Online-Privatheitskompetenz und Möglichkeiten der technischen Umsetzung mit dem Anonymisierungsnetzwerk Tor

Alexandra Lux und Florian Platzer

Zusammenfassung

Ziel der vorliegenden Arbeit ist die Erstellung einer Anonymitätsmatrix. Der Fokus liegt hierbei insbesondere in der Verbindung der technischen und psychologischen Komponenten der Betrachtung. Ausgangssituation ist die Verwendung einer Privacy Enhancing Technology, konkret dem Tor-Browser. So ist das Ziel, die Tor-Nutzergruppe in Bezug auf ihre Online-Privatheitskompetenz, Nutzungsweise und Grad der Anonymität zu erforschen. Hierzu wurde eine Online-Befragung ($N = 120$) sowie ein Leitfadeninterview mit einem Experten aus der IT-Sicherheitsforschung durchgeführt.

Schlüsselwörter

Anonymität • Privatheitskompetenz • Tor

1 Online-Privatheitskompetenz zur Erstellung und Wiederaufhebung anonymer Internetkommunikation

Im vorliegenden Abschnitt werden wir zunächst zentrale Begrifflichkeiten von Privatsphäre im Online-Kontext klären. Internetnutzer sind zwar oft um ihre Privat-

A. Lux (✉)
TU Darmstadt, Darmstadt, Deutschland
E-mail: alexandra.lux@sit.fraunhofer.de

F. Platzer
Fraunhofer SIT, Darmstadt, Deutschland
E-mail: florian.platzer@sit.fraunhofer.de

M. Friedewald et al. (Hrsg.), *Selbstbestimmung, Privatheit und Datenschutz,*
DuD-Fachbeiträge, https://doi.org/10.1007/978-3-658-33306-5_7

sphäre besorgt, besitzen jedoch nicht die entsprechenden Kompetenzen, um ihr Verhalten entsprechend anzupassen und so ihre Privatsphäre zu schützen.

Eine Möglichkeit, die Privatsphäre der Internetnutzer zu schützen, bietet das Anonymitäts-Netzwerk *Tor*[1]. Tor erlaubt eine anonyme Kommunikation über das Internet. Der dafür benötigte Tor-Browser kann zum Surfen sowohl des Clearnets als auch des Darknets, also für den Zugriff auf anonym bereitgestellte Internetdienste, sog. Hidden Services, verwendet werden.

Im Rahmen dieser Arbeit untersuchen wir einen Erklärungsansatz, welcher sich mit der Online-Privatheitskompetenz der Nutzer beschäftigt. Am Beispiel von Tor gehen wir auf *Privacy Enhancing Technologies* (PETs) ein, die eine Möglichkeit bieten, eigene Daten besser zu schützen und eine anonyme Internetkommunikation aufzubauen. Wir zeigen auf, welche Akteure einen Tor-Nutzer potenziell deanonymisieren können und welche zusätzlichen Technologien ein Tor-Nutzer hinzunehmen kann, um eine solche Deanonymisierung zu erschweren.

1.1 Privatsphäre im Online-Kontext

Das Verlangen nach Privatsphäre im Online-Kontext wird in Zeiten von Massenspeicherung und den Überwachungsmöglichkeiten des Internetverkehrs immer stärker. Bei der Definition von Privatsphäre wird in der Regel auf drei zentrale Arbeiten zurückgegriffen: Westin [31], Altman [2] sowie Burgoon [5]. Trepte und Dienlin führen die zentralen Aspekte dieser drei Ansätze wie folgt zu einer Definition zusammen:

> „Privatsphäre ist ein individueller Zustand der Abgeschiedenheit und Intimität (Westin 1967), der einer stetigen Regulierung von Zuviel und Zuwenig Privatsphäre unterliegt (Altman 1975), wobei sich zu jedem Zeitpunkt vier verschiedene Privatsphäredimensionen unterscheiden lassen: informationale, soziale, psychische und physische Privatsphäre“ (Burgoon, 1982) [5, S. 56].

Zwei entscheidende Faktoren sind in diesem Zusammenhang das *Privatsphäreverhalten* sowie der *Privatsphärekontext*. Dabei beschreibt das Privatsphäreverhalten eine Verhaltensweise, die die eigene Selbstauskunft anderen gegenüber einschränkt oder sich der Interaktion mit anderen entzieht [8]. Der Privatsphärekontext wiederum beschreibt die Situation, in der die Interaktion stattfindet. Dieser ist abhängig von der individuellen Wahrnehmung der Teilnehmer der Interaktion [28]. Immer wieder konstatieren Forschungsergebnisse eine Dissonanz zwischen Bedenken rund

[1] Tor Project, https://torproject.org, Zugegriffen am 15.10.2020

um Privatheit und dem Verhalten im Umgang mit den eigenen Daten [1, 20, 32]. Dieser Umstand wird auch als *Privacy Paradox* bezeichnet [3, 8]. Einer der angeführten Erklärungsansätze, wie es zu dieser Dissonanz kommen kann, ist die *Knowlegde Gap Hypothesis*. Sie beschreibt den Zustand, dass Personen zwar um ihre Privatsphäre besorgt sind, jedoch nicht die entsprechenden Kompetenzen besitzen, um ihr Verhalten entsprechend anzupassen und so ihre Privatsphäre zu schützen [6, 29].

Online-Privatheitskompetenz ist somit eine Möglichkeit das Online-Verhalten kohärenter zu den jeweiligen Privatsphärebedürfnissen der Nutzer zu gestalten [29]. Auf dieser Basis werden Nutzer in die Lage versetzt, Kontrolle über ihre digitale Identitäten zu erlangen [21]. Online-Privatheitskompetenz umfasst das Wissen um technische Möglichkeiten sowie diesbezügliche Regularien und institutionelle Praktiken zur Erreichung von Online-Privatheit als auch das Wissen um deren korrekte Anwendung [29]. Umfassende Forschungsergebnisse zeigen verschiedene Einflussfaktoren auf die Online-Privatheitskompetenz, wie demografische Variablen, digitale Kompetenz, das Bewusstsein für institutionelle Überwachungspraktiken und das Verständnis von vorgegebenen Richtlinien [21].

Entgegen bisherigen Arbeiten, in denen das Privacy Paradox vorrangig im Kontext der Nutzung sozialer Netzwerke betrachtet wurde [3, 8], beziehen wir uns auf die Nutzungsweise im Internet allgemein. Die Nutzungsweise von Tor kann in Bezug auf verschiedene Aspekte variieren. In Anlehnung an aktuelle Forschung [12] haben wir die Nutzung von Tor unter anderem durch die Erhebung der Nutzungshäufigkeit erfasst. Des Weiteren erfassten wir in diesem Rahmen die Themen, die bei der Nutzung vorrangig von Interesse sind [4, 19], sowie in welchem Privatsphärekontext, also Clearnet, Darknet oder dual, Tor verwendet wird. Außerdem erfragten wir noch die Art der Hidden Services, die besucht werden. Vor diesem Hintergrund möchten wir uns in einem ersten Schritt die Nutzungsweise von Tor und die Online-Privatheitskompetenz genauer anschauen. Erste Untersuchungen diesbezüglich zeigten, dass Tor-Nutzer eine höhere Online-Privatheitskompetenz besitzen, als reguläre Clearnet-Nutzer. So beantworteten diese im Schnitt 78,78 % der Fragen richtig [12]. So lautet unsere erste Forschungsfrage:

Forschungsfrage F1: Inwiefern variiert die Online-Privatheitskompetenz der Nutzer in Abhängigkeit ihrer Nutzungsweise von Tor?

