ÖFIT-Trendschau

Öffentliche Informationstechnologie in der digitalisierten Gesellschaft

Trendthema 30:

Darknet

Stand: Juni 2015

Kompetenzzentrum
Öffentliche IT

Herausgeber:
Jens Fromm und Mike Weber
Kompetenzzentrum Öffentliche IT
Fraunhofer-Institut FOKUS
Kaiserin-Augusta-Allee 31, D-10589 Berlin
Telefon: +49 30 3463 - 7173
Telefax: + 49 30 3463 - 99 - 7173
info@oeffentliche-it.de
www.oeffentliche-it.de
www.fokus.fraunhofer.de

Autorinnen und Autoren der Gesamtausgabe:
Mike Weber, Stephan Gauch, Faruch Amini, Tristan Kaiser, Jens Tiemann, Carsten Schmoll, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Christian Welzel, Jonas Pattberg, Jens Fromm, Michael Rothe, Oliver Schmidt

Gestaltung:
Reiko Kammer

ISBN: 978-3-9816025-2-4

Juni 2015

Bibliographische Angabe:
Weber, Mike, Jens Tiemann, Christian Welzel, Lutz Henckel, Gabriele Goldacker, Petra Hoepner, Nadja Menz, Maximilian Schmidt, Michael Stemmer, Florian Weigand, Jonas Pattberg, Jens Fromm, 2015: Darknet. In: Jens Fromm und Mike Weber, Hg., 2015: ÖFIT-Trendschau: Öffentliche Informationstechnologie in der digitalisierten Gesellschaft. Berlin: Kompetenzzentrum Öffentliche IT. http://www.oeffentliche-it.de/trendschau.

Darknet

Während gerne auch im Digitalen über die totale Transparenz diskutiert wird, spannt sich unter der Oberfläche des WWW ein tiefes, undurchsichtiges Netz. Der kryptographisch geschützte Teil dieser dunklen Seite des Internets, das Darknet, bietet einen Schutzraum nahezu vollständiger Anonymität – der von Drogen- und Waffenhändlern ebenso genutzt wird wie von Andersdenkenden in totalitären Regimen. Die Technik bietet somit sowohl ein Höchstmaß an Privatheit als auch eine ausgezeichnete Gelegenheit, diese kriminell zu missbrauchen. Die Politik muss sich in dieser technisch begründeten, neuen Dimension des Zwiespalts zwischen Privatheit und Strafverfolgung positionieren.

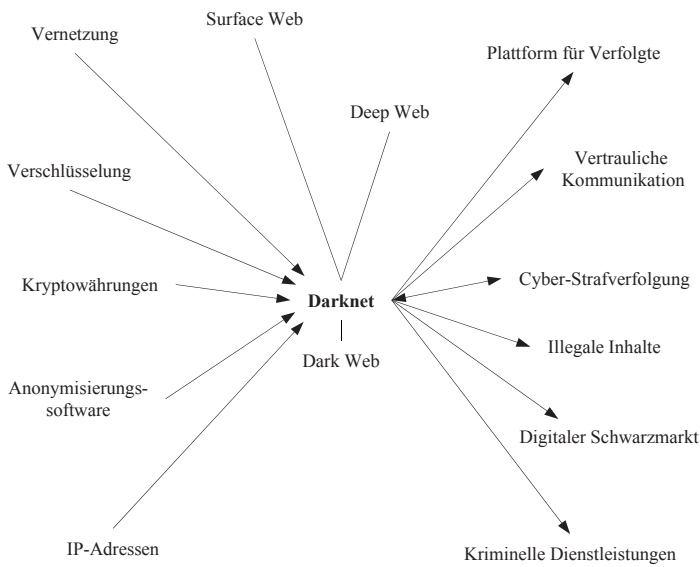

Abb. 1: Netzwerkartige Verortung des Themenfeldes: Vorläufer, Begleitphänomene und Folgen

