Ergebnisbericht „Technische Anlaufstelle für Betroffene von digitaler Gewalt in Partnerschaften“

Dialog für Cybersicherheit

Stand: November 2024

Informationen

Dieser Bericht wurde im Rahmen des „Dialogs für Cybersicherheit“ von Dezember 2023 bis November 2024 erarbeitet.
Initiatorinnen des Workstreams waren Dr. Katharina Witterhold (Bundesamt für Sicherheit in der Informationstechnik) und Celine Sturm (stellvertretend für den WEISSEN RING).

Mitwirkende Teilnehmende des Workstreams waren: Dr. Ina Bieber (Bundeskriminalamt), Kerstin Demuth (Bundesverband Frauenberatungsstellen und Frauennotrufe), Svenja Drews (WEISSER RING), Fatma Geisler (thefuturepast), Stephanie Hartmann (Bundesamt für Sicherheit in der Informationstechnik), Johanna Herz (WEISSER RING), Petra Hoffmann (Bundesamt für Sicherheit in der Informationstechnik), Ophélie Ivombo (Frauenhauskoordinierung), Nora Kluger (Bundesamt für Sicherheit in der Informationstechnik), Bettina Kloppig (Bundesarbeitsgemeinschaft der Seniorenorganisationen), Klaus Landefeld (eco e.V.), Nadja Menz (Fraunhofer-Institut für Offene Kommunikationssysteme FOKUS), Dr. Ayten Öksüz (Verbraucherzentrale Nordrhein-Westfalen e.V.), Inga Pöting („Ein Team gegen digitale Gewalt“), Anne Roth, Prof. Dr. Leonie Tanzcer (University College London) und Dr. Katharina Witterhold (Bundesamt für Sicherheit in der Informationstechnik).

Der Dialog für Cybersicherheit ist eine Maßnahme des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Das BSI hat dazu eine Geschäftsstelle eingerichtet.
Der Workstream „Technische Anlaufstelle für Betroffene von digitaler Gewalt in Partnerschaften“, aus dessen Arbeit dieser Bericht entstanden ist, wurde im Rahmen eines partizipativen und offenen Austauschs von der Geschäftsstelle und den Dialogpartnerinnen durchgeführt. BSI und das „Komitee des Dialogs für Cybersicherheit“ haben das Thema für den Workstream ausgewählt.
Der vorliegende Bericht wurde von den Workstream-Teilnehmer*innen eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. einzelner Teilnehmenden wider. Das BSI verfolgt mit dem Dialog für Cybersicherheit das Ziel, einen offenen gesellschaftlichen Diskurs zum Thema Cybersicherheit sowie damit verwandter gesellschaftlicher Themen zu ermöglichen. Die Maßnahme soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung an das Thema Cybersicherheit aus Sicht der Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Weitere Informationen zum „Dialog für Cybersicherheit“:
www.dialog-cybersicherheit.de
Kontakt Geschäftsstelle: projekt-digitalegesellschaft@bsi.bund.de
Stand: November 2024
Lizenz: Dieser Bericht steht unter der Lizenz Creative Commons CC-BY-SA-Lizenz 4.0 International

Zusammenfassung

Gewalt im sozialen Nahraum stellt ein drängendes gesellschaftliches Problem dar. Die Hellfeldzahlen zu Partnerschaftsgewalt steigen konstant an[1]. Sie geht oft mit Kontrolle und Manipulation der Betroffenen durch die Täter[2] einher. Die Digitalisierung erleichtert ihnen dies auf zahlreichen Wegen: u.a. durch Standortverfolgung, dem Mitlesen von E-Mails oder Social-Media-Nachrichten, heimlich oder offen installierten Bild- und Tonaufnahmegeräten werden die Gewaltanwendungen im sozialen Nahraum durch die Digitalisierung erweitert. Digitale Gewalt umfasst „Gewalthandlungen, die sich technischer Hilfsmittel und digitaler Medien (Handy, Apps, Internetanwendungen, Mails etc.) bedienen und Gewalt, die im digitalen Raum, z.B. auf Online-Portalen oder sozialen Plattformen stattfindet“[3]. Dass digitale Partnerschaftsgewalt eine Fortsetzung von analogen Gewaltverhältnissen ist, wird deutlich, wenn berücksichtigt wird, dass beispielsweise die Herausgabe von Login-Daten unter Zwang erfolgt oder aus Tätersicht unangemessene Online-Kommunikation der (Ex-)Partnerin mit der Androhung oder Ausübung physischer Gewalt bestraft wird.

Die Einrichtungen des Hilfesystems mit Beratungsstellen, Notrufen, Opferbegleitung und Frauenhäusern, die den Betroffenen – in gut 80 % der Fälle sind dies Frauen[4] – in diesen nicht nur belastenden, sondern mitunter auch gefährlichen Lebenssituationen zur Seite stehen, stellen die Ausweitung der Gewalt auf den digitalen Raum bereits seit Längerem fest. Doch sind die Berater*innen nur unzureichend darauf vorbereitet, Betroffenen auch in technischen Fragen, wie zum Beispiel der Accountwiederherstellung, der sicheren Einrichtung von Routern, dem Aufspüren von Spyware oder gar der IT-Forensik, adäquat zur Seite zu stehen. Es fehlt nicht nur an finanziellen Mitteln, hier umfassende Schulungen flächendeckend für das

[1] https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/HaeuslicheGewalt/haeuslicheGewalt_node.html für den Zeitraum 2019-2023 ; https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/HaeuslicheGewalt/haeuslicheGewalt_node.html für den Zeitraum 2019-2023; https://de.statista.com/statistik/daten/studie/1121554/umfrage/weibliche-opfer-von-gewalt-in-der-partnerschaft-in-deutschland/ für den Zeitraum 2013-2023. Hinzuweisen ist darauf, dass Hellfeldzahlen auch vom Anzeigeverhalten der Bürgerinnen und Bürger abhängig sind. Bei Partnerschaftsgewalt wird von einer hohen Dunkelfeldziffer ausgegangen. Dabei ist es auch möglich, dass in den letzten Jahren eine Verschiebung vom Dunkelfeld stattgefunden hat und entsprechende Delikte häufiger polizeilich bekannt werden.

[2] Bei digitaler Gewalt handelt es sich um eine Form geschlechtsspezifischer Gewalt bei der die Mehrzahl der Betroffenen Frauen und die Mehrzahl der Täter Männer sind. Entsprechend wird bei dem Begriff „Täter“ die männliche Schreibweise verwendet. Bei den Betroffenen wird, schon alleine aufgrund der häufig mitbetroffenen Kinder, wo möglich, eine neutrale Formulierung verwendet.

[3] https://www.frauen-gegen-gewalt.de/de/aktionen-themen/bff-aktiv-gegen-digitale-gewalt.html

[4] In 2023 wurde erneut ein Anstieg der Partnerschaftsgewalt um 6,5 % festgestellt. 79,2 % der Betroffenen sind Frauen. https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2024/Presse2024/240607_PM_BLB_Haeusliche_Gewalt.html 13.09.2024.

Unterstützungsnetzwerk anzubieten, sondern auch an Kapazitäten, intensive fachspezifische Weiterbildungen überhaupt in den Beratungsalltag zu integrieren[5]. Die im Rahmen des Workstreams durchgeführte Bedarfsanalyse unter den institutionellen Bedarfsträgern zeigt:

1) Häufigkeit digitaler Gewalt: 77,1% der befragten Beratenden sprechen häufig mit Ratsuchenden über digitale Gewalt. Die häufigsten Formen sind unerwünschte Kontaktaufnahme (87,6%) sowie digitale Diffamierung (56,6%) und bildbasierte sexualisierte Gewalt (44,7%). Der Missbrauch von Smart-Home-Technologien wird seltener thematisiert (12,5%).