Hypothese H1a: Abhängig von der Nutzungshäufigkeit von Tor variiert die Online-Privatheitskompetenz der Nutzer.

Hypothese H1b: Abhängig davon, ob Tor im Clearnet, Darknet oder beidem verwendet wird, variiert die Online-Privatheitskompetenz der Nutzer.

Hypothese H1c: Abhängig davon, für welche Themengebiete Tor vorrangig verwendet wird, variiert die Online-Privatheitskompetenz der Nutzer.

Hypothese H1d: Abhängig davon, welche Art von Hidden Services vorrangig genutzt wird, variiert die Online-Privatheitskompetenz der Nutzer.

Eine Möglichkeit, seine Daten besser zu schützen, ist der Einsatz von *Privacy Enhancing Technologies.* Doch auch hier bedarf es entsprechender Kompetenzen, wobei das Wissen um das Bestehen der Technologie nicht ausreicht. Vielmehr bedarf es zudem auch notwendiges Wissen um die Anwendung. Ergebnisse früherer Forschung belegen, dass Personen keine akkurate Introspektion betreffend ihres Wissens um Technologien zum Schutz der eigenen Privatsphäre haben [16]. Weitere Forschungen zeigen, dass das Wissen um technische Möglichkeiten nach demographischen Aspekten variiert [11]. Eine Umfrage ergab, dass 86 % der amerikanischen Teilnehmer Maßnahmen zur Erhöhung ihrer Anonymität ergriffen haben (bspw. Cookies löschen 64 %, Cookie-Blocker 41 %). Nur ein geringer Anteil der Befragten (14 %) gab an, Technologien wie bspw. VPN, Proxy-Server oder Tor zu verwenden. Außerdem indizierten die Ergebnisse, dass eine Nutzergruppe zwischen 18 und 29 Jahren sowie Personen mit höherem Bildungsabschluss tendenziell mehr Anonymisierungstechnologien verwendet. [22]. Wie zuvor bereits dargestellt, fokussiert die vorliegende Arbeit auf der Untersuchung der Tor-Nutzergruppe. Da allerdings auch mit der Verwendung von Tor eine Deanonymisierung nicht ausgeschlossen werden kann, bieten zusätzliche PETs potentiell einen höheren Schutz vor Deanonymisierung.
Vor diesem Hintergrund stellen wir die folgende Forschungsfrage:

Forschungsfrage F2: Inwiefern variieren die in Kombination zu Tor verwendeten Anonymisierungstechnologien in Abhängigkeit von der individuellen Nutzungsweise von Tor?

Hypothese H2a: Abhängig von der Häufigkeit der Nutzung von Tor variieren die zusätzlich in Kombination zu Tor verwendeten Anonymisierungstechnologien.

Hypothese H2b: Abhängig davon, ob Tor im Clearnet, Darknet oder beidem verwendet wird, variieren die in Kombination zu Tor verwendeten Anonymisierungstechnologien.

Hypothese H2c: Abhängig davon, für welche Themengebiete Tor vorrangig verwendet wird, variieren die in Kombination zu Tor verwendeten Anonymisierungstechnologien.

Hypothese H2d: Abhängig davon, welche Art von Hidden Services vorrangig genutzt wird, variieren die in Kombination zu Tor verwendeten Anonymisierungstechnologien.

Forschungsergebnisse [25] haben gezeigt, dass ein Großteil der Personen sich etwaiger weiterer Technologien, die zum Schutz ihrer Privatsphäre genutzt werden können, nicht bewusst ist. Betreffend der aktiven Verwendung von zusätzlichen Maßnahmen indizierten 13 % der Befragten keine Kenntnis von alternativen Suchmaschinen, welche keine Suchverläufe der Nutzer speichern (bspw. DuckDuckGo). 54 % der Befragten gaben an, Suchmaschinen dieser Art nicht zu verwenden. Ferner hatten 33 % keine Kenntnis über die Möglichkeit der Verwendung von Proxyservern zum Schutz der Privatsphäre. 41 % gaben wiederum an, Proxyserver nicht zu verwenden. 39 % der befragten Personen hatten keine Kenntnis von Anonymisierungsnetzwerken, wie beispielsweise Tor. Weitere 40 % gaben an, diese nicht zu verwenden [25]. Konform dazu fanden Weinberg et al. [30], dass der allgemeine Kenntnisstand über technische Möglichkeiten zur Verbesserung der Privatsphäre moderat ist. Die Anzahl der Personen, die entsprechende technische Möglichkeiten anwendet, ist gering.

Zudem bedarf es im Fall einer Anwendung auch die notwendige Kompetenz, da im Falle einer inkorrekten Anwendung sich der Privatsphäreschutz im Vergleich zum Verzicht auf die PET gar verschlechtern kann. Auf dieser Basis widersprechen wir der Argumentation früherer Arbeiten [12], wonach der Erklärungsansatz der Knowledge Gap Hypothesis alleinig auf Basis der Installation und Nutzung einer PET als Erklärungsansatz für das Privacy Paradox angesehen wird. Wie oben dargestellt, handelt es sich bei Online-Privatheitskompetenz um ein vielschichtiges Konstrukt, das nicht alleinig in dem Wissen um PETs besteht [29]. Um die Differenz zwischen Wissen um weitere technische Möglichkeiten in Form von PETs und der tatsächlichen Anwendung aktiv zu berücksichtigen, möchten wir den Effekt der zusätzlichen Verwendung von Anonymisierungstechnologien auf die Online-Privatheitskompetenz untersuchen und stellen hierfür die folgende Forschungsfrage:

Forschungsfrage F3: Inwiefern sagt die Online-Privatheitskompetenz der Nutzer die in Kombination mit Tor verwendete Anonymisierungstechnologien voraus?

Hypothese H3a: Nutzer, die eine höhere Online-Privatheitskompetenz besitzen, verwenden zusätzliche Anonymisierungstechnologien in Kombination zu Tor.

Hypothese H3b: Nutzer, die eine höhere Online-Privatheitskompetenz besitzen, haben Kenntnis von zusätzlichen Anonymisierungstechnologien in Kombination zu Tor.

Durch die Verwendung von Tor erhält man eine grundsätzliche Anonymität beim Surfen des Clear- und des Darknets. Trotzdem sind die Tor-Nutzer einer möglichen Deanonymisierung leicht ausgesetzt.

Nach Westin [31] wird unter Anonymität der Zustand verstanden, in welchem Freiheit von Identifikation und Überwachung an öffentlichen Orten oder während öffentlicher Handlungen besteht. Hayne und Rice [14] unterscheiden weiter zwischen sozialer und technischer Anonymität. *Soziale Anonymität* impliziert hierbei, dass keine Kontextinformationen zur Verfügung stehen, um die Identität zu enthüllen. Hier sind insbesondere Informationen gemeint, die durch Kommunikation und Verhalten mit anderen geteilt werden. *Technische Anonymität* hingegen impliziert, dass eine Rückverfolgbarkeit auf technischer Basis nicht möglich ist. Analog dazu wird technisch weiter zwischen Verbindungs- und Datenanonymität unterschieden. *Verbindungsanonymität* beschreibt hierbei die Identifikation des Senders bzw. des Empfängers während des Datentransfers. *Datenanonymität* beschreibt das Filtern und Identifizieren der gesendeten Daten [7].

