteidigung von Demokratie: ja, das müssen wir alle machen, auch Firmen. Konzerne als Hilfsheer? Ganz klar: nein. Polizei und Nachrichtendienste dürfen ihre Aufgaben nicht outsourcen, sondern müssen endlich Digitalisierung grundsätzlich verstehen lernen.*

*„Anonymous“ will mit Hacking und Löschen den Terrorismus bekämpfen. Ein legitimes Mittel für ein gutes Ziel?*

Dr. phil. Stephan G. Humer (Diplom-Soziologe und Informatiker) ist seit März 2013 Gründungsvorsitzender des Netzwerks Terrorismusforschung e. V. (NTF). Seine Sicherheitsforschungsschwerpunkte liegen dort in den Bereichen Terrorismus/Extremismus in der digitalen Sphäre und OSINT (Open Source Intelligence). Er ist außerdem Mitgründer der Deutschen Gesellschaft für Informationsfreiheit e.V., aktiv im Forschernetzwerk „Surveillance Studies“ (Uni Hamburg) und Mitglied der Arbeitsgruppe „Identitätsschutz im Internet“

(Uni Bochum). Zudem machte er sich als Gründer und Forschungsleiter des ersten Arbeitsbereichs Internetsoziologie in Deutschland an der Universität der Künste (UdK) Berlin in der digitalen Szene einen Namen. Seit März 2016 ist Humer Hochschuldozent und Leiter des Forschungs- und Arbeitsbereiches Internetsoziologie im Fachbereich Wirtschaft und Medien der Hochschule Fresenius Berlin. Damit ist Humer als „Digitalisierungserklärer“ das Gesicht des Forschungsfeldes Internet und Gesellschaft im deutschsprachigen Raum. Sein Wirken gilt der Analyse der Digitalisierung unserer Gesellschaft in all ihren sozialwissenschaftlichen Facetten, ganz besonders jedoch dem Schwerpunkt Sicherheit. Humers Schwerpunkte im Netzwerk sind Terrorismus, Extremismus und Organisierte Kriminalität im Allgemeinen sowie Linksextremismus/-terrorismus und Cyberterrorismus im Besonderen. Weitere Informationen: [www.humer.de](http://www.humer.de), Kontaktdaten: [stephan@internetsoziologie.at](mailto:stephan@internetsoziologie.at)



Foto: privat

*Es ist wahrscheinlich nur ein Kratzen an der Oberfläche, aber es ist ein wichtiges Signal: Seht her, wir gehen ganz konkret gegen die Barbaren vor. Wir leben leider in einer Zeit, in der zu viel Verantwortung institutionalisiert worden ist: Für nahezu alles sollen Behörden, Ämter, Anstalten verantwortlich sein. Das klappt aber nicht, wenn wir alle angegriffen werden. Wir alle müssen Freiheit, Menschenrechte und Demokratie verteidigen. Und wenn das eine Gegenrede durch „Anonymous“ in Form eines Website-Defacements einer IS-Terrorpropaganda-Website ist – warum nicht? Den „harten“ Antiterrorkampf können ohnehin nur Behörden wie Polizei und Militär führen.*

*Der Google-Ideas-Chef will gezielte Anzeigen auf die Bildschirme jener Nutzer schalten, die sich intensiv mit der Propaganda durch Terrorgruppen wie den IS beschäftigen. Funktioniert das aus Sicht der Internetsoziologie, Menschen auf diese Weise von ihren eigentlichen Intentionen abzulenken, sie zu stören, ihnen ein anderes „Produkt“ zu verkaufen? Lassen sich – wie in einer Pilotstudie des Londoner ISD – junge Männer, die nach Videos des IS suchen und am Anfang der Radikalisierung stehen, gar generell bremsen, wenn ihnen statt der gesuchten Videos andere von Ex-IS-Kämpfern gezeigt werden, die ihnen von einem Anschluss an den IS abraten?*

*Grundsätzlich funktionieren Ablenkung, Irritation und Gegenrede schon, es kommt im Detail aber auf die Methode und die Zielgruppe an. Ich sehe derzeit noch nicht, dass hier ausreichend viel gemacht wird. Die Gegenrede halte ich aber für eine der vielversprechendsten Lösungen, nur muss sie erstens noch viel stärker angewendet werden und zweitens breit aufgestellt sein. Das wiederum ist eine enorme und langfristige Aufgabe, für die die Zivilgesellschaft – Individuen wie auch Firmen – noch viel mehr Unterstützung braucht.*

*Junge Menschen, die sich langweilen, begrenzt fühlen und auf der Suche nach Abenteuern sind, sollen besonders anfällig für Anwerbeaktionen über Facebook und andere soziale Netzwerke sein. Liefse sich diese Suche nach Heldentaten nicht mit digitalen „Umleitungsattacken“ beziehungsweise gezielter Gegenrede umpolen, um sie beispielsweise für den Klimaschutz oder die Befreiung der Meere und Seen von Plastikmüll zu begeistern?*

*Das wäre sicher der zweite Schritt. Zuerst einmal muss man allen, die sich als Outsider empfinden, die Integration in die „normale“ Gesellschaft ermöglichen: Anerkennung, Perspektive, Verantwortung. Da geht es meist konkret um Job, Geld, Wohnung, Beziehung. Wenn dann ein Fundament da ist, kann man natürlich Angebote für ein weitergehendes Engagement schaffen. Aber die Frustrierten werden nicht gleich zu Klimaschützern. Sie wollen in aller Regel erst einmal ein ganz normales Leben. Das gilt freilich nicht für alle – vor allem nicht für die Hardcore-Ideologen. Aber dem Abfischen der Verzweifelten durch IS und Co. kann man so sicher begegnen.*