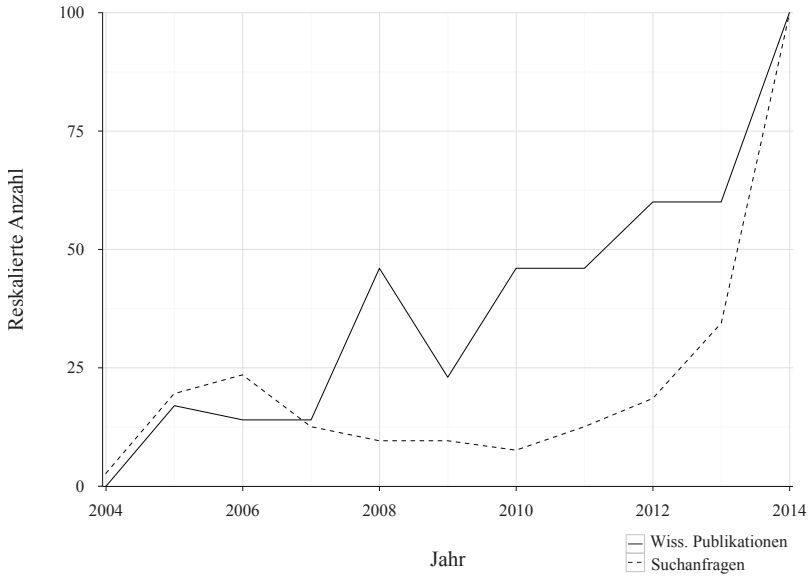

Abb. 2: Wissenschaftliche und gesellschaftliche Themenkonjunkturen

Kaufen und verkaufen, suchen oder einfach herumsurfen sind bekannte Aktivitäten im Internet, auch bezeichnet als Oberflächen-Web (»Surface Web«). Sucht man allerdings nach Drogen, ungepatchten Schwachstellen für Cyberangriffe oder möchte sich illegal Pässe beschaffen, dann muss man in das sogenannte Darknet abtauchen. Auf der dunklen Seite des Internets möchte man anonym bleiben.

Das Darknet ist nur ein kleiner Teilbereich des sogenannten Deep Web. Das Deep Web umfasst Server, Datenbanken und Dienste, die nichts Verbotenes bereitstellen, jedoch auch nicht für die breite Öffentlichkeit bestimmt sind und daher auch nicht von Suchmaschinen indexiert werden. Dies sind beispielsweise themenspezifische oder auch kostenpflichtige Fachdatenbanken oder Webseiten und -dienste, auf die nur mit spezieller Software oder mit entsprechenden Zugangsdaten zugegriffen werden kann. Schätzungen nach ist die Datenmenge im Deep Web um ein Vielfaches größer als die im Oberflächen-Web.

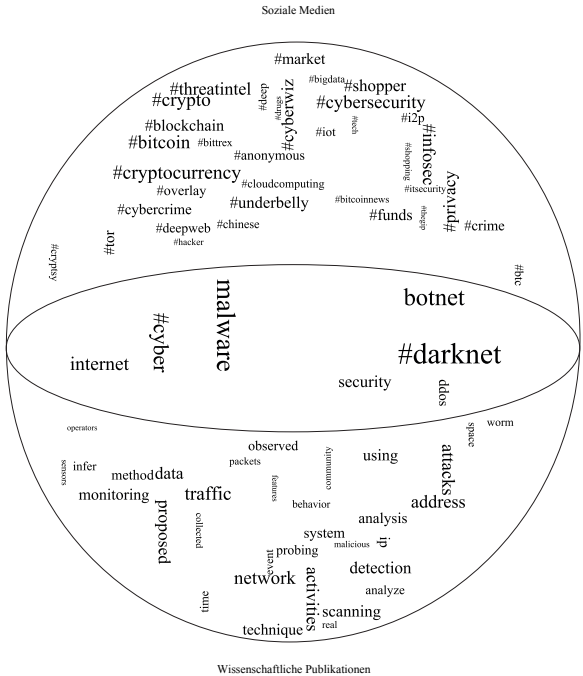

Abb. 3: Häufigkeit von Hashtags bei Twitter und von Stichworten in wissenschaftlichen Publikationen

Das Darknet lässt sich als anonymisierter Teil des Deep Web auffassen. Eine bekannte Anonymisierungssoftware ist die Freeware Tor. Durch Verwendung von Tor können die Netzaktivitäten eines Internet-Nutzers nicht nachverfolgt werden (anonymes Surfen). Datenpakete werden nach dem Zwiebelschalenprinzip – der ursprüngliche Name TOR stand für »The Onion Router« – verschlüsselt zwischen Tor-Servern weitergeleitet. Jeder Tor-Server kennt dabei nur seinen Vorgänger und seinen Nachfolger, aber nicht die gesamte Ende-zu-Ende Verbindung. So wird die wirkliche IP-Adresse eines Internet-Nutzers getarnt. Diese schrittweise Verschlüsselung benötigt zusätzliche Kommunikationswege zwischen den freiwillig bereitgestellten Tor-Ser-

vern, wobei die Routen automatisch in kurzen Abständen geändert werden. Daher sind die Antwortzeiten beträchtlich und die nutzbare Bandbreite niedrig.