Über die Nutzergruppe von Tor ist, wie für ein Anonymitätsnetzwerk zu erwarten, nicht viel bekannt. Bisherige Beschreibungen der Nutzergruppe orientieren sich vordergründig an der Motivation, die die Nutzer aufgrund ihrer Verortung haben, sich mit der Verwendung von Tor schützen zu wollen. Diesen Beschreibungen zufolge, besteht diese aus Personen verschiedener sozioökonomischer Hintergründe. So werden beispielsweise Journalisten, Strafverfolgungsbeamte, Whistleblower und Aktivisten aber auch Blogger (u. a.) als aktive Nutzergruppen genannt[2]. Gleichermaßen variieren auch die Motive zur Nutzung von Tor. Während die einen das Ziel haben, nicht identifiziert werden zu können, möchten andere primär ihre Daten schützen. In einer Online-Befragung von Harborth et al. wurde Anonymität als Hauptgrund für die Verwendung von PETs, wie bspw. Tor, angegeben [13]. Eine Dimension ist hierbei die Angst vor Deanonymisierung durch bspw. staatliche Akteure. Andere Arbeiten nennen als Motivation zur Nutzung von Tor das Bedürfnis, seine Daten

[2] Users of Tor. https://2019.www.torproject.org/about/torusers.html, Zugegriffen am 21.10.2020

zu schützen, das Bedürfnis, sich mit einer bestimmten Zielgruppe auszutauschen, politische Gründe oder den Konsum potentiell illegalen Materials [9, 10, 15].
Um zu klären, welche Technologie welchen Grad an Anonymität gegenüber welchem Akteur bietet, formulieren wir die folgende qualitative Forschungsfrage:

Forschungsfrage F4: Inwiefern schützen zusätzliche Anonymisierungstechnologien in Kombination mit Tor vor einer potentiellen Deanonymisierung?

Im Folgenden werden wir nun auf die technischen Grundlagen von Tor eingehen, um anschließend in einem nächsten Schritt potentielle Akteure der Deanonymisierung sowie zusätzliche Technologien zum Schutz der Anonymität zu extrahieren.

1.2 Das Tor-Netzwerk

Tor ist das größte und bekannteste Anonymitäts-Netzwerk. Durch das im Tor-Netzwerk verwendete Onion-Routing wird der gesamte Datenverkehr verschlüsselt durch einen Pfad bestehend aus mindestens drei Tor-Knoten geleitet, sodass keiner nachvollziehen kann, wer mit wem und über was kommuniziert. Der erste Knoten in einem solchen Pfad wird als „Guard-Knoten“ bezeichnet. Der mittlere Knoten im Datenpfad wird als „Middle-Knoten“ und der letzte als „Exit-Knoten“ bezeichnet. Abb. 1 zeigt einen Datenpfad, der durch das Tor-Netzwerk aufgebaut wird. Die IP-Adressen dieser Tor-Knoten selbst sind alle öffentlich bekannt. Dadurch kann

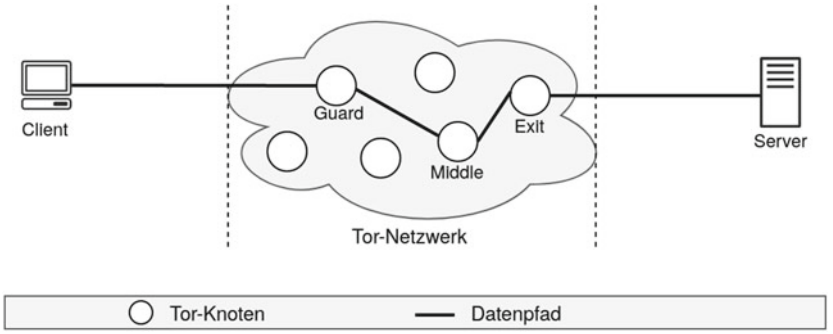


Abb. 1 Datenpfad durch das Tor-Netzwerk

der erwähnte Datenpfad aufgebaut werden, sodass die IP-Adressen der Tor-Nutzer verschleiert werden können und die Tor-Nutzer dadurch anonym sind. Der vom Tor-Nutzer angesprochene Server erfährt nur die IP-Adresse des Exit-Knotens anstatt die des Tor-Nutzers. Es ist allerdings trotz anonymer Kommunikation möglich zu erkennen, ob sich jemand mit dem Tor-Netzwerk verbindet und darüber kommuniziert. Um anonym über das Tor-Netzwerk surfen zu können, kann der Tor-Browser verwendet werden. Der Tor-Browser ist ein modifizierter Web-Browser, der durch die Tor-Software alle Daten durch das Tor-Netzwerk schickt.

1.3 Akteure als mögliche Angreifer

Die Angriffsmöglichkeiten gegen ein beliebiges System sind unzählig. Wir haben uns daher in Anlehnung an frühere Forschung darauf beschränkt, einen Überblick über mögliche Akteure zu geben, die die Anonymität der Tor-Nutzer angreifen können. Ries et al. bewerteten und stufen mögliche Angreifer nach deren subjektiven Einschätzung hinsichtlich auf verfügbare Ressourcen ein [23]. In unserer Arbeit betrachten wir folgende Akteure als Angreifer einer möglichen Deanonymisierung von Tor-Nutzern:

Regierung (R). Eine Regierung ist die höchste Instanz eines Staates und hat am meisten Ressourcen zur Verfügung, um einen beliebigen Angriff gegen die Anonymität eines Tor-Nutzers durchzuführen. Hierzu zählen staatliche Organisationen wie zum Beispiel Geheimdienste.
Internetknoten-Betreiber (IKB). Ein Internetknoten dient als Austauschpunkt des Internet-Datenverkehrs mehrerer Netzwerke. Internetknoten können einen beträchtlichen Teil des Datenverkehrs beobachten [18] und somit auch Datenverkehr zwischen den einzelnen Tor-Knoten.
Internet-Service-Provider (ISP). Der Internet-Service-Provider, oder auch Internetdienstanbieter, stellt den Internetanschluss der Internetnutzer zur Verfügung. Der ISP bekommt alle Internetpakete übermittelt, die von diesem Internetanschluss versendet oder empfangen werden.
Web-Service-Provider (WSP). Der Web-Service-Provider stellt einen Web-Service, wie z. B. eine Internet-Webseite über das Internet zur Verfügung.
Netzwerk-Administrator (NA). Ein Netzwerk-Administrator administriert ein Computernetzwerk und hat Einsicht in den gesamten Datenverkehr des betrachteten Netzwerkes.
Tor-Knoten-Betreiber (TKB). Tor-Knoten-Betreiber stellen Tor-Knoten (Guard- Middle- oder Exit-Knoten) dem Tor-Netzwerk zur Verfügung.

Externe Partei (EP). Eine externe Partei ist eine Einheit außerhalb des Anonymisierungssystem, die jedoch versucht, ein Teil dieses zu werden. Ein Beispiel wäre ein klassischer Hacker.

