Das Internet der Dinge
Die Auswirkungen »smarter« Geräte auf häusliche Gewalt

Leonie Maria Tanczer

Digitale Gewalt beschreibt wie digitale Medien (z.B. Handys oder das Internet) zur Belästigung oder Kontrolle von Personen genutzt werden. Im Zusammenhang mit häuslicher Gewalt und Gewalt in der Partnerschaft kann digitale Unterdrückung viele Formen annehmen (vgl. Dragiewicz u.a. 2018; Harris/Woodlock 2018; Woodlock 2017). Sie kann obszöne oder ungewollte Nachrichten oder Anrufe umfassen, bildbasierte Grenzüberschreitungen wie ›Rache Pornos‹ (vgl. Citron/Franks 2014; McGlynn/Rackley/Houghton 2017) sowie Aufspürgeräte, sogenannte Tracker, welche durch Mobiltelefone oder andere Systeme steuerbar sind. Digitale Gewalt ist hier als ein großes ›Sammelbecken‹ vorstellbar, in dem sowohl technisch ›einfache‹ Delikte sowie technisch anspruchsvollere Vergehen zusammenkommen. Die Letzteren beinhalten zum Beispiel unautorisierte Zugriffe auf E-Mail-Konten oder die Verwendung von dedizierter Spionagesoftware (Spyware)[1].

Das Internet der Dinge

Der rasante Technologiewandel bietet Täter*innen immer mehr Instrumente zur Kontrolle von Opfern und Betroffenen. Insbesondere der Anstieg von »smarten« Internet-verbundenen Geräten – auch bekannt als das »Internet der Dinge« (Internet of Things, kurz: IoT) – sollte genauer unter die Lupe genommen werden. IoT ist ein Überbegriff für verschiedene Technologien.

1 Siehe Beitrag: Der Feind in der eigenen Tasche. Stalkerware und digitale Überwachung im Kontext von Partnerschaftsgewalt.

Die Bezeichnung beschreibt Objekte – häufig Produkte, die zuvor offline und daher analog waren – welche jetzt netzwerkfähig sind. Solche miteinander verbundenen »Dinge« sind die direkte Erweiterung des Internets in eine Reihe von Geräten und Waren (vgl. Tanczer u.a. 2019b: 37). Das sich manifestierende neue digitale Umfeld – wie etwa das »Smart Home« – besteht somit nicht mehr nur aus Internet-verbundenen Telefonen, Laptops und Computern, sondern vielen anderen alltäglichen Gegenständen wie etwa Türen, Heizungen und Glühbirnen. Unsere »smarte« Zukunft zeichnet sich deshalb erstens durch eine Ausbreitung von verschiedenen Gebrauchsgegenständen aus, die scheinbar unsichtbar Daten sammeln; zweitens durch Systeme, die diese gesammelten Informationen interpretieren und nutzen; und drittens durch Antriebselemente, die auf Basis dieser Daten ohne direkte menschliche Handlung Maßnahmen ergreifen.

Solche »intelligenten« oder »digital aufgerüsteten« Produkte (vgl. Mattern/Floerkemeier 2010: 107) sind jedoch nicht nur die typischen Gadgets, die wir mit dem Begriff IoT verbinden. Neben gewohnten IoT-Geräten wie smarte Toaster, Türschlösser oder Kühlschränke, beschreibt der Begriff IoT auch winzige Sensoren, die Daten wie die Feuchtigkeit, Temperatur oder Luftqualität messen. Darüber hinaus bezeichnet IoT auch größere cyberphysische Systeme, die sowohl untereinander als auch mit dem Menschen kommunizieren können. Ein Beispiel hierfür wären selbstfahrende, autonome Fahrzeuge. Die Anwendungsbereiche des IoT sind daher breit gefächert und reichen von Geräten zur Steigerung der persönlichen Fitness, Produkte für die Unterstützung von betreutem Wohnen bis hin zu umfangreichen Verkehrsmanagement- und Verkehrsinfrastrukturen (vgl. Tanczer u.a. 2018e: 1). Die endlosen Möglichkeiten, die sich aus der Kommunikation zwischen Geräten und der damit assoziierten Datensammlung ergeben, erklärt, warum IoT-Systeme mit dem Begriff smart (im Sinne von klug) in Verbindung gebracht werden. Die Netzwerkfunktionalität birgt jedoch auch erhebliche Risiken, die einer genaueren Prüfung bedürfen. Auf den folgenden Seiten werden Erkenntnisse aus dem Forschungsprojekt Gender and IoT (GIoT) besprochen (vgl. Lopez-Neira u.a. 2019; Parkin u.a. 2019; Tanczer u.a. 2018b). GIoT ist ein interdisziplinäres Projekt am University College London (UCL) in Großbritannien. Das Forschungsteam hat die Veränderungen, die digitale Gewalt im Kontext von häuslicher Gewalt unterläuft, im Laufe der letzten drei Jahre genauer untersucht. Einige der Ergebnisse dieser Forschungsaktivitäten beinhalten Handlungsempfehlungen für Beratungsstellen, politische

Akteur*innen sowie IoT-Entwickler*innen (vgl. Tanczer u.a. 2018b; Tanczer u.a. 2018c; Tanczer u.a. 2019c).

Dieser Artikel enthält deshalb Informationen zu den Eigenschaften und denkbaren Auswirkungen von IoT-Systemen im Rahmen von häuslicher Gewalt. Daran anschließend folgt eine Auflistung möglicher Interventionsmöglichkeiten. Diese sollen vor allem den Betroffenen dienlich sein, mögen aber auch Hilfseinrichtungen, Industrievertreter*innen und Politiker*innen nützliche Ideen bieten. Alle besprochenen Vorschläge sollten selbstverständlich stetig neu bewertet, kontinuierlich verbessert und durchgehend getestet werden. Nur ein sich wiederholender, reflektierter sowie Trauma-informierter Interventionsprozess, basierend auf Forschungsdaten sowie den Bedürfnissen von Betroffenen, kann evidenzbasierte Lösungen sowie gut informierte Entscheidungen (von denen es leider immer noch nicht genug gibt) garantieren. Der Artikel präsentiert demnach hoffentlich eine geeignete Grundlage für Leser*innen, die sowohl in der Wissenschaft als auch der Praxis tätig sind. Er stellt Orientierungshilfen dar, um diese neue Form der IoT-unterstützten digitalen Gewalt besser zu verstehen und souveräner bekämpfen zu können.

Anstieg und Auswirkungen des Internets der Dinge

Trotz der zunehmenden Verbreitung digitaler Technik in unserem täglichen Leben gibt es immer noch wenig Forschung und Gutachten zu der wachsenden Bedrohung, die von digitaler Gewalt ausgeht (vgl. Henry/Powell 2018: 196). Bis heute ist die britische Frauenberatungsstelle Refuge eine der wenigen Organisationen in Großbritannien (wenn nicht sogar die Einzige), die digitale Gewalt explizit in ihrem Archiviersystem vermerkt. Als Folge dieser Dokumentation weist Refuge darauf hin, dass im Jahr 2019 72 % ihrer Klient*innen Gewalt durch digitale Systeme erlebten (vgl. Refuge 2020a: o.S.). Bedenkt man, dass dies nur die Erfahrung einer einzigen Beratungsstelle in Großbritannien ist, so muss davon ausgegangen werden, dass die Anzahl, der von digitaler Gewalt betroffenen Frauen, sehr hoch sein dürfte. Leider lässt die Statistik die Nuancen von digitaler Gewalt nicht erkennen und erlaubt es daher nicht, zwischen verschiedenen Formen, Ausprägungen und Schweregraden zu unterscheiden.