2) Digitalkompetenz: Täter nutzen soziale Medien, Messenger und Shoppingdienste häufig, um zu stalken oder zu diffamieren. Grundlegende Digitalkompetenz zum Schutz bei digitaler Gewalt ist deshalb das Ändern von Einstellungen in Apps und Accounts von Online-Diensten, bei dem ein Drittel der Befragten (29%) angaben, dass sie sich sehr sicher fühlen. Eine weitere Schutzmaßnahme kann das Melden von Beiträgen in Sozialen Medien darstellen, dabei gaben 40% der Befragten an, dass sie sich sehr sicher fühlen.

3) Beweissicherung: Für das Einleiten rechtlicher Schritte ist die Beweissicherung zentral. Lediglich ein Fünftel der Beratenden schätzt sich als sehr sicher ein, diese bei digitaler Gewalt durchführen zu können. Die Beweissicherung ist zudem Aufgabe der Polizei. Jedoch gaben nur ein Fünftel der Beratenden an, dass sie für die Beweissicherung an andere verweisen. Dies wäre jedoch wichtig, da je nach Gewaltform und Straftat, auch IT-forensische Beweissicherung erforderlich sein können und einfache Screenshots nicht ausreichen.

4) Technische Expertise: Beratende des Hilfesystems verfügen über psychosoziale Expertise. Es mangelt häufig an Kapazität, um sich das nötige technische Wissen anzueignen und auf dem aktuellen Stand zu halten, insbesondere bei komplexen Themen wie dem Auffinden von Spyware auf bspw. mobilen Endgeräten oder der sicheren Einrichtung von Routern und Smart-Home-Geräten. Des Weiteren liegt vertiefte IT-Expertise außerhalb ihrer fachlichen Zuständigkeit.

5) Bedarf an Unterstützung: Fast alle Befragten (96,7%) wünschen sich konkrete Hilfestellungen und Unterstützungsmöglichkeiten im Umgang mit digitaler Gewalt. Besonders gefragt

---

[5] Tanczer, L., López-Neira, I., & Parkin, S. (2021). 'I Feel Like We' Re Really Behind the Game': Perspectives of the United Kingdom's Intimate Partner Violence Support Sector on the Rise of Technology-Facilitated Abuse. Journal of Gender-Based Violence, 5(3), 431–450. https://bristoluniversitypressdigital.com/view/journals/jgbv/5/3/article-p431.xml

sind Schulungen, Ansprechpartner*innen mit technischer Expertise und Unterstützung bei der Beweissicherung.

6) Bevorzugte Formen der Unterstützung: Beratende bevorzugen für die eigene Unterstützung durch eine technische Anlaufstelle die Beratung via Telefon, Video oder persönlich vor Ort. Bei Unterstützungsleistungen und der Beratung von Betroffenen, wird die Beratung per Video am häufigsten als sinnvolle Variante benannt, gefolgt von der Beratung per Telefon oder vor Ort. Eine Beratung per E-Mail wird für Betroffene als weniger sinnvoll benannt. In manchen ländlichen Gebieten kann mangelhafte Internetverbindung eine Herausforderung sein, weshalb die Beratung per Video erschwert werden könnte. In anderen ländlichen Regionen wird die Möglichkeit zur Vor-Ort-Beratung als Herausforderung gesehen, da die Anreisewege sehr lang sind, sodass schnelle Hilfe fast kaum möglich ist.

Diese Ergebnisse zeigen den hohen Bedarf an technischer Unterstützung und Schulungen sowie die Herausforderungen in der Beratung von Betroffenen digitaler Gewalt. Für das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Befassung mit digitaler Gewalt ebenfalls neues Terrain. Seit 2021 hat das BSI die Aufgabe, auch Verbraucher*innen vor Gefahren zu schützen, die mit fehlender oder unzureichender IT-Sicherheit verknüpft sind. Dies betrifft insbesondere die Verletzung der Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Aus dieser Aufzählung wird ersichtlich, dass das BSI nicht für alle unter den Begriff der digitalen Gewalt fallenden Angriffe zuständig ist. Beispielsweise sind einschüchternde Nachrichten oder diffamierende Social-Media-Posts nicht mit fehlenden oder unzureichenden Maßnahmen der IT-Sicherheit verbunden. Die Schnittstelle ist jedoch gerade im Bereich der Partnerschaftsgewalt bzw. der digitalen Gewalt im sozialen Nahraum sehr hoch.

Die Auseinandersetzung mit diesem, im Bereich der IT-Sicherheit, bisher kaum wahrgenommenen Phänomen zeigt, dass das bislang im Bereich des digitalen Verbraucherschutzes vorherrschende Modell vom weit entfernten Angreifer mit finanziellen Interessen alleine nicht ausreicht. Auch in der IT-Sicherheit muss von der Annahme ausgegangen werden, dass Verbraucher*innen nicht immer in ausschließlich wohlmeinenden Beziehungen, Familien und Wohngemeinschaften usw. ihre IT nutzen. Daraus folgt eine ganze Reihe von Überlegungen, die für die weitere Ausgestaltung des digitalen Verbraucherschutzes von Bedeutung sind. Insbesondere gilt es, den Hinweis auf die Notwendigkeit der Implementierung nicht-missbräuchlichen Designs künftig in den Dialog mit Wirtschaft und Wissenschaft einzubringen und bei der Entwicklung von Standards für IT von Privathaushalten zu berücksichtigen.

Vor diesem Hintergrund war es das Ziel des Workstreams, ein umsetzbares Konzept für eine technische Anlaufstelle zu entwickeln, die

a) Betroffene von digitaler Gewalt so unterstützt, dass sie ihre informationelle Selbstbestimmung zurückgewinnen, ohne dabei Schaden zu nehmen und
b) Berater*innen den Aufbau grundlegender Kenntnisse im technischen Bereich durch die Entwicklung einer Beratungs-, Informations- und Vernetzungsstruktur ermöglicht, um digitale Aspekte von Gewaltphänomenen erkennen und Betroffene effektiv unterstützen zu können.
c) Betroffenen gleichzeitig Ansprechpartner*innen für weiterführende Fragen zur Verfügung stellt.
d) Berater*innen mit der erforderlichen technischen Expertise unterstützt, wenn diese außerhalb deren genuinen Aufgabenbereichs liegt. Das umfasst auch praktische Unterstützung, wie etwa forensische Untersuchungen von Geräten der Betroffenen sowie auch der Berater*innen und ihrer Institutionen.

In einem Workshop wurden zwei Modelle entwickelt – eines aus Sicht der Beratungsorganisationen und eines aus Sicht der Betroffenen und Ratsuchenden**.** Das Modell für Beratungsorganisationen sieht technische Anlaufstellen vor, die Beratende mit technischer Expertise unterstützen. Bei komplexen Fällen ist z.B. zur Schadensbegrenzung oder Spurensicherung eine Vor-Ort-Beratung vorgesehen. Die Aufgaben der technischen Anlaufstellen umfassen organisatorische und inhaltliche Koordination, das Bereitstellen von Informationsmaterial und Weiterbildungen, Fallberatung per Telefon oder Video und Wissensaustausch. Ein langfristiger Wissensaustausch und die Systematisierung von Fällen sollen aktuelle Einblicke in digitale Gewalt (z.B. zu neuen Angriffsvektoren) ermöglichen.

Demgegenüber ist das Modell für Betroffene dezentral organisiert, um einen barrierearmen Zugang sicherzustellen (d.h. Kontakt über E-Mail, Telefon, persönliche Vorsprache). Der Fokus liegt auf der Überprüfung kompromittierter Geräte bzw. dem Auffinden der Ursache des Problems (z.B. bei versteckten Geräten zum Abhören), forensischen Untersuchungen, Beweissicherung und einem Leihgerätebestand für Betroffene. Ein aufsuchender Service ist vorgesehen, wenn Geräte nicht transportiert werden können oder Betroffene die Ursache des Problems nicht selbst identifizieren können. Technisches Personal soll speziell geschult und angeleitet werden (u.a. durch Bereitstellung eines Führungszeugnisses und mit Schulungen zu geschlechtsspezifischer Gewalt, Trauma und IT-Forensik). Ein weiterer Baustein ist die Qualitätssicherung: Regelmäßige Evaluationen, Feedback der Betroffenen und Supervision für das technische Personal sollen die Beratungsqualität sichern. Für Konfliktfälle und eine gründliche Ersteinschätzung wird der technischen Beratung eine Clearing-Stelle angegliedert.