Eine weitere Eigenschaft von Tor ist die Möglichkeit, Dienste versteckt bereitzustellen (Hidden Services im Dark Web). Dienstleistungen und Daten im Darknet findet man nicht bei gewöhnlichen Suchmaschinen sondern beispielsweise im Hidden Wiki, das eine Sammlung von speziellen Links (erkennbar an der Endung .onion) zu Angeboten und illegalen Marktplätzen umfasst. Dass der berühmteste dieser Marktplätze »Seidenstraße« (»Silk Road«) hieß, deutet auf das beträchtliche wirtschaftliche Potenzial dunkel-digitaler Kriminalität. Bezahlt werden die Leistungen und Waren ebenfalls anonym mit Krypto-Währungen wie Bitcoins (s. Trendthema 3: Virtuelle Währung).

Anonymitätstechnologien wie Tor werden aber nicht nur für dunkle Machenschaften benötigt, sondern sind auch dann notwendig, wenn man aus gesellschaftlichen oder privaten Gründen eine Überwachung der eigenen Kommunikation verhindern möchte. Regimekritiker in vielen Ländern der Welt sowie Aktivisten und Journalisten sind auf diese Technologien für ihre vertrauliche elektronische Kommunikation angewiesen. Denn ursprünglich konzipiert wurde Tor nicht für Kriminelle, sondern für gemeinwohlorientierte Aktivitäten und hat dafür auch den Preis für Projekte mit gesellschaftlichem Nutzen von der Free Software Foundation erhalten.

Dieselbe Technologie eröffnet also unterschiedliche Einsatzmöglichkeiten für legale und illegale Zwecke. Aus einer gesamtgesellschaftlichen Perspektive ergeben sich daraus altbekannte Spannungsfelder in einer neuen Dimension. Privatheit kann innerhalb einer Gruppe über den gesamten Globus verteilt gelebt werden. Wofür diese privaten Räume genutzt werden, bleibt dabei ebenso verschlossen, wie in Vertrauensräumen in der nicht-digitalen Welt. Die besondere Bedeutung ergibt sich hier wie in der Digitalisierung insgesamt durch die zunehmende Wissensfundierung und leichtere Koordinierung: ob 3D-Druckvorlagen von Waffen für terroristische Anschläge oder Hinweise auf Versammlungsmöglichkeiten für verfolgte Gewerkschaftler.

Von Strafverfolgungsbehörden werden entsprechend immer wieder Verschlüsselung und Anonymisierung als Arbeitsbehinderung kritisiert. Kriminelle werden sich jedoch nicht durch eine Schwächung von Verschlüsselungstechnologien an ihren Taten hindern lassen. Die weitgehende Anonymität gegenüber staatlichen Stellen (oder auch großen Telekommunikations- und Internetunternehmen) verlangt hohes techni-

sches Wissen und Konspiration. Das Bedrohungspotenzial durch das Darknet bleibt daher strukturell beschränkt. Außerdem dienen diese Technologien auch als Handwerkszeug für die Polizei, um unerkannt Informationen zur Gefahrenabwehr zu sammeln oder verdeckt zu ermitteln.

Möglichkeiten	Wagnisse
– Schaffung von Vertrauensräumen im Internet durch anonyme Kommunikation – Stärkung der Zivilgesellschaft durch vertrauliche Kommunikationswege – Bereitstellung von Anonymisierungsdiensten durch vertrauenswürdige Internetprovider – Hohes praktiziertes Datenschutzniveau verringert den Bedarf nach Darknet-Techniken – Nutzung des Darknets zur Gefahrenabwehr und Strafverfolgung durch Sicherheitsbehörden – Möglichkeiten der anonymen Websuche bspw. für die Wirtschaft zur Konkurrenzanalyse	– Schutzräume für kriminelle und terroristische Aktivitäten – Schutz illegalen Besitzes und Vertriebs von Digital- und Wissensgütern wie Kopien urheberrechtlich geschützten Materials und 3D-Druckvorlagen für Waffen oder Fälschungen – Möglichkeit der Kommerzialisierung von Kriminalität (Crime-as-a-Service) – Anonymität macht verdächtig, da die kriminelle Nutzung dieses Grundrecht negativ belastet – Verwandte Technologien wie Krypto-Währungen erleiden einen Imageschaden

Handlungsraum a: Privatheit zulassen
Technologien zur privaten und vertraulichen Kommunikation im Internet sind für eine freie Zivilgesellschaft und für die Wirtschaft unverzichtbar.

Handlungsraum b: Polizeiarbeit unterstützen
Kriminalität lässt sich auch im Darknet aufspüren: digitale Kommunikation hinterlässt Spuren und nicht-digitale Waren müssen physisch zugestellt werden. Die Polizei muss auf dem Stand der Technik bleiben, um Informationen und Spuren sammeln und auswerten zu können. Internationale Kooperationen sind in diesem Feld gleichermaßen möglich wie erforderlich.