Die Analyse von Refuge verweist auf die gegenwärtigen Bemühungen zum Thema digitale Gewalt. Diese Bestrebungen setzen sich primär mit ›konventionellen‹ digitalen Risiken wie dem Missbrauch auf Social Media

Plattformen oder dem Vorbehalt von Geräten wie Laptops und Telefonen durch Täter*innen auseinander (vgl. Douglas/Harris/Dragiewicz 2019: 555). Allerdings verändert sich die Risikolandschaft für Betroffene ständig. Dies wird u.a. durch den zunehmenden Einsatz von Drohnen, Trackern oder »Hacker-for-Hire-Diensten«[2] in Gewaltbeziehungen immer deutlicher. IoT im Speziellen beschreibt eine Entwicklung von Technologien, welche die Risikoverläufe für Betroffene von häuslicher Gewalt erweitern können. Zugleich verschmilzt IoT mit einem ganzen Spektrum von anderen Anwendungsgebieten und Innovationen, einschließlich digitaler Zahlungssysteme, Blockchain-Technologien oder dem ominösen Begriff der künstlichen Intelligenz (vgl. Banerjee/Lee/Choo 2018). Letzteres kann als »Maschinelles Lernen« beschrieben werden und erklärt die Verwendung von statistischen Modellen, um Muster zu identifizieren und Präferenzen von Nutzer*innen besser einschätzen zu können.

Genau wie Handys und Laptops Teil unseres Lebens geworden sind, so können wir davon ausgehen, dass IoT gekommen ist, um zu bleiben. Schätzungen zufolge wird die Zahl der weltweit angeschlossenen IoT-Geräte jährlich um durchschnittlich 12 % steigen und voraussichtlich von fast 27 Milliarden im Jahr 2017 auf 125 Milliarden im Jahr 2030 wachsen (vgl. IHS Markit 2017: o.S.). Während diese Produkte noch nicht Teil jedes Haushalts sind und wir auch noch nicht über die exakten Daten zu ihrem Missbrauch in häuslichen Gewaltvorfällen verfügen (vgl. Tanczer u.a. 2018b: o.S.), sollte sich die Gesellschaft dennoch auf ihre missbräuchliche Verwendung vorbereiten. Eine ähnliche Dynamik haben wir auch im Zuge der Ausweitung digitaler Gewalt durch das Internet und Smartphones gesehen. In diesem Fall nahmen die Missbrauchsmuster parallel zu der steigenden Verfügbarkeit und Erschwinglichkeit dieser Systeme zu (vgl. Gámez-Guadix/Borrajo/Calvete 2018; Harkin/Molnar/Vowles 2020)[3]. In Anbetracht dieser Tatsache ist es von entscheidender Bedeutung, sich für die IoT-unterstützte Gewalt zu wappnen, vor allem, da ihr Gebrauch stetig wächst, ihre Funktionalität konstant zunimmt und die Kosten für diese Geräte immer weiter sinken.

2 Hacker-for-Hire-Dienste beschreiben Leistungen, welche gezielte Angriffe auf zum Beispiel E-Mail-Konten für jene bieten, die bereit sind für solche illegalen Aktivitäten zu bezahlen (vgl. Mirian 2019).

3 Siehe Beitrag: Erfahrungen mit der Beratung von betroffenen Mädchen und Frauen im Kontext digitaler Gewalt.

Was IoT-Systeme einzigartig macht, ist ihre Konnektivität, also ihre Verbundenheit untereinander. Mit diesen smarten Geräten können verschiedene Produkte miteinander verknüpft werden. Dadurch entsteht ein voneinander abhängiges Netzwerk, in dem im Grunde genommen alle einzelnen Gegenstände miteinander »sprechen« (vgl. Tanczer u.a. 2019b; Taylor u.a. 2018). Während viele IoT-Systeme gegenwärtig immer noch eine Form menschlichen Handelns erfordern – beispielsweise durch das Drücken einer Taste oder der Aktivierung über eine App – wird erwartet, dass sie bald ohne direktes menschliches Eingreifen operieren und die Gewohnheiten der Nutzer*innen im Laufe der Zeit ›lernen‹. Aufgrund ihrer Palette an Funktionen (einschließlich ihrer Fähigkeit ferngesteuert zu werden, Video- und Audioaufzeichnung zu tätigen und Standortinformationen zu teilen), haben IoT-Geräte das Potenzial, sowohl unser Verhältnis als auch unsere Interaktion mit digitalen Systemen sowie mit anderen Menschen zu verändern.

Die Risiken, die IoT für Betroffene von häuslicher Gewalt mit sich bringen, haben unter anderem Wissenschaftler*innen wie Leitão (2019), Strengers u.a. (2019) und Slupska (2019) begonnen zu erforschen. Deren Studien zeigen, welche Auswirkungen IoT auf die Sicherheit und Privatsphäre von Betroffenen digitaler Gewalt hat. In ähnlicher Weise führte das GioT-Forschungsteam eine »Usability«-Analyse[4] von persönlichen Sprachassistenten wie Google Home und Amazon Echo durch (vgl. Parkin u.a. 2019) und veröffentlichte eine Broschüre für Betroffene sowie Beratungsstellen (vgl. Tanczer u.a. 2018c). In beiden Publikationen wurden einige der häufigsten Risiken von IoT-Geräten zusammengefasst. Zu den Gefahren, die der gegenwärtige Stand der Literatur aufzeigt, gehören unter anderem der Missbrauch von smarten Technologien, um andere Menschen auszuspionieren, ihre Bewegungen zu verfolgen oder Kontrolle über sie auszuüben. Zum Beispiel ermöglicht die Fernsteuerung von Heizung, Beleuchtung und Jalousien es Täter*innen, ihre Opfer durch deren ungeahnten Einsatz aus der Ferne einzuschüchtern. Internet-verbundene Sicherheitskameras oder Smart TVs bieten die Gelegenheit Betroffene zu überwachen oder zu stalken. Intelligente Sicherheitssysteme wie Bluetooth-fähige Türschlösser bieten eventuell Zugang zu Immobilien. Alle diese Beispiele weisen auf die Fähigkeit von IoT-Systemen hin, ein Werkzeug für »Gaslighting« zu werden. Das letztgenannte Konzept beschreibt eine Form der psychischen

4 Eine Usability-Analyse beschreibt einen Gebrauchstauglichkeitstest, der Software- und Hardwareprodukte auf ihre potenzielle Verwendung sowie Missbrauch evaluiert.

Gewalt, die ein Opfer gezielt desorientiert und manipuliert, damit Betroffene sukzessive an deren Realität und Selbstbewusstsein zu zweifeln beginnen (vgl. Sweet 2019).