Langfristig sollen anonyme, technische Vorfallsdaten zu Angriffen in der digitalen Gewalt gesammelt werden, um die Verbreitung und Häufigkeit von Angriffsvektoren sowie deren technische Weiterentwicklung zu dokumentieren. Dies soll präventive und regulatorische Maßnahmen, effizientes Erkennen von Sicherheitsvorfällen sowie eine angemessene Reaktion darauf ermöglichen.

Beide Modelle sind komplementär und damit Teile desselben Konzepts. Die Koordinierungsstelle des ersten Modells könnte darüber hinaus auch Aufgaben wie die Konzeption von Anamnesebögen, Clearing-Stellen sowie Supervision übernehmen, während die dezentrale Struktur des zweiten Modells schnelle Unterstützung für Betroffene sichert.

Inhalt

1. Einleitung

Digitale Gewalt fungiert als Sammelbegriff für eine Reihe von sehr unterschiedlichen Gewaltformen. Darunter werden u.a. Cyberstalking, bildbasierte sexualisierte Gewalt, heimliche Aufnahmen, unerlaubtes Lokalisieren mit Trackern und auch Hate Speech subsumiert. Im Folgenden geht es konkret um digitale Gewalt im sozialen Nahraum. Kennzeichen dieser Form digitaler Gewalt ist, dass der Täter die betroffene Person kennt und damit unter Umständen über Informationen verfügt, die ein weit entfernter, anonymer Angreifer nicht hat, und mitunter auch physischen Zugriff auf die Person und ihre IT-Geräte besitzt. Ziel der im Regelfall wiederholten und andauernden Angriffe ist es, Macht und Kontrolle über das Verhalten der Betroffenen zu erlangen. Die Bandbreite möglicher Gewaltausübung ist lang: Missbrauch der E-Mail-Konten-Daten, um beispielsweise dem Arbeitgeber der Betroffenen in deren Namen zu kündigen, Lokalisieren der Betroffenen mit Hilfe eines versteckten Standort-Trackers, Erpressung mit intimen Fotos, Abbuchungen vom Online-Konto durch Umgehen des zweiten Faktors (was besonders einfach ist, wenn der Angreifer der Inhaber der von der Betroffenen verwendeten SIM-Karte ist) oder Unterkühlung des Zuhauses der Betroffenen, wenn Zugang zu deren smartem Heizkörperthermostat besteht.

1.1 Digitalisierung von Gewalt

Für Beratungsorganisationen, die ihre Expertise für gewöhnlich in den Bereichen psychosozialer und rechtlicher Beratung haben, sind diese neuen Gewaltformen schwer in ihre Beratungspraxis zu integrieren. Betroffene wissen häufig nicht, auf welche Art der (Ex-)Partner Informationen darüber erlangt hat, wo sie sich gerade aufhalten oder mit wem sie Kontakt haben.

Besonders schwierig für die Betroffenen ist die Situation, wenn die Gefahr besteht, dass ihr Smartphone kompromittiert ist und überwacht wird. Dann ist es kaum möglich, überhaupt nach Hilfe zu suchen, ohne dass der Täter es mitbekommt. Betroffene können nur schwer einschätzen und kontrollieren, wann der Täter Zugriff auf sensible Informationen bekommt oder entsprechende Handlungen im Namen der Betroffen ausführen könnte. Auch das Entfernen von so genannter Spyware sowie von niedrigschwelligen Formen der Überwachung, wie etwa Lokalisierung via „Familienfunktion“, kann für die Betroffenen zu physischer Gewalt durch den Täter führen. Digitale und analoge Gewalt trennt hier lediglich die Begriffsanalytik. Dies zeigt, dass eine nur auf technische Wiederherstellung der informationellen Selbstbestimmung abzielende Unterstützung zu kurz greift. Digitale Gewalt im sozialen Nahraum ist eingebettet in ein komplexes psychosoziales Gefüge und lässt sich davon nicht isoliert betrachten, ohne Betroffene potentiell zu schädigen.

War die Einrichtung technischer Geräte im Haushalt Aufgabe des Partners, ist die Angriffsfläche groß. Häufig ist vielen Nutzer*innen auch gar nicht bewusst, welche Daten bei der

Nutzung des Routers oder digital vernetzter Smart Home Geräte, wie beispielsweise smarte Saugwischern oder Türklingeln, gesammelt und damit potentiell von anderen ausgenutzt werden können – auch nach einer Trennung. Mitarbeitende von Beratungsorganisationen müssen zusätzlich zu ihren bisherigen Aufgaben auch im Bereich der technischen Beratung qualifiziert werden, um dieser Herausforderung adäquat begegnen zu können[6].

In der Öffentlichkeit ist das Problembewusstsein zu digitaler Gewalt im sozialen Nahraum noch gering ausgeprägt. Dies hat verschiedene Ursachen. Zum einen wird digitale Gewalt im öffentlichen Diskurs oft gleichgesetzt mit Hass und Hetze im Netz. Da hiervon unter anderem auch Personen betroffen sind, die über einen hohen Bekanntheitsgrad verfügen (z.B. Prominente und Politiker*innen), wird ihre Betroffenheit entsprechend stark wahrgenommen. Dazu trägt auch eine fehlende, etablierte Definition des Begriffes „digitale Gewalt“ bei[7].

Zum anderen gibt es zur Betroffenheit von digitaler Gewalt im sozialen Nahraum in Deutschland bisher wenige Daten und Studien. Die Polizeiliche Kriminalstatistik (PKS) kann erste, grundlegende Informationen zum sogenannten Hellfeld liefern. Einschränkend muss jedoch darauf hingewiesen werden, dass nur die polizeilich bekannt gewordenen Straftaten in der PKS erfasst werden, bei denen als Tatmittel das „Internet“ erfasst wurde. Es genügt folglich nicht, dass ein digitaler Anschluss verwendet wurde[8]. Zudem sind die Hellfeldzahlen abhängig vom Anzeigeverhalten der Bürgerinnen und Bürger. Das Lagebild Häusliche Gewalt 2023 wertet die Delikte *Bedrohung, Stalking und Nötigung* in (Ex-)Partnerschaften hinsichtlich der Verwendung des „Tatmittel Internet“ aus. Für 2023 können steigende Anteile an Fällen mit „Tatmittel Internet“ festgestellt werden: In 7,3 % der Fälle der erfassten Nötigungen wurde 2023 das Tatmittel Internet genutzt (2022: 5,9%). Ähnlich verhält es sich bei Bedrohung (2023: 8,7%; 2022: 7,8%). Deutliche höhere Anteile sind bei der Nachstellung (Stalking) zu beobachten (2023: 16,4%; 2022: 13,5%). Jedoch muss von einer deutlich höheren Dunkelziffer ausgegangen werden, da Taten von Partnerschaftsgewalt deutlich seltener angezeigt werden als

---

[6] Tanczer, L. (2021). Das Internet der Dinge: Die Auswirkung "Smarter" Geräte auf Häusliche Gewalt. In bff: Bundesverband Frauenberatungsstellen und Frauennotruf & N. Prasad (Eds.), Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung: Formen und Interventionsstrategien. (pp. 205-225). Berlin: Transcript Verlag. https://www.transcript-verlag.de/shopMedia/openaccess/pdf/oa9783839452813.pdf

[7] https://netzpolitik.org/2024/stalking-doxing-nacktfotos-was-ist-digitale-gewalt/

[8] „Erfasst werden grundsätzlich alle Delikte, zu deren Tatbestandsverwirklichung das Medium Internet als Tatmittel verwendet wird – die Verwendung eines PC/Notebooks pp. allein reicht nicht aus. Hier kommen sowohl Straftaten in Betracht, bei denen das bloße Einstellen von Informationen in das Internet bereits Tatbestände erfüllen (sog. Äußerungs- bzw. Verbreitungsdelikte) als auch solche Delikte, bei denen das Internet als Kommunikationsmedium bei der Tatbestandsverwirklichung eingesetzt wird.“ (BKA (2024): Häusliche Gewalt. Bundeslagebild 2023, https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/HaeuslicheGewalt/HaeuslicheGewalt2023.pdf?__blob=publicationFile&v=6, S. 25-26).