1.4 Technologien gegen eine Deanonymisierung

Durch das Benutzen des Tor-Browsers kann eine Verbindung zum Tor-Netzwerk hergestellt werden. Dieser verhindert allerdings nicht die Erkennung, dass man sich mit dem Tor-Netzwerk verbunden hat. Demzufolge können die Internetanschlüsse zurückverfolgt werden, die sich mit dem Tor-Netzwerk verbunden haben. Auf Basis von extensiver und allumfassender Literaturrecherche wurden Technologien extrahiert, die man zusätzlich zu der Tor-Software hinzunehmen kann, um eine potentielle Deanonymisierung zu erschweren. Nachfolgend beschreiben wir kurz alle Technologien, die wir in unserer Arbeit betrachten:

VPN. Bei einem ***V****irtual* ***P****rivate* ***N****etwork* wird ein virtueller Tunnel zu einem VPN-Anbieter aufgebaut, durch welchen alle Internetdatenpakete verschlüsselt geleitet werden. Der VPN-Anbieter schickt anschließend alle Datenpakete zum eigentlichen Ziel weiter. Das Vorschalten eines VPNs vor das Tor-Netzwerk kann zusätzlichen Schutz vor dem Guard-Knoten bieten, während ein VPN nach dem Tor-Netzwerk geschaltet zusätzlichen Schutz vor dem Exit-Knoten bieten kann. Hierbei verwendet man allerdings eine zusätzliche Instanz, der man vertrauen muss - den VPN-Anbieter.
Live-(Betriebs-)Systeme. Bei einem Live-(Betriebs-)System wie z. B. Tails oder Whonix werden alle Internet-Verbindungen standardmäßig über das Tor-Netzwerk geleitet. Wie in Abb. 2 zu sehen ist, werden, falls man nicht solche Betriebssysteme verwendet, nur die Daten über das Tor-Netzwerk anonym verschickt, die der Tor-Nutzer direkt über den Tor-Browser versendet. Alle anderen Daten werden weiterhin über Verbindungen des Clearnets verschickt und sind somit nicht anonymisiert.
Bridges und Pluggable Transports (PTs). Bridge-Knoten, sind Tor-Knoten, die nicht öffentlich gelistet werden und so als zusätzliche Einstiegspunkte in das Tor-Netzwerk dienen können, wenn bspw. eine Regierung alle öffentlich bekannten Tor-Knoten blockiert. Durch Pluggable Transports kann der Datenverkehr verschleiert werden, sodass es nicht mehr ersichtlich ist, dass dieser Datenverkehr Tor-Pakete (die eine eindeutige Struktur aufweisen [24]) beinhaltet. Somit kann man eine anonyme Verbindung zum Tor-Netzwerk herstellen.
Eigener Tor-Knoten als Guard-Knoten. Wie in Abb. 1 gezeigt, ist der Guard-Knoten der erste Tor-Knoten in einem Datenpfad, zu dem man sich direkt verbindet.

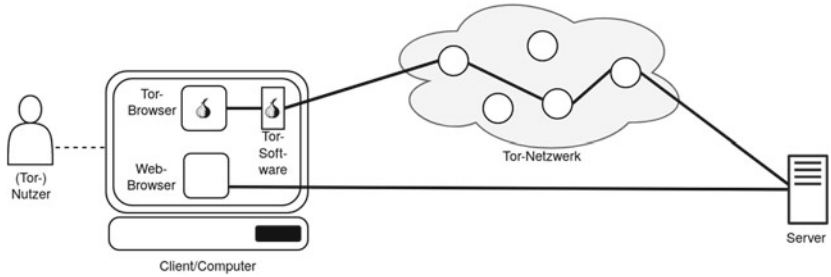


Abb. 2 Verbindungsaufbau über den Tor-Browser vs. Web-Browser

Durch die direkte Verbindung kennt der Guard-Knoten die IP-Adresse des Tor-Nutzers. Demzufolge besitzt der Guard-Knoten eine potentielle Gefahr, Tor-Nutzer angreifen und deanonymisieren zu können. Eine Abhilfe hierfür wäre das Aufsetzen eines eigenen Tor-Knotens und diesen als Guard-Knoten für alle Tor-Verbindungen zu wählen.

PGP. PGP steht für Pretty Good Privacy und wird benutzt, um u. a. digitale Dateien oder Nachrichten zu verschlüsseln und digital zu signieren.

TorChat. TorChat ist ein dezentrales Chatprogramm, das alle Chat-Nachrichten über das Tor-Netzwerk leitet. Neben verschlüsselten Textnachrichten bietet TorChat auch eine sichere Übertragung von Dateien.

Die Verwendung des Tor-Browsers bietet einen Grad an Anonymität auf technischer Basis. Aufgrund unterschiedlicher Ressourcen, die verschiedenen Akteuren zur Verfügung stehen, variiert der Grad der Anonymität allerdings gegenüber unterschiedlichen Akteuren. Die Verwendung von zusätzlichen Technologien kann hier punktuell Abhilfe schaffen.

2 Design und Methode

Für die Beantwortung der Forschungsfragen erfolgt eine Datenerhebung in Form eines Online-Fragebogens (FF1-3) sowie eines Leitfadeninterviews (FF4) mit einem Experten aus dem Bereich der IT-Sicherheitsforschung. Im nachfolgenden Abschnitt werden wir zuerst die Erhebung mittels eines Online-Fragebogens sowie die entsprechenden Variablen erläutern. Daran anschließend werden wir das Vorgehen im Rahmen des Leitfaden-Experteninterviews beschreiben.

2.1 Online-Befragung der Tor-Nutzer

Die Erhebung von Nutzerinformationen, wie Online-Privatheitskompetenz sowie Nutzungsweise ist im Rahmen einer Online-Befragung von Tor-Nutzern erfolgt.

Analysen der Sprache der Inhalte des Tor-Netzwerks zeigen, dass über 75 % des Angebots in englischer Sprache, gefolgt von u. a. Russisch und Deutsch, vorhanden ist [26, 27]. Um ein möglichst großes Publikum zu erreichen, wurde der Fragebogen auf Englisch und Deutsch zur Verfügung gestellt. Der Fragebogen wurde auf den Servern der Fraunhofer Gesellschaft gehostet und via LimeSurvey administriert. Die Einstellungen wurden so getroffen, dass auch eine Teilnahme mit dem Tor-Browser, ohne JavaScript, möglich war. Die Verteilung des Fragebogens erfolgte sowohl im Clear- als auch im Darknet.

Insgesamt bestand der Fragebogen aus 31 Fragen, wobei die erste Frage erfasste, ob die Person den Tor-Browser schon einmal verwendet hatte. Wurde diese Frage verneint, war der Fragebogen an dieser Stelle zu Ende. Um bei den Fragen voranzuschreiten, war die Beantwortung aller Fragen verpflichtend. Einzig die Fragen zur Soziodemografie waren optional.

2.2 Experteninterview

In einem ersten Schritt wurden anhand extensiver Literaturrecherche Technologien aus der Literatur extrahiert, die zusätzlich zur Verwendung des Tor-Browsers eine mögliche Deanonymisierung erschweren. Da sich die Möglichkeit einer potentiellen Deanonymisierung maßgeblich an den vorhanden Ressourcen bemisst, die dem Angreifer zur Verfügung stehen, wurden diese in Anlehnung an frühere Forschung [23] auf die folgenden Ausprägungen festgelegt: Regierung, Internetknoten-Betreiber, Internet-Service-Provider, Web-Service-Provider, lokaler Netzwerkadministrator, Tor-Knoten-Betreiber, externe Partei. In einer Matrix wurde den Technologien dann für jeden oben genannten potentiellen Angreifer auf der Basis eines Experteninterviews eine Gewichtung zugeteilt. Diese orientiert sich an dem Aufwand, mit dem es hinsichtlich der Ressourcen des Angreifers zu einer Deanonymisierung kommen kann.