Parallel zu der missbräuchlichen Nutzung von IoT-Fähigkeiten fehlt es smarten Systemen häufig an etablierten Sicherheits- und Datenschutzstandards (vgl. Brass u.a. 2018; DeNardis 2020; DeNardis/Raymond 2017; Schneier 2017). In der Tat sind sie häufig mangelhaft konzipiert, bieten keine regelmäßigen Software-Updates und fordern Benutzer*innen oftmals nicht auf, Standardkennwörter zu ändern. Außerdem basieren IoT-Geräte auf der inhärenten Annahme, dass sich alle Benutzer*innen eines kommunalen Haushalts gegenseitig vertrauen und einen gleichen Kenntnisstand über den Umgang mit diesen Technologien haben. Dies berücksichtigt weder die in einer Gewaltbeziehung vorherrschende Machtdynamik zwischen Täter*in und Opfer (vgl. McCarthy/Mehta/Haberland 2018), noch dass Mitbewohner*innen gegebenenfalls unterschiedliche Präferenzen oder Datenschutzanforderungen haben (vgl. Muir/Joinson 2020).

Ferner durchläuft unsere Gesellschaft auch aktuell einen Wandel: weg von persönlichen zu gemeinschaftlichen, kollektiven Geräten. Diese Verschiebung weist darauf hin, dass wir Wege finden müssen, um digitale Produkte besser zu sichern. Zum einen bedeutet das, dass es nun nicht nur einzelne, personenbezogene Daten zu schützen gilt. Vielmehr müssen Daten über jede Person, die einen IoT-unterstützten Haushalt betritt, effektiv gesichert, aber auch gelöscht und modifiziert werden können. Zum anderen verändern solche »Gruppengeräte« die Dynamiken eines Haushaltes (vgl. Strengers u.a. 2019). Da in vielen Familien primär Männer – wie etwa Partner oder Söhne – für den Kauf, Installation und Wartung von technischen Systemen verantwortlich sind, kann eine solche Besitz- und Nutzungsverlagerung dazu führen, dass Frauen noch stärker von relevanten Entscheidungen sowie der Verwendung von digitalen Technologien ausgeschlossen werden.

Auch wenn smarte Produkte sicherlich auch positive Effekte für Betroffene von häuslicher Gewalt bieten können (vgl. Burdon/Douglas 2017: o.S.), die Allgegenwart, Reibungslosigkeit und Verbreitung von unseren neuen *immeran*-Geräten beschreibt einen besorgniserregenden Trend. Vor diesem Hintergrund werden im folgenden Abschnitt einige mögliche Interventionsoptionen erörtert. Diese Empfehlungen können hoffentlich dazu beitragen, den Missbrauch von IoT-Systemen gegen Betroffene von häuslicher Gewalt zu bekämpfen.

Interventionsmöglichkeiten

Viel zu häufig folgt der Entdeckung von Problemen, die durch Technik hervorgerufen wird, ein Aufruf nach noch mehr Technik. Doch kaum ein gesellschaftliches Übel – sei es häusliche Gewalt, Gewalt in der Partnerschaft oder sexueller Missbrauch – kann, noch sollte es, durch technische Mittel allein gelöst werden. Stattdessen sollte eine Mischung aus sozio-technischen Interventionsmöglichkeiten zum Einsatz kommen.

Menschenbezogene Interventionen

Partnergewalt ist kein neues Phänomen. Es ist ein grundsätzlich komplexes, systemisches und strukturelles Problem. Es umfasst eine Reihe von kontrollierenden und einschränkenden Verhaltensweisen, die nicht einfach durch eine App oder eine »Anti-Rape Technology«[5] bewältigt werden können. Eine tiefgreifendere Einsicht, die es in Hinblick auf digitale Gewalt zu teilen gibt, ist, dass es Interventionen benötigt, die sich an dem Bedarf der betroffenen Personen orientieren. Diese müssen die soziale Dynamik von Gewaltmustern berücksichtigen und sollten *von* Menschen *für* Menschen eingesetzt werden.

Betroffene digitaler Gewalt

Die aktuelle Bandbreite an ›raschen Lösungen‹, um digitaler Gewalt entgegenzuhalten, ist häufig belastend für die Betroffenen. Gegenwärtige Ansätze fordern von Betroffenen zu agieren, ihr Verhalten zu ändern und pro- sowie reaktive Maßnahmen zu treffen (vgl. Harris/Woodlock 2018: 539). Solche Interventionen sind zeitaufwändig, anspruchsvoll und kreieren zusätzliche Bürden für Personen, die bereits mit einer Palette von Stressfaktoren und Überlegungen konfrontiert sind. Derlei Lösungen umfassen Apps zum Protokollieren von Gewaltvorfällen[6], Webseiten, Beratungsdatenbanken und

5 Anti-Rape Technologies oder zu Deutsch Anti-Vergewaltigungstechnologien bezeichnen eine Bandbreite an Produkten, die zum Zweck der Verhinderung oder Abschreckung von Vergewaltigung erfunden wurden. Beispiele umfassen Keuschheitsgürtel, Anti-Fummel-Sticker, reißresistente Kleidung, Schnelltests die Drogen in Getränken evaluieren können bis hin zu »smarten« Ringen, die einen Panikknopf zum Alarmieren von Bekannten enthalten (vgl. Harris 2019: o.S.).

6 Siehe hierzu die Hestias Bright Sky-App und die NO STALK-App vom Weißen Ring.

Checklisten zum Nachlesen, wie auf digitale Gewalt reagiert werden kann[7] sowie Online-Beschwerdeformulare, um beispielsweise die Verwendung von nicht einvernehmlich geteilten Bildern zu melden.[8] Tatsächlich ist sogar das GIoT-Forschungsteam dieser Dynamik gefolgt und hat einen IoT-Überblick (vgl. Tanczer u.a. 2018d) sowie eine Ressourcenliste (vgl. Tanczer u.a. 2019c) veröffentlicht. Obgleich gut gemeint, kreieren all diese Maßnahmen Annahmen zum ›richtigen‹ Umgang mit Technologien und verschieben die Verantwortung, sich gegen solche Vorgehen zu wehren, an die Opfer anstelle der Verursacher*innen von Gewalt.

Eine stärkere Betonung sollte deshalb – wie auch bei analoger Gewalt – auf Opfer-zentrierte Lösungen gelegt werden. Vorgeschlagene Maßnahmen sollten nicht verlangen, dass Betroffene etwas zu lesen, melden oder verändern hätten. Vielmehr müssen Ansätze geschaffen werden, die ihre Situation erleichtern. Dies kann etwa durch die Bereitstellung von »One-Stop« Konzepten – sprich die Zentralisierung von verschiedenen Anlaufstellen, welche auch technische Unterstützung bieten – erreicht werden (vgl. Rising Sun 2020: o.S.). Ebenso mag die Einführung spezialisierter digitaler Gewalt-Hotlines, gezielter digitaler Gewalt-»Kliniken« (Havron u.a. 2019) sowie der Ausbau technischer Fähigkeiten im Beratungssektor dienlich sein (Tanczer u.a. 2018b: 6).

Die Kritik an der technischen ›Aufrüstung‹ und ›Reformierung‹ von Opfern durch Trainings oder durch die Vermittlung anderer Ratschläge ist von großer Relevanz in Bezug auf IoT. Smarte Geräte sind vielfältig. Ihre Einstellungen und Funktionen unterscheiden sich häufig und oft kann ein einziges Softwareupdate die Nutzer*innenoberfläche verändern. Solche Modifizierungen können dazu führen, dass Betroffene veröffentlichte schriftliche Anleitungen oder YouTube Videoerklärungen nicht Schritt für Schritt folgen können. Bedenkt man in welcher Belastungssituation sich Gewaltopfer befinden, so wird deutlich, wie problematisch und womöglich sogar unrealistisch solche Erwartungshaltungen sein können.