Taten außerhalb sozialer Beziehungen[9]. Dabei ist es möglich, dass in den letzten Jahren eine Verschiebung vom Dunkelfeld stattgefunden hat und entsprechende Delikte häufiger polizeilich bekannt werden. Daten zum Dunkelfeld digitaler Gewalt liegen aktuell noch nicht vor. Derzeit führen das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ), das Bundesministerium des Innern und für Heimat (BMI) und das Bundeskriminalamt (BKA) gemeinsam die geschlechterübergreifende Studie „Lebenssituation, Sicherheit und Belastung im Alltag (LeSuBiA)“ durch, die neben bundesweit repräsentativen Daten zu Gewalterfahrungen in (Ex-)Paarbeziehungen und sexualisierte Gewalt, erstmals auch Daten zu Gewalt im digitalen Raum erhebt.[10]

Für den Aufbau von Unterstützung durch IT-Expert*innen stellt sich vor diesem Hintergrund die Schwierigkeit, die erforderlichen Kompetenzen genauer zu umreißen. Welche Angriffsvektoren werden genutzt? Wie technisch versiert gehen die Angreifer vor? Welche präventiven Maßnahmen sind hilfreich und umsetzbar? Welche reaktiven Maßnahmen helfen den Betroffenen und sichern potentielle Beweise?

1.2 Digitalkompetenzen

Vielen Menschen ist das Missbrauchspotential sich ständig wandelnder digitaler Technologien nicht bewusst. Die Kompetenzen, dies zu erkennen und sich angemessen zu schützen, sind in der Gesellschaft unterschiedlich stark ausgeprägt. So wie Technikkenntnisse insgesamt weiterhin stark geschlechtsspezifisch verschieden sind, gibt es auch bei digitalen Geräten eine deutliche stereotype Rollenverteilung. Täter sind zumeist kreativ bei der Nutzung von Hard- wie Software für übergriffige und manipulative Zwecke, für die diese nicht konzipiert waren. Leider mangelt es den Produkten oft an Optionen zum Schutz vor digitalen Gewaltformen.

Nach bisherigem Kenntnisstand lassen sich für keine Bevölkerungssegmente Aussagen zu einer gehäuften Prävalenz machen – die einzige Ausnahme scheint hier das Alter zu sein. So sind laut Prasad (2021, S. 28) vor allem jüngere Frauen gefährdet.[11] Die Angriffsfläche vergrößert sich jedoch in dem Maße, in dem Nutzer*innen bei der Einrichtung und Nutzung von technischen Geräten und Anwendungen auf andere angewiesen sind oder zu sein glauben. Dies kann ein Produkt der persistenten geschlechtlichen Hausarbeitsteilung sein, was sich mitunter auf Unterschiede in der Digitalkompetenz zwischen Frauen und Männern zurückführen lässt.

---

[9] LKA Nordrhein-Westfalen (2020): Sicherheit und Gewalt in Nordrhein-Westfalen- Forschungsbericht. Kriminalistische-Kriminologische Forschungsstelle. Düsseldorf; LKA Niedersachsen (2022): Bericht zu Gewalterfahrungen in Paarbeziehungen. Sonderbericht zur Befragung zu Sicherheit und Kriminalität in Niedersachsen 2021, Landeskriminalamt Niedersachsen, Hannover.

[10] https://www.bka.de/lesubia

[11] Prasad N (2021) Digitalisierung geschlechtsspezifischer Gewalt Zum aktuellen Forschungsstand. In: Prasad N (ed.) *Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung: Formen und Interventionsstrategien*. Bielefeld: transcript Verlag, pp. 17–46.

Aber auch Personen mit Behinderung,[12] ältere Menschen und Personen mit geringerer Bildung oder in besonders herausfordernden Lebenssituationen sind anfällig für dieses Phänomen. Einen wesentlichen Faktor im Kampf gegen digitale Gewalt stellt deshalb das kontinuierliche Empowerment von Betroffenen dar sowie ein gesamtgesellschaftlicher Dialog, der sich kritisch mit der Kultur der Überwachung auseinandersetzt, die sich mit scheinbar sinnvollen Anwendungen wie dem Standortteilen in Familien salonfähig zu machen versucht.

Berater*innen haben in der Regel nicht die zeitlichen und monetären Ressourcen, zusätzlich die nötige technische Expertise aufzubauen, um dieses zusätzliche Themenfeld abzudecken. Da aber inzwischen viele Fälle von Gewalt im sozialen Nahraum digitale Aspekte beinhalten, ist ein Mindestmaß an diesbezüglicher Weiterbildung unbedingt sinnvoll. Die Berater*innen müssen einschätzen können, welche Möglichkeiten mit dem Missbrauch technischer Geräte und Anwendungen einhergehen, um ihn in den Fällen, mit denen sie konfrontiert sind, auch erkennen zu können.

1.3 Methodisches Vorgehen

Um eine klarere Vorstellung davon zu bekommen, welche Kompetenzen und Leistungen eine technische Anlaufstelle beinhalten muss, wurde im ersten Schritt eine Bedarfsanalyse durchgeführt. Ein zweites Arbeitspaket recherchierte und sichtete Best Practices – denn insbesondere in den USA, aber auch in Australien, Österreich, Großbritannien und in Baden-Württemberg gibt es bereits Einrichtungen, die genau diese bzw. eine ähnliche Beratungsleistung enthalten, aus deren wichtige Erkenntnisse für eine technische Anlaufstelle in Deutschland gewonnen werden konnten. Diese beiden Stränge wurden schließlich im Rahmen eines Workshops von den Teilnehmenden des Workstreams zusammengebracht und daraus ein Prototyp entwickelt, der die Organisationsstruktur, Leistungen und Anforderungen umfasst.

[12] https://www.esafety.gov.au/sites/default/files/2021-09/TFA%20WWICD_accessible.pdf

2. Bedarfsanalyse

Im Rahmen des Workstreams wurde eine Bedarfserhebung unter den institutionellen Bedarfsträgern durchgeführt. Der Fragebogen wurde auf Grundlage der Erfahrungen der Workstreamteilnehmenden und ihrer Vorarbeiten[13] gemeinsam erstellt. Mittels einer Online-Befragung unter den Berater*innen von WEISSER RING, bff und Frauenhauskoordinierung wurden Themenschwerpunkte und Erfahrungen im Bereich digitaler Gewalt bei Beratenden erhoben.

Die drei befragten Beratungsorganisationen haben das Ziel, den Betroffenen und Opfern von digitaler Gewalt zu helfen, ihre Rechte zu stärken und vertrauliche, individuelle Unterstützung bereitzustellen. Bei der Interpretation der Ergebnisse der Bedarfsanalyse ist zu berücksichtigen, dass die beteiligten Organisationen unterschiedliche Ausrichtungen und Beratungsstrukturen haben: So bietet der WEISSE RING als Deutschlands größter Verein für Opferhilfe eine breit angelegte Unterstützung für Opfer von digitaler Gewalt sowie allen anderen Straftaten an und ist deutschlandweit mit Außenstellen zur Beratung vertreten. Mit bff und Frauenhauskoordinierung sind dem gegenüber auch zwei Dachverbände aus dem Frauengewaltschutz beteiligt gewesen. Sie unterstützen das Hilfesystem durch Informationen, Austausch und politische Interessensvertretung. Hierbei repräsentiert der bff die Frauenberatungsstellen und Frauennotrufe. Frauenhauskoordinierung vertritt in erster Linie Frauenhäuser. Die Beratungsorganisationen weisen unterschiedliche Beschäftigungsverhältnisse auf. Während bspw. in den Frauenberatungsstellen und in Frauenhäusern primär hauptamtliche Fachkräfte aus dem sozialen Bereich tätig sind, beraten und unterstützen beim WEISSEN RING geschulte Ehrenamtliche die Betroffenen und Opfer.