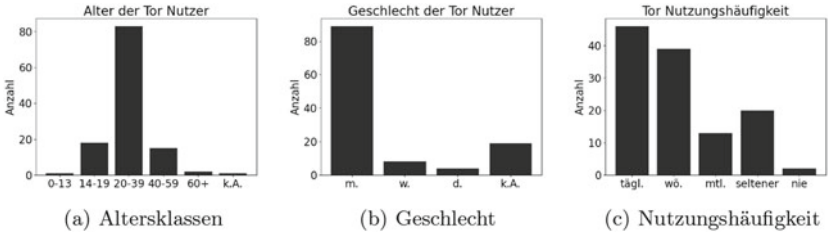
3 Ergebnisse

Nachfolgend werden wir zuerst eine deskriptive Beschreibung des Datensets sowie der soziodemografischen Daten präsentieren. Daran anschließend analysieren wir

die Fragen auf die von uns gestellten Hypothesen hin. Abschließend präsentieren wir das Ergebnis des Experteninterviews zur Erstellung einer Anonymitätsmatrix.

3.1 Datenbeschreibung

Der Fragebogen wurde insgesamt 238 Mal aufgerufen, wovon 120 Personen ihn komplett ausfüllten. Dabei gaben $N = 206$ Nutzer (86,55 %) an, den Tor-Browser schon einmal verwendet zu haben. $N = 11$ (4,62 %) Personen gaben an, den Tor-Browser noch nie verwendet zu haben und beendeten dadurch die Umfrage. $N = 21$ Nutzer (8,82 %) beendeten die Umfrage, ohne die Frage zu beantworten.
Von den 120 Personen, die den Fragebogen komplett ausgefüllt haben, konstituierte die Altersgruppe zwischen 20 bis 39 Jahren mit $N = 83$ (69,17 %) den Großteil der Teilnehmer. $N = 18$ (15,0 %) gehörten der Altersgruppe 14 bis 19 an, gefolgt von $N = 15$ (12,5 %) für die Gruppe der 40 bis 59 jährigen. Eine Person (0,83 %) gab an unter 14 zu sein, $N = 2$ (1,67 %) weitere über 60. $N = 1$ Person enthielt sich der Angabe (vgl. Abb. 3a).
Von den Personen, die freiwillig Angaben zu ihrem Geschlecht gemacht haben, sind $N = 89$ (74,17 %) männlichen Geschlechts, $N = 8$ (6,67 %) weiblich sowie $N = 4$ (3,33 %), die sich mit der Kategorie „anderes“ identifiziert haben (vgl. Abb. 3b).
$N = 46$ (38,33 %) Personen gaben an, Tor täglich zu nutzen. $N = 39$ (32,5 %) nutzen Tor wöchentlich, $N = 13$ (10,83 %) monatlich und $N = 20$ (16,67 %) nutzen Tor seltener. $N = 2$ (1,67 %) Personen gaben an, Tor nie zu verwenden (vgl. Abb. 3c).



(a) Altersklassen (b) Geschlecht (c) Nutzungshäufigkeit

Abb. 3 Teilnehmer der Umfrage

3.2 Analyse

Die Online-Privatheitskompetenz der Tor-Nutzer wurde anhand der Online-Privatheitskompetenzskala OPLIS [17] gemessen. Hierbei wurde der Fragenblock zu „Wissen über Datenschutzrecht" aufgrund der Tatsache ausgelassen, dass dieser auf Basis von deutschem/europäischem Recht entstanden ist, sich die vorliegende Umfrage jedoch an Tor-Nutzer weltweit richtete. Somit umfasste die Erhebung der Online-Privatheitskompetenz 15 statt 20 Fragen. Um eine Vergleichbarkeit der Ergebnisse zu erreichen, wurde im Rahmen der Analyse, angelehnt an neueste Untersuchungen, der Score von 15 auf 20 Fragen extrapoliert [12].

Die Ergebnisse indizieren, dass Tor-Nutzer im Schnitt 81,65 % der Fragen richtig beantwortet haben. Weitere Analysen betreffend soziodemografischer Aspekte zeigten in einer Varianzanalyse keinen signifikanten Effekt des Alters der Tor-Nutzer auf ihre Online-Privatheitskompetenz ($F(2,113) = 1.92$, $p = .152$). Betreffend dem Bildungsgrad hat eine Varianzanalyse ergeben, dass es einen signifikanten Effekt des Bildungsabschlusses auf die Online-Privatheitskompetenz gab ($F(4,112) = 2.98$, $p = .022$). Eine anschließende post-hoc Analyse mit paarweise durchgeführten t-Tests zeigt, dass Personen, die das Abitur abgeschlossen haben ($M = 13.14$, $SD = 1.53$), eine höhere Privatheitskompetenz zeigen, als solche, die studiert haben (($M = 12.12$, $SD = 1.65$), $t(36.53) = 2.60$, $p = .013$, $d = 0.63$), oder auch als solche, die keinen Schulabschluss haben (($M = 11.59$, $SD = 1.80$), $t(31.45) = 2.83$, $p = .08$, $d = 0.9$).

H1a-d postulieren einen Effekt der Nutzungsweise von Tor auf die Online-Privatheitskompetenz. Die Ergebnisse von *H1a* zeigen auf Basis der Berechnung einer einfaktoriellen ANOVA, dass es keinen statistisch signifikanten Effekt der Häufigkeit der Nutzung des Tor-Browsers auf die Online-Privatheitskompetenz der Nutzer gibt ($F(4,115) = 0.239$, $p = .916$). Die Ergebnisse von *H1b* zeigen auf Basis der Berechnung einer einfaktoriellen ANOVA, dass es keinen statistisch signifikanten Effekt des Kontexts der Nutzung des Tor-Browsers auf die Online-Privatheitskompetenz der Nutzer gibt ($F(2,117) = 1.443$, $p = .24$). Die Ergebnisse von *H1c* indizieren, dass Personen, die am Themenbereich „Anonymität" interessiert sind, höhere Werte auf der Online-Privatheitskompetenz-Skala ($M = 12.59$, $SD = 1.58$) erreichten, als solche, die am Themenbereich „Anonymität" nicht interessiert sind (($M = 11.96$, $SD = 1.77$), $t(95.69) = -2.01$, $p = .047$, $d = 0.38$). Die Ergebnisse für *H1d* zeigen, dass Personen, die Tor für „Marktplätze/Handelsseiten" nutzen, niedrigere Werte ($M = 11.32$, $SD = 1.57$) auf der Online-Privatheitskompetenzskala erreichten, als solche, die Tor nicht für „Marktplätze/Handelsseiten" nutzen (($M = 12.52$, $SD = 1.64$), $t(26.01) = 3.065$, $p = .005$, $d = 0.74$).