Das GIoT-Forschungsteam war immer darauf bedacht, Betroffenen keine universellen technischen ›Ratschläge‹ zu geben. Jede Empfehlung muss die

7 Siehe hierzu eSafety Women und bff-Webseite www.aktiv-gegen-digitale-gewalt.de. Auf dieser Plattform finden Betroffene von geschlechtsspezifischer digitaler Gewalt Informationen und Beratungsangebote in Fachberatungsstellen.

8 Siehe hierzu den Priority Channel der spanischen Datenschutzbehörde.

einzigartige Situation des Opfers berücksichtigen und sich an deren jeweiligem Risikoprofil ausrichten. Es empfiehlt sich zum Beispiel einer Person nicht schlichtweg die Anregung zu geben, ihr Passwort zu ändern; vor allem nicht, wenn die Möglichkeit besteht, dass der/die Täter*in heimlich Kontrolle über jene Technologie hat. Die Anweisung solche Einstellungen zu revidieren, kann bei gewalttätigen Partner*innen Verdacht und Misstrauen auslösen. Dies wiederum kann dazu führen, dass eine Gewaltsituation weiter eskaliert und sich das Opfer in einer noch brenzligeren Situation vorfindet. Die Berücksichtigung der verschiedenen Phasen der Gewalt in der Partnerschaft und die konkrete Situation, in der ein Opfer ist, sind daher von entscheidender Bedeutung (vgl. Matthews u.a. 2017b: 2193). Das Knowhow, das der Beratungssektor in Bezug auf die Evaluierung von Gewaltkontexten derzeit hat, darf deshalb nicht unterschätzt werden. Des Weiteren bieten diese Organisationen nicht nur risikobasierte Unterstützung für Betroffene, sondern ein professionelles und menschliches Element, das kein Chatbot, keine App oder Ressourcenliste jemals in der Lage sein wird zu geben.

Täter*innen

Daten und Informationen über digitale Gewalt und insbesondere, IoT-unterstützten Missbrauch sind rar. Evidenzbasierte Einblicke in das Verhalten und den Umgang von Gewalttäter*innen können daher nicht angeboten werden. Nichtsdestotrotz gibt es eine wachsende Zahl von Literatur, die sich auf Täter*innen fokussiert – einschließlich Veröffentlichungen zu der Verbreitung von nicht einvernehmlich geteilten Bildern und Videos (vgl. Eaton u.a. 2020), digitale Gewalt-bezogene Deliktfaktoren (vgl. Duerksen/Woodin 2019; Muncaster/Ohlsson 2019; Reyns 2019) und Studien zu Straftäter*innen, die beispielsweise in »Cyber-Sextortion«, sprich Erpressungsmechanismen, involviert sind (vgl. O'Malley/Holt 2020). Diese Untersuchungen müssen erweitert werden.

In Großbritannien arbeitet das Drive-Projekt mit Täter*innen von häuslicher Gewalt zusammen, um die Sicherheit von Opfern und Betroffenen zu erhöhen (vgl. Hester u.a. 2019: o.S.). Weniger als ein Prozent der Täter*innen unterziehen sich spezieller Interventionen und Rehabilitierungsprozesse, um ihr Verhalten zu ändern (vgl. Drive Partnership 2020: o.S.). Aufgrund dieser geringen Zahl wird eine wichtige Gelegenheit verpasst, Täter*innen daran zu hindern ihr Opfer weiter zu bedrohen sowie neue potenzielle Opfer zu finden. Da Täter*innen eine Reihe von Werkzeugen zur psychologischen, körperli-

chen, sexuellen, finanziellen und emotionalen Gewalt zur Verfügung stehen, müssen Interventionen sich auch zunehmend damit auseinandersetzen, welchen Einfluss neue Technologien auf Täter*innen haben. Daher haben zum Beispiel mehr als 70 Unterzeichner*innen im Jahr 2020 die britische Regierung dazu aufgefordert in eine explizite Täter*innen-Strategie zu investieren (vgl. Drive Partnership 2020: o.S.). Sofern diese Strategie Umsetzung findet, kann hoffentlich auch ein stärkerer Fokus auf digitale Gewalttäter*innen gelegt werden.

Beratungsstellen und Polizei

Im Zuge des GIoT-Projekts stellte das Forschungsteam einen Mangel an Bewusstsein und Kapazität rund um das Thema digitale Gewalt fest. Beratungsstellen sind sich zwar der Folgenschwere von digitaler Gewalt bewusst, aber ihre Expertise, sich insbesondere den Risiken durch aufkommende Technologien wie dem IoT zu stellen, ist eingeschränkt (vgl. Lopez-Neira u.a. 2019: 25). Staatliche Stellen sowie Beratungsstellen fühlen sich noch nicht einmal in der Lage zufriedenstellend oder umfassend auf ›konventionelle‹ Formen von digitaler Gewalt zu reagieren; wie zum Beispiel die Beratung von Betroffenen von Spyware oder online Belästigungen. Dieser Mangel an Fachwissen ist besorgniserregend, insbesondere da noch stärkeres technisches Potenzial erforderlich sein wird, um IoT-unterstützte Missbrauchsfälle zu bewältigen. Das Wissen und die Kompetenz des Sektors müssen deshalb erhöht werden. Während Beratungsstellen begonnen haben Trainingseinheiten zur sicheren Nutzung von digitaler Technik für Betroffene zur Verfügung zu stellen, braucht der Sektor mehr Unterstützung sowie finanzielle Förderung. Diese Zuwendungen erlauben Organisationen in die notwendigen Ressourcen zu investieren und auf die vorhandenen Schwachstellen in Hinblick auf die Bandbreite digitaler Gewaltmuster zu reagieren (vgl. Powell/Henry 2018; Snook/Chayn/SafeLives 2017; Think Social Tech/Snook/SafeLives 2019).

Es bedarf der Schulung von Beratungspersonal und dem Zugang zu technischem Knowhow. Dies kann beispielsweise über die Einrichtung einer speziellen digitalen Gewalt-Hotline für Betroffene (vgl. Tanczer u.a. 2018b: 6) und dem Sicherheitscoaching von Beratungsstellen erreicht werden (vgl. Tanczer 2018a: o.S.). Darüber hinaus werden zusätzliche Mittel benötigt, um die steigenden Schulungskosten und Qualifizierungsbemühungen auszugleichen. Dies ist vor allem deshalb erforderlich, da diese Trainings kontinuierlich durchgeführt und aktualisiert werden müssen. So erhielt

beispielsweise eine der größten Frauenberatungsstellen in Großbritannien einen dreijährigen Förderzuschuss, um das interne, organisationstechnische Wissen zum Thema digitale Gewalt von Grund auf aufzubauen (vgl. Refuge 2020b: o.S.). Die Institution zählt nun zu einer der führenden Akteur*innen in diesem Gebiet in Großbritannien, hat speziell dafür vorgesehene »Tech Abuse Leads« und ihr Beratungsrepertoire umgekrempelt und gibt auch international wichtige Impulse.