Die Fragebögen wurden von den drei zentralen Stellen an die einzelnen Beratungseinheiten versandt. Eine eindeutige Zuordnung, ob Mitarbeitende oder Leiter*innen der Stellen geantwortet haben ist nicht möglich. Innerhalb des Erhebungszeitraumes vom 12.04.2024 bis zum 08.05.2024 erhielten wir 521 Rückmeldungen, von denen 131 dem bff, 145 dem WEISSEN RING sowie 245 der Frauenhauskoordinierung zuzuordnen sind.[14] Alle Fragen konnten freiwillig ausgefüllt werden, sodass es keine Pflichtangaben gab. Daher unterscheiden sich die Fallzahlen bei den einzelnen Fragen.

---

[13] Tanczer, L., López-Neira, I., & Parkin, S. (2021). 'I Feel Like We'Re Really Behind the Game': Perspectives of the United Kingdom's Intimate Partner Violence Support Sector on the Rise of Technology-Facilitated Abuse. Journal of Gender-Based Violence, 5(3), 431–450. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3931045

[14] Die Rohdaten sowie Detailauswertungen wurden den Bedarfsträger*innen zur weiteren Verwendung in den Frauenhäusern und Beratungsstellen zur Verfügung gestellt.

2.1. Thematisierung digitaler Gewaltformen in der Beratung

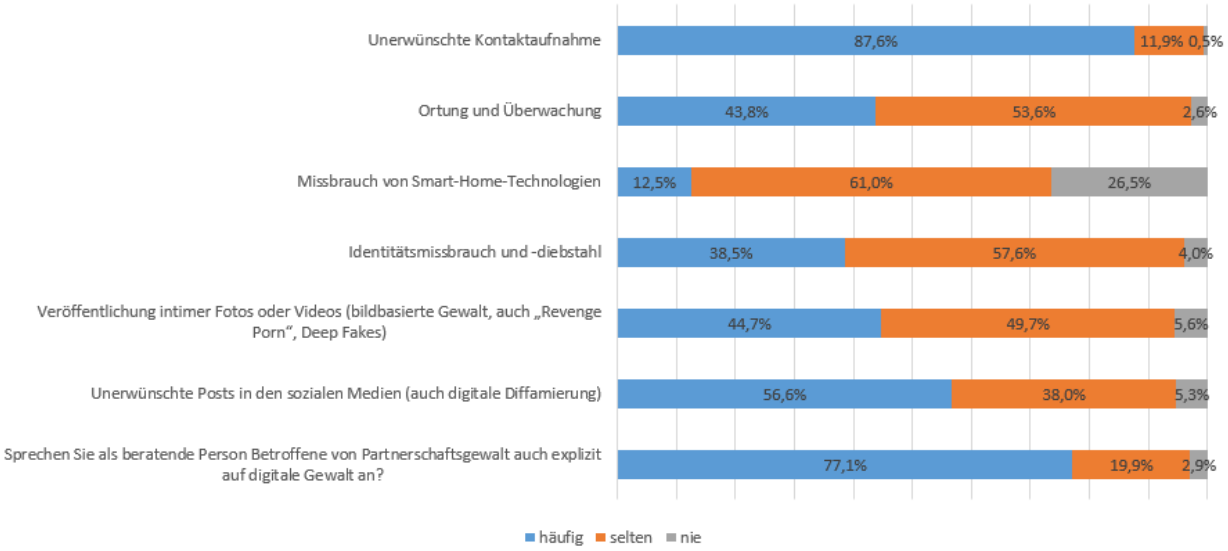

Abbildung 1: Häufigkeit der digitalen Gewaltformen in Beratung (in Prozent)"

Von allen befragten Personen gaben 77,1 % an, dass sie Ratsuchende im Gespräch häufig explizit auf digitale Gewalt ansprechen, 19,9 % tun dies selten und 2,9 % nie. Bei der Einschätzung, welche digitalen Gewaltformen in den Gesprächen thematisiert werden, wird unerwünschte Kontaktaufnahme am häufigsten benannt (87,6 %). Etwa die Hälfte der Befragten thematisiert im Beratungsgespräch häufig unerwünschte Posts in den sozialen Medien und digitale Diffamierung (56,6 %). 44,7 % der befragten Berater*innen gaben an, dass bildbasierte Gewalt ebenfalls häufig in den Beratungen Thema ist. Nur 12,5 % der Befragten geben an, dass der Missbrauch von Smart-Home-Technologien häufiger in ihrer Beratung vorkommt.

Für die Frage danach, warum die digitalen Gewaltformen unterschiedlich häufig in den Beratungsgesprächen angesprochen werden, existieren unterschiedliche Lesarten. In der Befragung wurden sowohl Beratungsstellen als auch Frauenhäuser befragt. Diese haben teilweise einen unterschiedlichen Fokus im Gespräch mit (potentiellen) Betroffenen, wodurch zum Beispiel Ortungstechnologien oder unerwünschte Kontaktaufnahmen im Akutfall in den Frauenhäusern höher priorisiert werden als Smart-Home-Technologien, die meist im Haushalt zurückgelassen werden. Zudem muss berücksichtigt werden, dass es in den Beratungsorganisationen unterschiedliche Kenntnis- und Wissensstände zu digitaler Gewalt und deren Ausprägungsformen gibt, was dazu führt, dass auch die Fähigkeit, bestimmte Gewaltformen zu benennen, als solche erkennen und einordnen zu können, unterschiedlich verteilt ist.