H2a-d postulieren einen Effekt der Nutzungsweise von Tor auf die in Kombination zu Tor genutzten Anonymisierungstechnologien. Die Ergebnisse zu *H2a* haben auf Basis einer Varianzanalyse ergeben, dass es einen signifikanten Effekt der Nutzungshäufigkeit gab ($F(3,114) = 5.20$, $p = .02$). Eine anschließende post-hoc Analyse mit paarweise durchgeführten t-Tests zeigt, dass Personen, die täglich Tor benutzen ($M = 5.50$, $SD = 1.22$), mehr Technologien kennen, als solche, die Tor wöchentlich (($M = 4.69$, $SD = 1.52$), $t(72.61) = 2.66$, $p = .01$, $d = 0.71$), monatlich (($M = 4.62$, $SD = 1.33$), $t(72.61) = 2.66$, $p = .01$, $d = 0.59$) oder noch seltener (($M = 4.10$, $SD = 1.74$), $t(27.49) = 3.26$, $p = .003$, $d = 1.00$) benutzen. Da die Gruppen im Rahmen der Analyse von *H2b* nicht normalverteilt waren, wurde ein Kruskal-Wallis Rangsummentest durchgeführt. Dieser zeigt, dass es einen signifikanten Effekt des Netzwerktyps auf die Anzahl der bekannten Technologien gab ($H(2) = 22.229$, $p < .001$). Eine anschließende post-hoc Analyse mit paarweise durchgeführten t-Welch-Tests zeigt, dass Personen, die beide Netzwerke ansteuern ($M = 5.39$, $SD = 1.16$), mehr Technologien kennen, als solche Personen, die Tor nur für das Clearnet benutzen (($M = 4.09$, $SD = 1.75$), $t(47.15) = -3.951$, $p < .001$, $d = -0.88$), oder als solche, die Tor nur für das Darknet benutzen (($M = 4.29$, $SD = 1.54$), $t(47.15) = -3.951$, $p = .022$, $d = -0.81$). Für *H2c* hat eine Varianzanalyse gezeigt, dass Personen, die am Themenbereich „Pornographie“ interessiert sind, weniger Anonymisierungstechnologien ($M = 3.94$, $SD = 1.75$) kennen, als diejenigen, die am Themenbereich „Pornographie“ nicht interessiert sind (($M = 5.05$, $SD = 1.42$), $t(19.62) = 2.480$, $p = .022$, $d = 0.76$). Darüber hinaus kennen Personen mit Interesse am Bereich „Software“ mehr Anonymisierungstechnologien ($M = 5.80$, $SD = 0.56$), die zusätzlich zu Tor verwendet werden können, als diejenigen, die am Themenbereich „Software“ nicht interessiert sind (($M = 4.76$, $SD = 1.56$), $t(53.31) = 24.42234$, $p < .001$, $d = -0.70$). Die Analyse von *H2d* hat gezeigt, dass Personen, die „Krypto“-Dienste in Anspruch nehmen, mehr Anonymisierungstechnologien kennen ($M = 5.61$, $SD = 0.76$) als solche, die „Krypto“-Dienste nicht in Anspruch nehmen (($M = 4.64$, $SD = 1.63$), $t(108.10) = 19.56$, $p < .001$, $d = -0.67$). Personen, die „Filesharing“-Dienste nutzen, kennen mehr Anonymisierungstechnologien ($M = 5.43$, $SD = 1.03$) als solche, die „Filesharing“-Dienste nicht nutzen (($M = 4.78$, $SD = 1.58$), $t(42.71) = 5.62$, $p = .022$, $d = -0.43$). Personen, die „Foren“ benutzen, kennen mehr Anonymisierungstechnologien ($M = 5.28$, $SD = 1.25$) als diejenigen, die „Foren“ nicht benutzen (($M = 4.49$, $SD = 1.65$), $t(108.08) = 8.59$, $p = .004$, $d = -0.54$).

Tab. 1 zeigt, dass insgesamt 27 der Befragten angaben, ein VPN als zusätzliche Anonymisierungstechnologie vor das Tor-Netzwerk schalten. 17 der Befragten

Tab. 1 Tor-Nutzer, die angaben, eine Technologie zusätzlich zu Tor zu nutzen

Technologie	VPN (vor)	VPN (nach)	Tails Whonix	Bridges und PTs	Eigener Guard-Knoten	PGP
Anzahl	27	17	54	27	11	67

gaben an, ein VPN hinter das Tor-Netzwerk zu schalten. Live-Betriebssysteme wie Tails oder Whonix nutzen 54 der Befragten. Über Bridge-Knoten verbinden sich 27 Nutzer mit dem Tor-Netzwerk und 11 gaben an, einen eigenen Guard-Knoten für die Verbindung in das Tor-Netzwerk zu nutzen. PGP wird von 67 Nutzern zusätzlich verwendet. Eine Mehrfachnennung war möglich.

In Abb. 4 werden die prozentualen Anteile der Tor-Nutzer, die eine zusätzliche Technologie zu der Verwendung von Tor hinzunehmen, illustriert. Konkret wurden hier die zusätzlichen Anonymisierungstechnologien auf die Variablen der a) Nutzungshäufigkeit, b) Art der Hidden Services, c) Nutzungsweise und d) Themengebiete dargestellt. Beispielsweise nutzen von den 67 Personen, die angeben PGP zu verwenden, ca. 51 % Tor täglich, 28 % wöchentlich und 21 % seltener (vgl. Abb. 4a). Am meisten werden zusätzliche Technologien hinzugenommen, wenn Foren oder soziale Netzwerke im Darknet angesurft werden. Für den Aufruf von pornografischen Seiten wird hingegen weniger zusätzliche Technologien hinzugenommen (vgl. Abb. 4b). Nutzer, die Tor zum Surfen sowohl ins Clearnet als auch ins Darknet verwenden, nutzen vermehrt zusätzliche Technologien, als Nutzer, die Tor nur für das Darknet oder nur für das Clearnet nutzen (vgl. Abb. 4c). Am häufigsten werden zusätzliche Technologien bei Tor-Nutzern hinzugenommen, die sich für die Themen „Anonymität" und „(IT-) Sicherheit" interessieren. Am wenigsten von Nutzern, die sich für Themen wie zum Beispiel Kunst, Online-Spiele, Sport oder Wissenschaft interessieren. Diese werden in Abb. 4d nicht mit angegeben.

H3a-b postuliert einen kausalen Effekt der Online-Privatheitskompetenz der Nutzer auf die in Kombination zu Tor verwendeten Anonymisierungstechnologien. Die Ergebnisse von *H3a* zeigen auf Basis der Berechnung einer linearen Regressionsanalyse keine statistisch signifikanten Ergebnisse ($F = 0.9737$). Auf Basis unserer Werte kann somit nicht von einem derartigen Effekt ausgegangen werden.

H3b Die Ergebnisse von *H3b* zeigen auf Basis der Berechnung einer linearen Regressionsanalyse keine statistisch signifikanten Ergebnisse ($F = 0.2299$). Es besteht somit auf Basis unserer Werte kein linearer Effekt der Online-Privatheitskompetenz der Nutzer auf die Anzahl der einem Nutzer bekannten Anonymisierungstechnologien.