Während es nicht ausreicht, die Verantwortung für den Erhalt solcher Mittel einzelnen Organisationen zu überlassen, müssen nachhaltige Subventionen für die Umsetzung solcher spezialisierten Dienste garantiert werden. Diese Bemühungen betreffen auch die Strafverfolgung und Justiz. Beispielsweise Polizeieinheiten, die sich sowohl auf häusliche Gewalt als auch auf Internetkriminalität fokussieren, sind aufgefordert enger zusammenzuarbeiten. Zusätzlich muss ermöglicht werden, dass auf digitale Gewaltvorfälle rasch und professionell reagiert wird. Polizeisektionen brauchen die notwendigen technischen Fähigkeiten, um die Vielzahl an digitalen Geräten, welche durch den Zuwachs an smarten Systemen weiter steigen werden, effektiv und zeitgerecht zu analysieren. Nur die zügige Evaluation dieser Produkte ermöglicht Klarheit für Betroffene sowie eine prompte Ahndung von Täter*innen.

Letzten Endes muss auch das Risiko von digitaler Gewalt in der Gefährdungsbeurteilung und Sicherheitsplanung von Betroffenen einbezogen werden (vgl. Tanczer u.a. 2018b: 6). Das GIoT-Forschungsteam stellte hierbei fest, dass digitale Gewalt gegenwärtig weder bei Beratungsstellen noch bei der Polizei ausreichend in diesen Gefährdungsbeurteilungen und noch weniger in der Sicherheitsplanung von Opfern berücksichtigt wird. Selbst wenn digitale Gewalt bedacht wird, so beinhalten diese Leitfäden kaum Referenzen zu neuen Technologien. Diese Mängel bergen ein Risiko für Betroffene, welche aufgrund ihrer individuellen Bedürfnisse womöglich nicht die richtige Beratung und Anweisungen erhalten.

Technologie- und designorientierte Intervention

Anstatt *mehr* Technik zu fordern, appelliert das GIoT-Forschungsteam an die Industrie, sich auf die Erarbeitung *besserer* technischer Lösungen zu konzentrieren. Dazu gehört auch die Verbesserung der Sicherheitsfunktionen, die Leichtigkeit, mit der Privatsphäre-Änderungen umgesetzt werden können und die allgemeine Weiterentwicklung der Nutzer*innenfreundlichkeit

von IoT-Geräten (vgl. Parkin u.a. 2019). Unternehmen müssen proaktiv den Missbrauch ihrer Systeme voraussehen und mit Bedacht verhindern. Um die Auswirkungen von digitaler Gewalt in der Partnerschaft besser berücksichtigen zu können, empfiehlt es sich eine Kooperation zwischen der Wirtschaft und dem Beratungssektor anzustreben. Informatiker*innen und Informationssicherheitsspezialist*innen ist es empfohlen, eng mit Sozialarbeiter*innen und anderen Akteur*innen, die Betroffene von häuslicher Gewalt unterstützen, zusammenzuarbeiten. Solch ein Austausch ermöglicht es Risiken und Schwachstellen, die im Kontext der Gewalt in der Partnerschaft gefährlich werden könnten, zu erkennen und dagegen zu intervenieren (vgl. Slupska/Tanczer im Erscheinen). Des Weiteren können die Sicherheits- und Privatsphäre-Bedürfnisse von Betroffenen in der Entwicklung von IoT Systemen priorisiert werden (vgl. Arief u.a. 2014; Matthews u.a. 2017a; Matthews u.a. 2017b).

Es wäre kurzsichtig davon auszugehen, dass eine einzige technische Optimierung und Designänderung dieses ungemein komplexe, sozio-technische Problem ›lösen‹ wird. Selbstverständlich sind Vorschläge wie die gezielte Verwendung von Eingabeaufforderungen, die standardmäßige Lieferung von Produkten mit der höchsten Sicherheits- und Privatsphäre-Einstellung oder die Fähigkeit von Benutzer*innen die Zugangsberechtigungen von verschiedenen IoT-Geräten zu überprüfen, willkommen. Diese technischen Ansätze werden jedoch niemals allen möglichen Missbrauch-Szenarien vorbeugen können. IoT-Entwickler*innen sind daher aufgefordert zu eruieren, welche pro- und reaktiven Maßnahmen eine Firma in Kraft setzen kann. Mögliche Optionen wären hierbei digitale Gewalt-Leitfäden für Mitarbeiter*innen, die im Kundendienst arbeiten und womöglich in Kontakt mit Betroffenen kommen (vgl. Communications Alliance Ltd. 2018). Ebenso sollten Unternehmen sich die Frage stellen, wie sie auf die mögliche gewaltbezogene Verwendung ihrer Systeme reagieren würden.

Legislative und politikzentrierte Interventionen

Zusätzlich zu den menschenbezogenen sozialen und technischen Interventionsoptionen müssen sowohl die Gesetzgebung als auch die Politik die potenziellen Risiken von IoT-unterstützter digitaler Gewalt berücksichtigen. Relevante Akteur*innen sind hierbei nicht nur die nationalen Regierungen, sondern auch Bundesländer, Gemeinden bis hin zu Wohnungsbaugesellschaften. Letztere werden in Zukunft IoT Technologien in geplante Bauten installieren.

All diese Institutionen sollten von dem sogenannten »Zuckerbrot und Peitsche« Zugang Gebrauch machen. Ersteres betrifft beispielsweise Anreize zur Erhöhung der Sicherheit von IoT Geräten durch freiwillige Programme oder Steuervorteile (vgl. Department for Digital, Culture, Media and Sport 2018: o.S.). Letzteres beschreibt strafbare Maßnahmen wie etwa die Durchsetzung verbindlicher Vorschriften und Strafen. Global haben die Regierungen auch damit begonnen, spezielle Einheiten einzurichten, die sich mit dem Thema der digitalen Sicherheit beschäftigen. Die *eSafety*-Kommission in Australien ist ein solches Beispiel. Das Büro leitet und koordiniert die Sicherheitsbemühungen zwischen Commonwealth-Abteilungen, Industrievertreter*innen und Behörden. eSafety hat auch die Befugnis Beschwerden von Einzelpersonen nachzugehen. Ihr Handlungsrahmen beinhaltet u.a. bildbasierte Vergehen wie ›Rache Pornos‹ (vgl. eSafety Commissioner 2020: o.S.). Die Kommission hat ebenfalls begonnen eine separate Frauensektion einzurichten, die sich mit der Sicherheit, Privatsphäre und den Bedürfnissen von Frauen online auseinandersetzt.