2.2 Technische Beratungskompetenz zu digitaler Gewalt

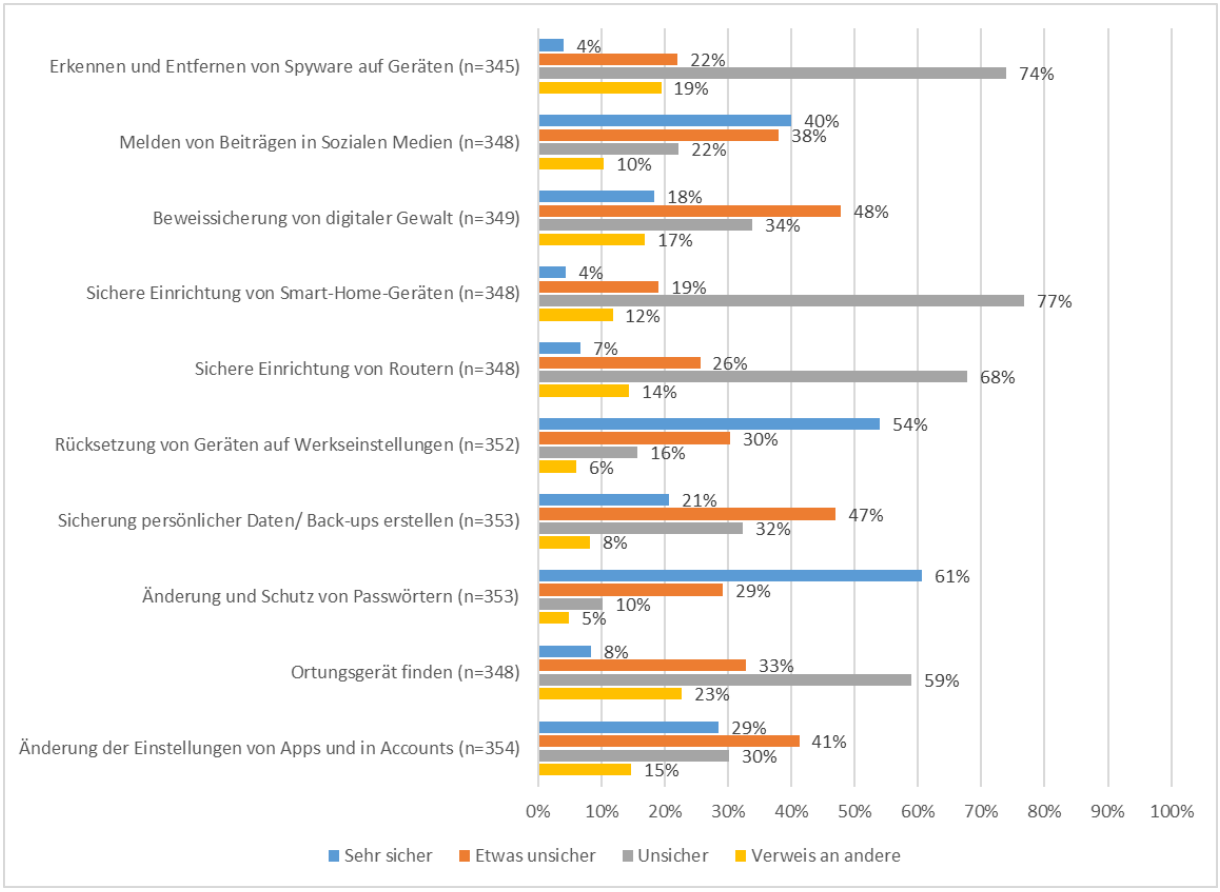

Abbildung 2: Sicherheit im Umgang mit digitaler Gewalt

Im Rahmen einer Selbsteinschätzung konnten die Befragten angeben, wie sicher sie sich beim Umsetzen unterschiedlicher digitaler Schutzmaßnahmen fühlen. Auffällig ist, dass die beratenden Personen sich beim Schutz und Ändern von Passwörtern sowie dem Zurücksetzen von Geräten auf Werkseinstellungen in der Regel sehr sicher fühlen. Möglicherweise ist dies darauf zurückzuführen, dass es sich um Aktivitäten handelt, die mittlerweile regelmäßig im Alltag vieler Nutzer*innen umgesetzt werden, wodurch eine gewisse Vertrautheit mit den Tätigkeiten entsteht. Gleichermaßen handelt es sich um Aktivitäten, bei denen man auf eine große Bandbreite an Anleitungen oder Informationsmaterial zurückgreifen kann, was eine zusätzliche Entlastung beim Auseinandersetzen mit den Technologien sein kann.

Täter nutzen soziale Medien, Messenger und Shoppingdienste häufig, um zu stalken oder zu diffamieren. Eine grundlegende Digitalkompetenz zum Schutz bei digitaler Gewalt ist deshalb das Ändern von Einstellungen in Apps und in Accounts von Online-Diensten. Hier gaben ein Drittel der Befragten (29 %) an, dass sie sich sehr sicher fühlen. Eine weitere Schutzmaßnahme kann das Melden von Beiträgen in Sozialen Medien darstellen, dabei gaben 40 % der Befragten an, dass sie sich sehr sicher fühlen. Neben dem Meldevorgang ist die Beweissicherung zentral, um rechtliche Schritte gegen Täter einleiten zu können. Hier wird jedoch deutlich,

dass nur ein Fünftel der Beratenden sich sehr sicher darin einschätzt, eine Beweissicherung bei digitaler Gewalt durchführen zu können. Nur ein Fünftel der Beratenden gab an, dass sie für die Beweissicherung an andere Akteure verweisen, obwohl es sich dabei um eine der Hauptaufgaben der Polizei handelt. Die Beratungsorganisationen berichten, dass es sehr unterschiedliche Erfahrungen damit gibt, ob die Polizei bei der Beweissicherung unterstützt oder überhaupt Anzeigen zu digitalen Gewaltformen aufnimmt.[15]

Die geringe Anzahl an Fällen, in denen Beratende generell an eine andere Person oder Institution verweisen, ist ein weiterer Indikator dafür, dass Strukturen gebraucht werden, die mit technischer Expertise Beratungsorganisationen bei ihrer Arbeit unterstützen.

Insgesamt lässt sich an der Grafik die Tendenz ablesen, dass die Unsicherheit der Beratenden mit zunehmend erforderlicher technischer Expertise steigt. Das Lokalisieren von Ortungsgeräten, Auffinden von Spyware und die sichere Einrichtung von Routern und Smart-Home-Technologien wird mit einer hohen Unsicherheit verbunden. Dies ist ein weiterer Hinweis darauf, dass es an technischer Expertise und Unterstützungsmöglichkeiten in der Beratung (potentieller) Betroffener von digitaler Gewalt mangelt.

2.3 Bedarfe der Beratenden

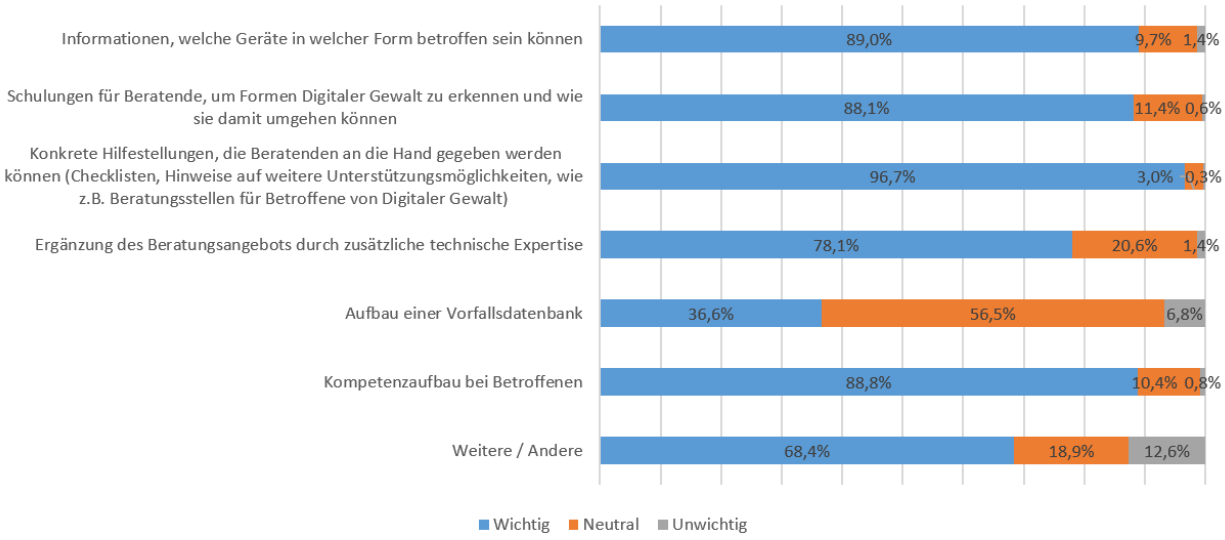

Abbildung 3: Was würden Sie sich als beratende Person für Hilfestellungen zum Thema digitale Gewalt wünschen und wie wichtig wären Ihnen diese? (n= 521)

Werden die Beratenden danach gefragt, welche Art von Unterstützung sie sich zum Thema digitale Gewalt wünschen, ergibt sich ein sehr breit gefächerter Bedarf. So wünschen sich

[15] Siehe auch „Bewohner*innenperspektiven auf den Schutz vor digitaler Gewalt im Frauenhaus“, S.10-16 https://www.frauenhauskoordinierung.de/fileadmin/redakteure/Publikationen/Handreichungen_Arbeitshilfen/22-11-29_FHK_Bericht_Bewohnerinnenperspektiven_auf_den_Schutz_vor_digitaler_Gewalt_im_Frauenhaus.pdf

nahezu alle Befragten (96,7 %) konkrete Hilfestellungen und Hinweise auf Unterstützungsmöglichkeiten zum Thema digitale Gewalt. Mehr als drei Viertel der Befragten wünschen sich konkrete Informationen zu möglicherweise betroffenen Geräten, einen Kompetenzaufbau auf Seite der Betroffenen (88,8 %), Schulungen für Beratende (88,1 %) und die Ergänzung bestehender Beratung durch technische Expertise (78,1 %). Der hohe und breit gefächerte Bedarf lässt sich dahingehend interpretieren, dass es offene Flanken hinsichtlich vorhandener technischer Unterstützung und Wissen gibt, sich die Beratenden der Situation jedoch bewusst sind und Unterstützung annehmen würden. Der Bedarf spiegelt sich auch in den offenen Angaben wider, in denen der Bedarf nach präventiven sowie vor allem auch technischen und forensischen Hilfestellungen noch einmal explizit geäußert wurde (vgl. Tabelle 1). Lediglich der Aufbau einer Vorfallsdatenbank ist niedriger priorisiert (36,6 %, vgl. Abbildung 3), wobei in den Auswertungsgesprächen mit den Institutionen gemutmaßt wird, dass dieses Antwortverhalten in einem Zusammenhang mit der Befürchtung eines zusätzlichen Dokumentationsaufwandes steht.