*Werden wir zu einer „Stasi“-Gesellschaft, wenn Nutzer dazu aufgerufen werden, andere Nutzer sozialer Netzwerke zu melden, die auffällige Statements abgeben?*

*Es kommt wie so oft auf die Dosis an. Wenn jetzt beispielsweise jeder von uns anfängt, jeden Tag Dutzende Falschparker zu melden, weil man die Technik dazu, beispielsweise das Smartphone oder eine Dashcam, ohnehin dabei hat, dann läuft natürlich etwas falsch. Dasselbe gilt natürlich für das Melden von entsprechenden Statements bei Facebook oder Twitter. Wir müssen viel mehr als bisher lernen, das richtige Maß zu finden. Wann ist Ignorieren richtig, nach*

## Über die Vereinigung

Das Netzwerk *Terrorismusforschung e. V. (NTF)* versteht sich als Plattform für Forschung, Medien, Behörden und Politik, um u. a. die Themenkomplexe Terrorismusbekämpfung, Extremismus und politische Gewalt auf multidisziplinärer Ebene auszuloten.

Der Verein wurde als Netzwerk im Januar 2007 von den Doktoranden Anna Goppel (Universität Zürich), Daniel Meßelken (Universität Leipzig) und Anne Schwenkenbecher (Humboldt-Universität zu Berlin) gegründet. Ihr Ziel war es, Nachwuchsforscher unterschiedlicher Disziplinen, die sich wissenschaftlich mit Terrorismus auseinandersetzen, in Verbindung zu bringen. Im März 2013 wurde die Interessengemeinschaft aufgelöst und der Verein gegründet. Der Vorstand besteht seitdem aus Dr. Stephan G. Humer (Universität der Künste Berlin), Sebastian Baden (HfG Karlsruhe) und Bernd Zywiets (Universität Mainz).

## Weiterführende Literatur

Der Sammelband *„Terrorismus A/D: Wechselwirkungen zwischen analoger und digitaler Sphäre“* wird herausgegeben vom Vorsitzenden des Netzwerks *Terrorismusforschung e. V.* und Herausgeber der Schriftenreihe *„Digitale Wissenschaft“* im CSW-Verlag, Univ.-Doz. Dr. Stephan G. Humer. Der Band lotet auf multidisziplinärer Ebene die Wechselwirkungen zwischen analoger und digitaler Sphäre in Hinblick auf Terrorismus und Extremismus aus.

Cyberterrorismus ist kein neues Phänomen: Nicht erst seit der Hochphase des islamistischen Terrors rund um 9/11 dürfte allgemein bekannt sein, dass alle Beteiligten – Staaten wie Terroristen – versuchen, digitale Entwicklungen wie das World Wide Web massiv für ihre Zwecke zu nutzen, beispielsweise auf der Propaganda- und der Rekrutierungsebene. Das Digitale potenziert sowohl die Chancen als auch die Risiken, es löst sie jedoch nicht automatisch ab.

Format: Kindle Edition und Print

Dateigröße: 1 314 KB

Seitenzahl der Print-Ausgabe: 162 Seiten

Verlag: CSW-Verlag (12. Februar 2015), Preis: 24,99 Euro

*dem uralten Netzmotto „Don't feed the troll“? Wann ist Gegenrede richtig? Wann müssen Polizei und Staatsanwaltschaft ran? Dies alles ist im digitalen Raum immer noch schwieriger als im analogen Alltag, weil jahrelang der soziale Aspekt der Digitalisierung in Politik, Bildung und Gesellschaft stark vernachlässigt worden ist. In diese Lücke ist der IS gestoßen, hat sie erobert und damit große Erfolge verzeichnen können. Heute merken wir das auf schmerzhafteste Art und Weise und müssen nun doppelt und dreifach intensiv versuchen, einen plausiblen Umgang mit diesem Phänomen zu finden.*

*Ist die Digitalisierung denn schon so weit, mit Hilfe künstlicher Intelligenz IS-Propaganda und -Verlautbarungen im Netz aufzuspüren und zu löschen, zu manipulieren oder mit Gegenrede zu bekämpfen?*

*Sicherlich gibt es zahlreiche interessante Ansätze, die auch genutzt werden sollten, sobald sie hilfreich erscheinen. Doch am Ende geht es um den Menschen. Viele der IS-Kämpfer sind im Sinne westlicher Wettbewerbsgesellschaften das, was man landläufig einen Versager nennt. Auch wenn man ihn mit algorithmischer Gegenrede vielleicht kurzfristig in seinem Radikalisierungsprozess stört, so braucht er doch langfristig eine ganz altmodische Lebensperspektive, um vom Terror Abstand zu nehmen. Wir sehen ja in Frankreich und Belgien, wohin Ignoranz gegenüber „den anderen“ führen kann. Jeder muss die Chance haben, sich in unser Gemeinwesen zu integrieren, auch wenn dies ohne Wenn und Aber mit Pflichten verbunden ist. Ich sehe deshalb die Chance nur in der Variante, Technik dort maximal einzusetzen, wo sie nachweislich sinnvoll ist, und in allen anderen Bereichen voll und ganz auf das Soziale zu setzen. Keiner der betroffenen gesellschaftlichen Teilbereiche – Technik, Recht oder Soziales – kann für sich allein die Siegesformel reklamieren.*

Das Interview führte OBJEKTSpektrum-Redakteurin Annegret Handel-Kempf.