Erschwerend für politische Akteur*innen ist, dass es derzeit keine konsistente quantitative Erfassung von digitaler Gewalt gibt (vgl. Tanczer u.a. 2018b: 5). Dieser Mangel macht es schwierig, das volle Ausmaß und den Schweregrad des Problems einzuschätzen sowie evidenzbasierte Interventionen durchzuführen. Daten sind erforderlich, um den Umfang des Problems zu verstehen und potenzielle Veränderungen im Laufe der Zeit zu überwachen. Hierbei könnte es sehr hilfreich sein, wenn Betreuungsstellen, einschließlich Polizeikräften und Beratungsstellen im Kontext häuslicher Gewalt, ihre Berichterstattungsmuster beziehungsweise Dokumentation überdenken. Änderungen von Archivierungssystemen und Dokumentationsbemühungen müssen – um dem komplexen Thema gerecht zu werden – nicht nur die Anzahl, sondern die genauen Arten von Technologien, die im Kontext von digitaler Gewalt zum Einsatz kommen, vermerken. Diese Modifikation würde es nicht nur erlauben eine fundierte Basis digitaler Gewaltdaten zu generieren, sondern den Finger auf jene Firmen und IoT-Entwickler*innen zu richten, welche sich als primäre Plattformen für digitale Gewalt herausstellen. Eine nationale Analyse von digitaler Gewalt in der jährlichen »Crime Survey for England and Wales«, die vom Statistischen Bundesamt (ONS) oder Regulierungsbehörden wie dem Amt für Kommunikation (OFCOM) in Großbritannien durchgeführt werden würde, könnte helfen solche Informationen über die Jahre hinweg zusammenzustellen.

Zuletzt muss auch gewährleistet werden, dass sowohl das Internetrecht als auch das Gewaltschutzgesetz zukunftssicher gemacht werden. Dies ist vor allem in Hinblick auf das erwartete Wachstum an IoT-Geräten gekoppelt (vgl. Tanczer 2019a: o.S.). Eine Gesetzgebung wie zum Beispiel das bevorstehende »Online Harms White Paper« und »Online Safety Bill« in Großbritannien (vgl. HM Government 2019, 2020) muss die Risiken von digitaler Gewalt in der Partnerschaft durch smarte Systeme explizit adressieren. Alle politischen Entscheidungen, die diese aufkommende Bedrohung ignorieren, riskieren Schwachstellen, die in Anbetracht des langwierigen Gesetzgebungsprozesses schwer revidiert werden können. Kritiker*innen, die argumentieren, dass ein solcher Ansatz Innovation bremsen würde, bedenken nicht, dass neue Erfindungen auch in einer reflektierten, achtsamen Umgebung kreiert werden können. Ein Verweis zur Umsetzung der Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union ist hierbei hilfreich. Anstatt der Horrorszenarien, welche Konkurse und ein »Ende der Innovation« vorahnten, hat sich vielmehr gezeigt, dass die Wirtschaft sich nicht nur mit der Situation zurechtgefunden hat, sondern dass sogar Privatsphäre-garantierende Innovationen ermöglicht worden sind (vgl. Martin u.a. 2019). Eine ähnliche Sichtweise könnte für IoT-Produkte herangezogen werden. Zu bedenken gilt, dass Unternehmen seit fast über einem Jahrhundert generellen Gesundheits- und Hygienestandards unterliegen, so kann es doch nicht zu viel verlangt sein, ähnliche Sicherheitsstandards von IoT-Geräten zu erwarten.

Fazit

In diesem Kapitel wurden Informationen zu den Eigenschaften und möglichen Auswirkungen von IoT-Systemen in Zusammenhang mit häuslicher Gewalt diskutiert. Einsichten des britischen GIoT-Forschungsprojekts wurden besprochen und Interventionsmöglichkeiten für unterschiedliche Interessengruppen skizziert. Letztere umfassen eine Mischung aus sozialen, technischen und politischen Lösungsvorschlägen wie etwa die Notwendigkeit statistische Evaluierungen über dieses aufkommende Phänomen zu generieren. Im Allgemeinen drängen wir Akteur*innen, die sowohl in der Forschung als auch in der Praxis aktiv sind, dazu einen erweiterten Blickwinkel auf das Problem der digitalen Gewalt zu werfen. ›Konventionelle‹ Technologien wie Mobiltelefone und Laptops gehören zwar nach wie vor wahrscheinlich zu den prominenteren Geräten, durch die Gewalt in der Partnerschaft ausgeführt

wird. Nichtsdestotrotz kann der Anstieg an smarten Produkten nicht unkritisch gegenübergestanden werden. Ich hoffe daher hier Denkanstöße angeboten zu haben und einen ersten Einblick in die Zukunft von häuslicher Gewalt zu liefern. Interessierte Leser*innen, die sich gerne weiter mit diesem Thema beschäftigen wollen, sind herzlich dazu eingeladen sich für unseren monatlichen GIoT E-Mail-Newsletter auf der *UCL STEaPP* Webseite zu registrieren. Im Zuge dieses Rundbriefes werden neuste wissenschaftliche Veröffentlichungen, Strategien zur Unterstützung von Betroffenen sowie aktuelle politische und technische Geschehnisse geteilt.

Danksagung

Das GIoT Forschungsprojekt erhielt Fördergelder von UCLs Collaborative Social Science Domain, dem NEXTLEAP Projekt (688722), dem PETRAS IoT Forschungshub (EP/N02334X/1) und UCL Public Policy. GIoT läuft in Zusammenarbeit mit dem Londoner VAWG Consortium, Privacy International und dem PETRAS National Centre of Excellence for IoT Systems Cybersecurity. Die Autorin bedankt sich bei ihren GIoT Kollegin*innen Dr. Simon Parkin, Dr. Trupti Patel, Isabel Lopez Neira, Professor George Danezis und Julia Slupska für ihre stetige Unterstützung sowie allen Personen und Institutionen, die in den letzten drei Jahren mit dem GIoT Projekt aktiv zusammengearbeitet haben.

Literatur

Arief, Budi/Coopamootoo, Kovila/Emms, Martin/van Moorsel, Aad (2014): »Sensible Privacy: How We Can Protect Domestic Violence Survivors Without Facilitating Misuse«, in: Proceedings of the 13th Workshop on Privacy in the Electronic Society, WPES '14. New York, NY: ACM, S. 201-204.

Banerjee, Mandrita/Lee, Junghee/Raymond Choo, Kim-Kwang (2018): »A Blockchain Future for Internet of Things Security: A Position Paper«, in: Digital Communications and Networks, Vol. 4 Nr. 3, S. 149-160.

Brass, Irina/Tanczer, Leonie Maria/Carr, M./Elsden, M./Blackstock, J. (2018): »Standardising a Moving Target: The Development and Evolution of IoT Security Standards«, in: Living in the Internet of Things: Cybersecurity of the IoT – 2018. London: IET.

Burdon, Mark/Douglas, Heather (2017): »The Smart Home Could Worsen Domestic Abuse. But the Same Technology May Also Make Us Safer«. The Conversation. https://theconversation.com/the-smart-home-could-worsen-domestic-abuse-but-the-same-technology-may-also-make-us-safer-82897 [Zugriff: 3.7.2020].

Citron, Danielle/Franks, Mary Anne (2014): »Criminalizing Revenge Porn«, in: Wake Forest Law Review, Nr. 49, S. 345-391.

Communications Alliance Ltd. (Hg.) (2018): »G660:2018 Assisting Customers Experiencing Domestic and Family Violence Industry Guideline«. Sydney: Communications Alliance Ltd. https://commsalliance.com.au/__data/assets/pdf_file/0003/61527/Communications-Guideline-G660-Assisting-Customers-Experiencing-Domestic-and-Family-Violence.pdf [Zugriff: 3.7.2020].

DeNardis, Laura (2020): »Internet in Everything. Freedom and Security in a World with No Off Switch«. New Haven/London: Yale University Press.