Anzahl	Themenfeld
15	Präventive Hilfestellungen (z.B. Anleitungen, Workshops für (potentiell) Betroffene)
13	Forensische Hilfestellungen (z.B. Beweissicherung)
12	Technischer Support/ Fachberatung
11	Reaktive Hilfestellungen (z.B. Anleitungen, Betroffenheitsfeststellung)
10	Juristische Unterstützung (z.B. Beratung, Sanktionierung)
8	Fachaustausch
4	Technische Lösungen
4	Sonstige (z.B. Fallbesprechungen, Finanzierung)

*Tabelle 1: Gewünschte Hilfestellungen seitens der Berater*innen*

Um die Bedarfe weiter zu konkretisieren, wurde ebenfalls erfragt, mithilfe welchen Mediums die technische Beratungs- oder Unterstützungsleistung idealerweise stattfinden sollte. Beratende wünschen sich für sich selbst technische Unterstützungsleistungen per Telefon (262 Nennungen), Video (244 Nennungen) und vor Ort (240 Nennungen). 140 Befragte fänden für sich eine Unterstützung per E-Mail hilfreich. Im Rahmen der Frage wurden Mehrfachnennungen zugelassen, es handelte sich um keine Pflichtfrage. Durch die hohe Antwortquote ist anzunehmen, dass Beratende bei der Ergänzung ihres eigenen Angebotes durch technische Beratung offen für unterschiedliche Informationskanäle wären und tendenziell einen hohen Bedarf an Ergänzungen haben.

Dem gegenüber gaben Beratende an, dass sie für Betroffene, ergänzend zu ihren Beratungsangeboten, eine technische Beratung per Video sinnvoll fänden (303 Nennungen), dicht gefolgt von der telefonischen Beratung (211 Nennungen) und der Beratung vor Ort (128

Nennungen). Hier lässt sich, trotz zugelassener Mehrfachantwort, eine Priorisierung von Beratungsangeboten erkennen, welche in der Regel schneller erfolgen können. So kann bei der Beratung per Video oder Telefon schneller Hilfe erfolgen und ist mit weniger Zeitverlust verbunden, als eine Anreise vor Ort oder ein langer Schriftwechsel bei der Beratung per E-Mail.

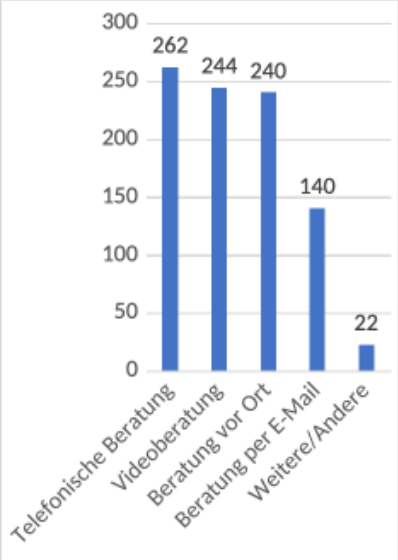

Abbildung 4: In welcher Form wäre eine technische Beratung für Sie eine sinnvolle Ergänzung zu Ihrem Beratungsangebot? Für Sie als beratende Person (n = 512, Mehrfachantwort)

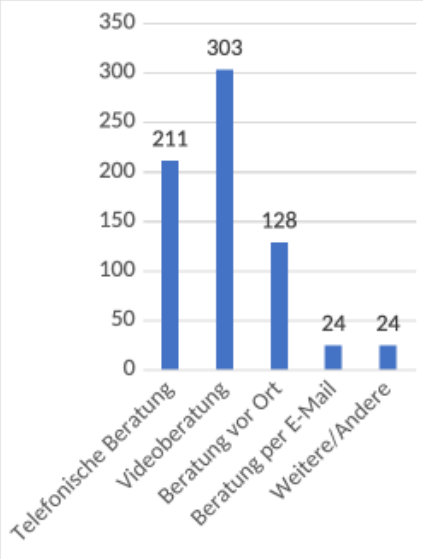

Abbildung 5: In welcher Form wäre eine technische Beratung für Sie eine sinnvolle Ergänzung zu Ihrem Beratungsangebot? Für betroffene Personen (n = 512, Mehrfachantwort)

Die zugehörigen offenen Angaben geben weiteren Aufschluss über die Entscheidung der Befragten und stützen die Interpretation der Ergänzungen zum Beratungsangebot. So werden eine einfache Erreichbarkeit und schnelle Terminvergabe im Rahmen der Angebote als besonders wünschenswert geäußert, was die Bevorzugung von Video und Telefon erklärt. Jedoch wurden auch weitere Faktoren, wie zum Beispiel die Barrierefreiheit, Möglichkeit zu Dolmetschungen, Verfügbarkeit mehrsprachiger Materialien und Anonymität bei der Beratung als Herausforderung angesprochen. Einzelfälle schildern diese Herausforderungen besonders für den ländlichen Raum, in welchem die Internetanbindung teilweise zu schlecht für Videoberatungen ist und wo eine Vor-Ort-Beratung mit hohen Reiseaufwänden einhergehen würde. Um diese Herausforderungen, abhängig von den regionalen Umständen, angemessen lösen zu können, ist die weitere Zusammenarbeit mit Beratungsorganisationen und ein engmaschiger Austausch mit Beratenden erforderlich.

3. Best Practices

Digitale Gewalt im sozialen Nahraum ist kein auf Deutschland beschränktes Phänomen. Andere Länder sind in Bezug auf die Unterstützung von Betroffenen und Beratungsorganisationen bei digitaler Gewalt schon sehr gut aufgestellt. Dennoch gibt es auch in der Bundesrepublik erste Ansätze, technische Expertise, psychosoziale und rechtliche Beratung miteinander zu verzahnen. In einem ersten Schritt wurde durch die Befragung von Expertinnen sowie eine Internetrecherche eine Liste von möglichen Best Practices erstellt:

1. *Women's Service Network* (WESNET) (Australien)[16]
2. *Remote Tech Clinic to Combat Tech-Enabled Domestic Abuse in Rural Wisconsin* der University of Wisconsin (USA)
3. *Cornell Tech's Clinic to end tech abuse*[17] (CETA) der *Cornell University* (USA)
4. *Kompetenzstelle gegen Cyber-Gewalt an Frauen* der Stadt Wien (Österreich)
5. *Koordinierungsstelle zu digitaler Gewalt im sozialen Nahraum* von *Frauen helfen Frauen e.V*. Heidelberg
6. Modellprojekt *Interaktion* des *Bundesverbandes Frauenberatungsstellen und Frauennotrufe* (Deutschland)
7. Modellprojekt *IT-Beratung* von *Frauenhauskoordinierung* (Deutschland)
8. Multiplikator*innen-Ausbildung für Fachkräfte aus dem Gewaltschutz von *Ein Team gegen digitale Gewalt* (Deutschland)

Aus Zeit- und Kapazitätsgründen konnten nicht alle vorhandenen Initiativen recherchiert und gesichtet werden. Beispielsweise fehlt in der obigen Aufzählung das Angebot von *Refuge*[18] (Großbritannien) und die *Technology-Enabled Coercive Control Clinic* der Universität Seattle[19]. Erst kürzlich ist eine Publikation erschienen, die einen Überblick und eine ausführliche Diskussion von Best Practices im Bereich digitale Gewalt bietet (Pickering 2024).[20]

Das **Women's Service Network (WESNET)** ist die führende Frauenorganisation in Australien, die sich für die Bekämpfung von häuslicher und interfamiliärer Gewalt einsetzt. WESNET

---

[16] Ebenfalls recherchiert wurde das Safety Net Project des National Network to End Domestic Violence (NNEDV) (USA), welches im Folgenden aufgrund der strukturellen Ähnlichkeit zu WESNET nicht weiter betrachtet wird.