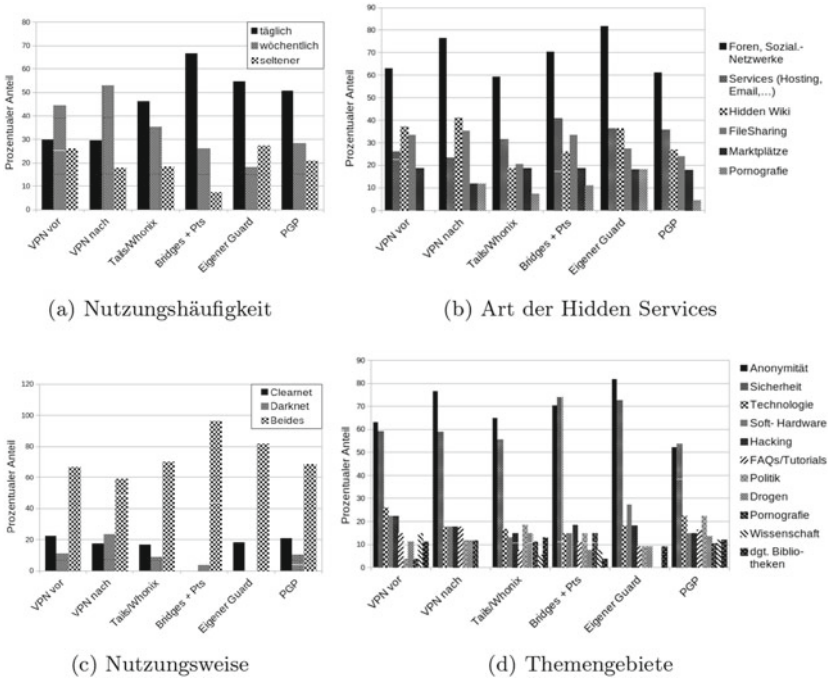


Abb. 4 Prozentualer Anteil der Tor-Nutzer, die eine weitere Technologie zusätzlich zu Tor nutzen

3.3 Anonymitätsmatrix

Forschungsfrage 4 untersucht, inwiefern zusätzliche Anonymisierungstechnologien in Kombination mit Tor vor einer potentiellen Deanonymisierung schützen. Die erstellte Matrix gibt an, welcher Akteur aus Kap. 1.3 erkennen kann, ob ein bestimmter Tor-Nutzer mit den jeweiligen eingesetzten Technologien

a) Tor benutzt und
b) welche Aktivität der Tor-Nutzer über das Tor-Netzwerk durchführt.

Die Einstufung erfolgt mittels der Skala

● schwer, ◑ mittel, ○ leicht

Tab. 2 Anonymitätsmatrix R

Akteur / Technologie	R (a)/(b)	IKB (a)/(b)	ISP (a)/(b)	NA (a)/(b)	TKB_G (a)/(b)	TKB_M (a)/(b)	TKB_E (a)/(b)	WSP (a)/(b)	EP (a)/(b)
Tor-Browser	○/◑	○/●	○/●	○/●	○/●	●/●	⊛/⊛	⊛/⊛	●/●
VPN (vor)	○/◑	◑/●	●/●	●/●	●/●	●/●	⊛/⊛	⊛/⊛	●/●
VPN (nach)	○/◑	○/●	○/●	○/●	○/●	●/●	●/●	⊛/⊛	●/●
Tails, Whonix	○/◑	○/●	○/●	○/●	○/●	●/●	⊛/⊛	⊛/⊛	●/●
Bridges, PTs	◑/◑	●/●	●/●	●/●	○/●	●/●	⊛/⊛	⊛/⊛	●/●
Eigenen Guard-Knoten	○/◑	○/●	○/●	○/●	n/a	●/●	⊛/⊛	⊛/⊛	●/●
TorChat	○/◑	○/●	○/●	○/●	○/ ●	●/●	●/●	●/●	●/●

Regierung. IKB: Internetknoten-Betreiber. ISP: Internet-Service-Provider. NA: Netzwerk-Administrator. TKB_G: Tor-Knoten-Betreiber (Guard). TKB_M: Tor-Knoten-Betreiber (Middle). TKB_E: Tor-Knoten-Betreiber (Exit). WSP: Web-Service-Provider. EP: Externe Partei.
Aufheben der Verbindungsanonymität: ● schwer, ◑ mittel, ○ leicht
Aufheben der Datenanonymität: ⊛

In dieser Skala wird nur die Verbindungsanonymität berücksichtigt, also Informationen, die ausgewertet werden können, die aufgrund des Verbindungsaufbaus selbst anfallen. Die Datenanonymität, also die Dateninhalte, die über diese Verbindung verschickt werden, werden in der angegebenen Skala nicht berücksichtigt. All diese Informationen könnte aber der Exit-Knoten auslesen, sollte der Tor-Nutzer anstatt einer HTTPS-Verbindung nur eine unverschlüsselte HTTP-Verbindung zum Server im Clearnet aufbauen. Gibt der Tor-Nutzer dann u. a. personenbezogene Daten wie beispielsweise den Namen, die Adresse oder andere kritische Informationen über sich selbst bekannt, ist dadurch auch die soziale Anonymität gefährdet. Gleiches gilt für den Web-Service-Provider, der einen Tor-Nutzer identifizieren kann, wenn dieser sich z. B. auf einer Plattform mit seinen Benutzernamen anmeldet. In der Matrix werden solche Aspekte mit

⊛ (Datenanonymität)

gekennzeichnet. Tab. 2 zeigt die erstellte Matrix.

Zu Beachten ist, dass eine Regierung immer die Möglichkeit einer Quellen-TKÜ (Telekommunikationsüberwachung) hat. Durch einen sog. Bundestrojaner kann eine Regierung immer ausspähen, welcher Tor-Nutzer mit wem über was kommuniziert, da dieser Trojaner alle Daten vor dem Verschlüsseln und dem Verschicken in das Tor-Netzwerk direkt auf dem Anwender-PC ausliest. Sollte eine TKÜ zum Einsatz kommen, wird dies hier als *mittel* eingestuft.

4 Diskussion

Ziel der vorliegenden Arbeit war es, die Tor-Nutzergruppe auf ihre Online-Privatheitskompetenz, die Nutzungsweise und Grad der Anonymität zu erforschen. Außerdem wurde eine Anonymitätsmatrix erstellt, in welcher aufgezeigt wurde, inwieweit diverse PETs in Kombination zu Tor vor einer Deanonymisierung vor entsprechenden Akteuren schützt. Die vorliegende Analyse zeigt eine höhere Online-Privatheitskompetenz im Vergleich zu regulären Internetnutzern. Hier gilt es allerdings zu beachten, dass unsere Werte auf Basis von 15 Fragen der OPLIS-Skala auf 20 extrapoliert wurden. Allerdings sind diese Ergebnisse übereinstimmend mit jüngsten Forschungsergebnissen [12]. Einflussfaktoren sind hierbei der Bildungsabschluss, Interessengebiete wie „Anonymität“ sowie die Nutzungsweise für „Marktplätze“. Im Gegensatz zu früheren Arbeiten konnte kein Einfluss des Alters der Nutzer auf die Online-Privatheitskompetenz festgestellt werden. Einflussfaktoren betreffend des Wissens bzw. der Verwendung zusätzlicher Anonymisierungstechnologien sind die Interessensbereiche der Verwendung, wie „Pornografie“ und „Software“, sowie der Kontext der Anwendung. Die Nutzergruppen, die am meisten zusätzliche Technologien verwenden, interessieren sich für die Themen Anonymität und Sicherheit und rufen Foren oder soziale Netzwerke im Darknet auf. Jedoch ist es fraglich, inwieweit Personen, die nicht gesetzeskonformes Material anbieten oder konsumieren wollen, an einer solchen Umfrage teilnehmen und, wenn sie teilnehmen, inwieweit sie diese Informationen angeben.