DeNardis, Laura/Raymond, Mark (2017): »The Internet of Things as a Global Policy Frontier«, in: School of Law, Nr. 51, Davis: University of California, S. 475-497.

Department for Digital, Culture, Media and Sport (Hg.) (2018): »Code of Practice for Consumer IoT Security«. London: Department for Digital, Culture, Media & Sport. https://gov.uk/government/publications/code-of-practice-for-consumer-iot-security [Zugriff: 3.7.2020].

Douglas, Heather/Harris, Bridget/Dragiewicz, Molly (2019): »Technology-Facilitated Domestic and Family Violence: Women's Experiences«, in: The British Journal of Criminology, Vol. 59 Nr. 3, S. 551-570.

Dragiewicz, Molly/Burgess, Jean/Matamoros-Fernández, Ariadna/Salter, Michael/Suzor, Nicolas P./Woodlock, Delanie/Harris, Bridget (2018): »Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms«, in: Feminist Media Studies, Vol. 18 Nr. 4, S. 609-625.

Drive Partnership (2020): »A Domestic Abuse Perpetrator Strategy for England And Wales. Call to Action«. London: Drive Project (Hg.). https://driveproject.org.uk/wp-content/uploads/2020/01/Call-to-Action-Final.pdf [Zugriff: 3.7.2020].

Duerksen, Kari/Woodin, Erica (2019): »Technological Intimate Partner Violence: Exploring Technology-Related Perpetration Factors and Overlap with in-Person Intimate Partner Violence«, in: Computers in Human Behavior, Nr. 98, S. 223-231.

Eaton, Asia/Noori, Sofia/Bonomi, Amy/Stephens, Dionne/Gillum, Tameka (2020): »Nonconsensual Porn as a Form of Intimate Partner Violence. Using the Power and Control Wheel to Understand Nonconsensual Porn Perpetration in Intimate Relationships«, in: Trauma, Violence, & Abuse, Vol 20. Nr. 10, S. 1-15. https://doi:10.1177/1524838020906533

eSafety Commissioner (2020): »Our Legislative Functions«. Australian Government (Hg.). https://esafety.gov.au/about-us/who-we-are/our-legislative-functions [Zugriff: 30.3.2020].

Gámez-Guadix, Manuel/Borrajo, Erika/Calvete, Esther (2018): »Partner Abuse, Control and Violence Through Internet and Smartphones: Characteristics, Evaluation and Prevention«, in: Papeles Del Psicólogo – Psychologist Papers, Vol. 39 Nr. 3, S. 218-227.

Harkin, Diarmaid/Molnar, Adam/Vowles, Erica (2020): »The Commodification of Mobile Phone Surveillance: An Analysis of the Consumer Spyware Industry«, in: Crime, Media, Culture, Vol. 16 Nr. 1, S. 33-60.

Harris, Bridget (2019): »Anti-Rape Devices May Have Their Uses, but They Don't Address the Ultimate Problem«. The Conversation (Hg.). https://theconversation.com/anti-rape-devices-may-have-their-uses-but-they-dont-address-the-ultimate-problem-123011 [Zugriff: 30.3.2020].

Harris, Bridget/Woodlock, Delanie (2018): »Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies«, in: The British Journal of Criminology, Vol. 59 Nr. 3, S. 530-550.

Havron, Sam/Freed, Diana/Chatterjee, Rahul/McCoy, Damon/Dell, Nicola/Ristenpart, Thomas (2019): »Clinical Computer Security for Victims of Intimate Partner Violence«, in: 28th USENIX Security Symposium. Santa Clara, CA, S. 105-122.

Henry, Nicola/Powell, Anastasia (2018): »Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research«, in: Trauma, Violence, & Abuse, Vol. 19 Nr. 2, S. 195-208.

Hester, Marianne/Eisenstadt, Nathan/Ortega-Avila, Ana/Morgan, Karen/Walker, Sarah-Jane/Bell, Juliet (2019): »Evaluation of the Drive Project – A Three-Year Pilot to Address High-Risk, High-Harm Perpetrators of Domestic Abuse«. Bristol: University of Bristol. https://driveproject.org.uk/wp-content/uploads/2020/01/Drive-Evaluation-Report-Executive-Summary-Final.pdf [Zugriff: 3.7.2020].

HM Government (Hg.) (2019): »Online Harms White Paper«. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf [Zugriff: 3.7.2020].

IHS Markit (Hg.) (2017): »The Internet of Things: A Movement, Not a Market«. Englewood, Colorado: IHS Markit. https://cdn.ihs.com/www/pdf/IoT_ebook.pdf [Zugriff: 3.7.2020].

Leitão, Roxanne (2019): »Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse«, in: ACM Conference on Designing Interactive Systems, S. 527-539. https://doi:10.1145/3322276.3322366

Lopez-Neira, Isabel/Patel, Trupti/Parkin, Simon/Danezis, George/Tanczer, Leonie Maria (2019): »Internet of Things: How Abuse Is Getting Smarter«, in: Safe – The Domestic Abuse Quarterly, Vol. 63, S. 22-26.

Martin, Nicholas/Matt, Christian/Niebel, Crispin/Blind, Knut (2019): »How Data Protection Regulation Affects Startup Innovation«, in: Information Systems Frontiers, Vol. 21 Nr. 6, S. 1307-1324.

Mattern, Friedemann/Floerkemeier, Christian (2010): »From the Internet of Computers to the Internet of Things«, in: Sachs, Kai/Petrov Ilia/Guerrero, Pablo (Hg.), From Active Data Management to Event-Based Systems and More, Lecture Notes in Computer Science, Berlin/Heidelberg: Springer, S. 242-259.

Matthews, Tara/O'Leary, Kathleen/Turner, Anna/Sleeper, Manya/Palzkill Woelfer, Jill/Shelton, Martin/Manthorne, Cori/Churchill, Elizabeth F./Consolvo, Sunny (2017a): »Security and Privacy Experiences and Practices of Survivors of Intimate Partner Abuse«, in: IEEE Security Privacy, Vol. 15 Nr. 5, S. 76-81.

Matthews, Tara/O'Leary, Kathleen/Turner, Anna/Sleeper, Manya/Palzkill Woelfer, Jill/Shelton, Martin/Manthorne, Cori/Churchill, Elizabeth/Consolvo, Sunny (2017b): »Stories from Survivors: Privacy & Security Practices When Coping with Intimate Partner Abuse«, in: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17. New York, NY, S. 2189-2201.

McCarthy, Katharine/Mehta, Ruchi/Haberland, Nicole (2018): »Gender, Power, and Violence: A Systematic Review of Measures and Their Association with Male Perpetration of IPV«, in: PLoS One, Vol. 13 Nr. 11, o.S. https://doi:10.1371/journal.pone.0207091

McGlynn, Clare/Rackley, Erika/Houghton, Ruth (2017): »Beyond ›Revenge Porn‹: The Continuum of Image-Based Sexual Abuse«, in: Feminist Legal Studies, Vol. 25 Nr. 1, S. 25-46.

Mirian, Ariana (2019): »Hack for Hire«, in: Communications of the ACM, Vol. 62 Nr. 12, S. 32-37.

Muir, Kate/Joinson, Adam (2020): »An Exploratory Study Into the Negotiation of Cyber-Security Within the Family Home«, in: Frontiers in Psychology, Vol. 11 Nr. 424, S. 1-14.