Betreffend der Anonymitätsmatrix kann generell gesagt werden, dass der Grad der Anonymität davon abhängig ist, welche Ressourcen einem Angreifer zur Verfügung stehen. Ob und wie gut ein Akteur einen Tor-Nutzer deanonymisieren kann, hängt maßgeblich von den Ressourcen des Angreifers ab. Auf Basis dieser Ergebnisse kommen wir zu dem Schluss, dass es einen 100-prozentigen Schutz vor einer möglichen Deanonymisierung nicht geben wird. In Anlehnung an frühere Arbeiten werden dem Akteur „Regierung“ die meisten Ressourcen attribuiert [23]. So hat sie die meisten Möglichkeiten, das Internet flächendeckend überwachen zu können. Insbesondere wäre eine Regierung in der Lage, andere Akteure zum Kooperieren anzuweisen und demzufolge alle Ressourcen der anderen Akteure zu nutzen.

Danksagung Das dieser Publikation zugrunde liegende Verbundprojekt PANDA wurde vom Bundesministerium für Bildung und Forschung unter den Förderkennzeichen 13N14355 und 13N14356 gefördert. Für den Inhalt dieser Publikation sind die Autoren verantwortlich. Die Autoren bedanken sich insbesondere bei York Yannikos für wertvollen Input zur Durchführung der Studie. Außerdem bedanken sie sich bei Oskar Rudolf für die Unterstützung bei der Auswertung der Studie sowie Adrian Worring Pozo und Adrian Kailus für die Unterstützung

bei der Vorbereitung der Durchführung. Schließlich bedanken sie sich bei Charlotta Jacobsen für das Korrekturlesen und ihre Unterstützung beim Editieren.

Literatur

1. Acquisti, A., Gross, R.: Imagined communities: awareness, information sharing, and privacy on the Facebook. In: International Workshop on Privacy Enhancing Technologies. S. 36–58. Springer, Berlin (2006)
2. Altman, I.: The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding. Irvington, New York (1975)
3. Barnes, S.B.: A privacy paradox: social networking in the United States. First Monday (2006)
4. Biryukov, A., Pustogarov, I., Thill, F., Weinmann, R.P.: Content and popularity analysis of tor hidden services. In: 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (ICDCSW). S. 188–193. IEEE (2014)
5. Burgoon, J.K.: Privacy and communication. Ann. Int. Commun. Assoc. **6**(1), 206–249 (1982)
6. Debatin, B., Lovejoy, J.P., Horn, A.K., Hughes, B.N.: Facebook and online privacy: attitudes, behaviors, and unintended consequences. J. Comput. Mediat. Commun. **15**(1), 83–108 (2009)
7. Diaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring anonymity. In: International Workshop on Privacy Enhancing Technologies. S. 54–68. Springer, Berlin (2002)
8. Dienlin, T., Trepte, S.: Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur. J. Soc. Psychol. **45**(3), 285–297 (2015)
9. Gehl, R.W.: Weaving the Dark Web: Legitimacy on Freenet, Tor, and I2P. MIT Press, Cambridge (2018)
10. Gehl, R.W., Synder-Yuly, J.: The need for social media alternatives. Democratic Commun. **27**(1), 78–78 (2016)
11. Graeff, T.R., Harmon, S.: Collecting and using personal data: consumers' awareness and concerns. J. Consum. Market. (2002)
12. Harborth, D., Pape, S.: How privacy concerns, trust and risk beliefs, and privacy literacy influence users' intentions to use privacy-enhancing technologies: The case of Tor. ACM SIGMIS Database: The DATABASE Adv. Inf. Syst. **51**(1), 51–69 (2020)
13. Harborth, D., Pape, S., Rannenberg, K.: Explaining the technology use behavior of privacy-enhancing technologies: The case of Tor and Jondonym. Proc. Priv. Enhancing Technol. **2020**(2), 111–128 (2020)
14. Hayne, S.C., Rice, R.E.: Attribution accuracy when using anonymity in group support systems. Int. J. Hum.-Comput. Stud. **47**(3), 429–452 (1997)
15. Jardine, E.: Privacy, censorship, data breaches and internet freedom: the drivers of support and opposition to dark web technologies. New Media Soc. **20**(8), 2824–2843 (2018)
16. Jensen, C., Potts, C., Jensen, C.: Privacy practices of internet users: self-reports versus observed behavior. Int. J. Hum.-Comput. Stud. **63**(1–2), 203–227 (2005)
17. Masur, P.K., Teutsch, D., Trepte, S.: Entwicklung und validierung der online-privatheitskompetenzskala (oplis). Diagnostica (2017)

18. Murdoch, S.J., Zieliński, P.: Sampled traffic analysis by internet-exchange-level adversaries. In: International Workshop on Privacy Enhancing Technologies. S. 167–183. Springer, Berlin (2007)
19. Owen, G., Savage, N.: Empirical analysis of tor hidden services. IET Inf. Secur. **10**(3), 113–118 (2016)
20. Paine, C., Reips, U.D., Stieger, S., Joinson, A., Buchanan, T.: Internet users' perceptions of „privacy concerns" and „privacy actions". Int. J. Hum.-Comput. Stud. **65**(6), 526–536 (2007)
21. Park, Y.J.: Digital literacy and privacy behavior online. Commun. Res. **40**(2), 215–236 (2013)
22. Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., Dabbish, L.: Anonymity, privacy, and security online. Pew Res. Center **5** (2013)
23. Ries, T., Panchenko, A., Engel, T. et al.: Comparison of low-latency anonymous communication systems-practical usage and performance. In: Ninth Australasian Information Security Conference. S. 77–86. ACS, Australia (2011)
24. Saputra, F.A., Nadhori, I.U., Barry, B.F.: Detecting and blocking onion router traffic using deep packet inspection. In: 2016 International Electronics Symposium (IES). S. 283–288. IEEE, New Jersey (2016)
25. Shelton, M., Rainie, L., Madden, M.: Americans' privacy strategies post-snowden. Pew Research Center (2015), http://www.pewinternet.org/2015/03/16/Americans-Privacy-Strategies-Post-Snowden/
26. Spitters, M., Verbruggen, S., van Staalduinen, M.: Towards a comprehensive insight into the thematic organization of the tor hidden services. In: 2014 IEEE Joint Intelligence and Security Informatics Conference. S. 220–223. IEEE, California (2014)
27. Steinebach, M., Schäfer, M., Karakuz, A., Brandl, K., Yannikos, Y.: Detection and analysis of tor onion services. In: Proceedings of the 14th International Conference on Availability, Reliability and Security, S. 1–10. ACM, New York (2019)
28. Trepte, S., Dienlin, T.: Privatsphäre im internet. Neue Medien und deren Schatten. Mediennutzung, Medienwirkung und Medienkompetenz, , S. 53–79 (2014)
29. Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A., Lind, F.: Do people know about privacy and data protection strategies? towards the „online privacy literacy scale" (oplis). In: Reforming European data protection law, S. 333–365. Springer, Dordrecht (2015)
30. Weinberger, M., Zhitomirsky-Geffet, M., Bouhnik, D.: Factors affecting users' online privacy literacy among students in Israel. Online Inf. Rev. **41**, 655–671 (2017)
31. Westin, A.: Privacy and freedom new york atheneum, 1967. Privacy and Personnel Records, The Civil Liberties Review (Jan./Feb., 1976) S. 28–34 (1967)
32. Wills, C., Zeljkovic, M.: A personalized approach to web privacy-awareness, attitudes and actions. Worcester Polytechnic Institute, Worcester (2010)