Muncaster, Laura/Ohlsson, Ioan (2019): »Sexting: Predictive and Protective Factors for Its Perpetration and Victimisation«, in: Journal of Sexual Aggression, S. 1-13. https://doi:10.1080/13552600.2019.1645220

O'Malley, Roberta Liggett/Holt, Karen (2020): Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime. Journal of Interpersonal Violence, S. 1-26. https://doi:10.1177/0886260520909186

Parkin, Simon/Patel, Trupti/Lopez-Neira, Isabel/Tanczer, Leonie Maria (2019): »Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-Facilitated Tech-Abuse«, in: Proceedings of the New Security Paradigms Workshop, NSPW '19. San Carlos, Costa Rica: Association for Computing Machinery, S. 1-15.

Powell, Anastasia/Henry, Nicola (2018): »Policing Technology-Facilitated Sexual Violence against Adult Victims: Police and Service Sector Perspectives«, in: Policing and Society, Vol. 28 Nr. 3, S. 291-307.

Refuge (Hg.) (2020a): »72 % of Refuge Service Users Identify Experiencing Tech Abuse«. https://refuge.org.uk/72-of-refuge-service-users-identify-experiencing-tech-abuse/ [Zugriff: 1.3.2020].

Refuge (Hg.) (2020b): »Tech Abuse and Empowerment Service«. https://refuge.org.uk/our-work/our-services/tech-abuse-empowerment-service/ [Zugriff: 29.3.2020].

Reyns, Bradford W. (2019): »Online Pursuit in the Twilight Zone: Cyberstalking Perpetration by College Students«, in: Victims & Offenders, Vol. 14 Nr. 2, S. 183-198.

Rising Sun (Hg.) (2020): »One Stop Shops«. https://risingsunkent.com/services/one-stop-shops/ [Zugriff: 29.3.2020].

Schneier, Bruce (2017): »The Internet of Things Will Upend Our Industry«, in: IEEE Security Privacy, Vol. 15 Nr. 2, S. 108-11s8.

Slupska, Julia (2019): »Safe at Home: Towards a Feminist Critique of Cybersecurity«, in: St Antony's International Review, Nr. 15, S. 83-100.

Slupska, Julia/Tanczer, Leonie Maria (im Erscheinen): »Intimate Partner Violence (IPV) Threat Modeling: Tech Abuse as Cybersecurity Challenge in the Internet of Things (IoT)«, in: Bailey, J./Flynn, A./Henry, N. (Hg.), Handbook on Technology-Facilitated Violence and Abuse: International Perspectives and Experiences, Bingley: Emerald Publishing.

Snook/Chayn/SafeLives (2017): »Tech vs Abuse: Research Findings 2017«. London: Comic Relief (Hg.). https://safelives.org.uk/sites/default/files/resources/Tech%20vs%20abuse%20report.pdf [Zugriff: 3.7.2020].

Strengers, Yolande/Kennedy, Jenny/Arcari, Paula/Nicholls, Larissa/Gregg, Melissa (2019): »Protection, Productivity and Pleasure in the Smart Home: Emerging Expectations and Gendered Insights from Australian Early Adopters«, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI '19, New York, NY: ACM, S. 645:1-645:13.

Sweet, Paige (2019): »The Sociology of Gaslighting«, in: American Sociological Review, Vol. 84 Nr. 5, S. 851-875.

Tanczer, Leonie Maria (2018a): »Tackling Tech Risks for Domestic Violence and Abuse«. https://medium.com/policy-postings/tackling-tech-risks-for-domestic-violence-and-abuse-581a07b41020 [Zugriff: 24.6.2020].

Tanczer, Leonie Maria/Lopez-Neira, Isabel/Parkin, Simon/Patel, Trupti/Danezis, George (2018b): »Gender and IoT (G-IoT) Research Report: The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse«. London: University College London.

Tanczer, Leonie Maria/Lopez-Neira, Isabel/Patel, Trupti/Parkin, Simon/Danezis, George (2018c): »Gender and IoT (G-IoT) Policy Leaflet: Tech Abuse – Smart, Internet-Connected Devices Present New Risks for Victims of Domestic Violence & Abuse«. London: University College London.

Tanczer, Leonie Maria/Patel, Trupti/Parkin, Simon/Danezis, George (2018d): »Gender and IoT (G-IoT) Tech Abuse Guide: How Internet-Connected Devices Can Affect Victims of Gender-Based Domestic and Sexual Violence and Abuse«. London: University College London.

Tanczer, Leonie Maria/Steenmans, I./Elsden, M./Blackstock, J./Carr, M. (2018e): »Emerging Risks in the IoT Ecosystem: Who's Afraid of the Big Bad Smart Fridge?«, in: Living in the Internet of Things: Cybersecurity of the IoT – 2018, London: IET.

Tanczer, Leonie Maria (2019a): »The Government Published Its Draft Domestic Abuse Bill, but Risks Ignoring the Growing Threat of Tech Abuse«. https://medium.com/policy-postings/the-government-published-its-draft-domestic-abuse-bill-but-risks-ignoring-the-growing-threat-of-368a6fb70a14 [Zugriff: 27.2.2020].

Tanczer, Leonie Maria/Brass, Irina/Elsden, Miles/Carr, Madeline/Blackstock, Jason (2019b): »The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape«, in: Ellis, Ryan/Mohan, Vivek (Hg.), Rewired: Cybersecurity Governance, Hoboken, New Jersey: Wiley, S. 37-56.

Tanczer, Leonie Maria/Patel, Trupti/Parkin, Simon/Danezis, George (2019c): »Gender and IoT (G-IoT) Resource List: How Internet-Connected Devices Can Affect Victims of Gender-Based Domestic and Sexual Violence and Abuse«. London: University College London.

Taylor, P./Allpress, S./Carr, Madeline/Lupu Emil/Norton, J./Smith, L./Blackstock, Jason/Boyes Hugh/Hudson-Smith, A./Brass, Irina/Chizari, H./Cooper, R./Coulton, Paul/Craggs, B./Davies, N./De Roure, David/Elsden, Miles/Huth, M./Lindley, Joseph/Maple, Carsten/Mittelstadt, Brent/Nicolescu, Razvan/Nurse, Jason/Procter, Rob/Radanliev, Petar/Rashid, A./Sgandurra, D./Skatova, A./Mariarosaria, Taddeo/Tanczer, Leonie Maria/Vieira-Steiner, R./Watson, Jeremy/Wachter, Sandra/Wakenshaw, Susan Y. L./Carvalho, Graca/Thompson, Rob/Westbury, P. (2018): »Internet of Things: Realising the Potential of a Trusted Smart World«. London: Royal Academy of Engineering (Hg.).

Think Social Tech/Snook/SafeLives (2019): »Tech vs Abuse: Research Findings 2019«, in: Comic Relief, The Clothworkers' Foundation and Esmée Fairbairn Foundation (Hg.). https://d1c4e1f2-14ed-423b-8bab-01c0ad397d8f.filesusr.com/ugd/464d6d_b465be597dee4e04b8fac09363e4ef62.pdf [Zugriff 6.7.2020].

Woodlock, Delanie (2017): »The Abuse of Technology in Domestic Violence and Stalking«, in: Violence Against Women, Vol. 23 Nr. 5, S. 584-602.