[17] Im englischsprachigen Raum wird statt von digitaler Gewalt von Tech Abuse oder auch Technology facilitated Abuse gesprochen. In der Darstellung der Best Practices wird der in Deutschland gängige Begriff der digitalen Gewalt verwendet.

[18] Refuge's Technology-Facilitated Abuse and Economic Empowerment Team are the only UK specialist service directly supporting survivors facing complex tech and economic abuse concerns: https://refugetechsafety.org/about-us-3/

[19] https://newbegin.org/find-help/staying-safe/technology-safety/

[20] https://www.churchillfellowship.org/ideas-experts/ideas-library/international-reflections-creating-best-practice-for-survivors-of-technology-facilitated-abuse

wurde 1992 gegründet und vertritt aktuell etwa 350 Mitgliedsorganisationen in ganz Australien, zu denen auch Technologieexpert*innen und Einrichtungen speziell für Frauen gehören, wie Notunterkünfte, Frauenhäuser, sichere Häuser und Beratungsstellen. Die folgenden Ausführungen beziehen sich auf das Angebot von WESNET für digitale Gewalt. Ein wichtiger Aspekt darüber hinaus betrifft die Rolle von WESNET als Lobby-Verband, der den für die Finanzierung notwendigen Grundetat von der australischen Regierung einfordert. Beispielsweise wurde die Förderung des Programms zu digitaler Gewalt in 2019 aufgrund auslaufender Projektmittel eingestellt. WESNET hat es mittlerweile erreicht, dass die Mittel ab 2023 fortgesetzt und sogar verdoppelt werden. Die Unterstützungsangebote von WESNET im Bereich digitale Gewalt beinhalten:

- Sichere Smartphones, die an Überlebende von partnerschaftlicher/häuslicher Gewalt ausgegeben werden, inkl. eines Guthabens von 30 $.
- Bildung und Unterstützung durch die WESNET Expert*innen für technische Sicherheit für Berater*innen. Betroffene erhalten z.B. nicht nur ein neues Smartphone, sondern werden auch dazu ermächtigt, dieses selbständig sicher einzurichten und zu nutzen.
- Web-Portal techsafety.org.au: Enthält u.a. das Survivor Toolkit: sechs verschiedene Ausgangsproblemlagen (Leben mit jemandem, der einen überwacht, sich von jemandem trennen wollen, der einen überwacht, Betroffenheit von Hate Speech, Stalking durch unbekannte Person, Betroffenheit durch die Arbeit mit Klienten bei Lehrern, Sozialarbeitern o.ä., Beratung von anderen, die von digitaler Gewalt betroffen sind. In den meisten Fällen werden dann Checklisten oder auch Fragen zur Einschätzung, ob digitale Gewalt vorliegt oder vorliegen könnte, vorgehalten.) Die Seite führt alle Informationen zu digitaler Gewalt zusammen, auch die Trainings. Für Berater*innen gibt es auch noch ein separates Angebot mit Flyern und weiterführender Literatur sowie Informationen zur Nutzung von Technologie im Beratungsprozess.
- Appsafetycentre: Gibt Praktiker*innen und Betroffenen einen Überblick über Apps, die in einer Situation von digitaler Gewalt und häuslicher Gewalt nützlich sein können. Dies umfasst u.a. Apps zur Unterstützung der Dokumentation, zur Weiterbildung und Informationen oder auch, um einen Notruf abzusetzen und Hilfe zu holen. Auch App-Entwickler*innen können hier Empfehlungen erhalten, was bei der Entwicklung von Sicherheitsapplikationen zu bedenken ist (verwiesen wird dabei auf die US-amerikanische Schwesterorganisation NNEDV).
- Peer-to-Peer-Training: Berater*innen, die über gute IT-Kompetenzen verfügen und Erfahrungen im Bereich digitale Gewalt haben, bieten Trainings für andere Berater*innen an. WESNET übernimmt dabei die Koordination und Organisation.
- Öffentlichkeitsarbeit (Interview mit Facebook) und Vernetzung (jährliche Konferenz zum Thema digitale Gewalt und Partnerschaftsgewalt), aber auch Forschung und

Entwicklung (beispielsweise hat WESNET auch zur Entwicklung des Tinytool zum Aufspüren von Stalkerware beigetragen). Hinzu kommen Umfragen unter den Berater*innen bzw. Frontline Workers, wie in 2020[21], bei der die Rolle von Kindern und deren technischen Geräten im Kontext von häuslicher Gewalt in Trennungssituationen erhoben wurde.

Die **CETA, die Clinic to End Tech Abuse** der Cornell University ist ein gutes Beispiel für die enge Verknüpfung von Forschung und Hilfesystem. Studierende werden hier in die Betreuung von Fällen einbezogen, die Fälle selbst erhoben und ausgewertet. Die Beratung der Betroffenen erfolgt direkt (vor Ort) durch entsprechende Expert*innen mit IT-Kenntnissen (Graduierte, Doktorand*innen etc.) der Cornell Tech, einer öffentlichen Universität. Die IT-Expert*innen erhalten ergänzende Schulungen, die sie zum sensiblen Umgang mit Betroffenen von Partnerschaftsgewalt befähigen. Die technische Beratung der Betroffenen durch die IT-Expert*innen erfolgt ehrenamtlich.

Zur Umsetzung besteht eine enge Zusammenarbeit mit einer Beratungsstelle für Familien und Gewaltbetroffene, um den wechselseitigen Informations- und Erfahrungsaustausch kontinuierlich zu gewährleisten. Die Weiterbildung bzw. auch die Terminvereinbarung für die technische Beratung erfolgt über den Kontakt zur Beratungsstelle für Gewaltbetroffene, sodass diese in der Regel auch psychosozial betreut und versorgt werden können, sofern dies notwendig sein sollte.

Die Erstellung von Material zur Weiterbildung nicht nur für Betroffene, sondern auch für Berater*innen gehört zum Leistungsspektrum der Tech Clinic. Diese Weiterbildungsangebote werden kostenpflichtig angeboten und dienen damit auch der Finanzierung der Clinic. Die Kosten für Fortbildungen variieren dabei, da bspw. Beratungsorganisationen günstigere Tarife erhalten als Unternehmen. Das Angebot der technischen Beratung ist auf das Einzugsgebiet der Universität konzentriert. Gemeinsam mit zwei weiteren Tech Clinics wurde zudem ein Ratgeber erstellt, der eine Hilfestellung beim Aufbau einer technischen Anlaufstelle bieten soll und auch Gegenstand der Betrachtung im Workstream war.[22]

Die **Remote Tech Clinic to Combat Tech-Enabled Domestic Abuse in Rural Wisconsin** ist an die University of Wisconsin angegliedert. Sie bietet Unterstützung für Betroffene von Partnerschaftsgewalt (Intimate Partnership Violence), die in ländlichen Gegenden wohnen und

[21] https://wesnet.org.au/about/research/2ndnatsurvey/
[22] https://www.techabuseclinics.org/

keinen direkten Zugang zu Unterstützung vor Ort haben. Dabei wendet sich das Angebot an Betroffene und deren Fachberatung, die gemeinsam remote beraten werden. Zusätzlich werden die Fälle erhoben, ausgewertet und auf dieser Basis weitere Materialen wie das Toolkit zur Einrichtung von Tech Clinics oder Trainingsprogramme für Freiwillige (weiter) entwickelt.

Dieser Ansatz ist aus verschiedenen Gründen als sehr wertvoll für die weitere Ausarbeitung des Konzepts hervorzuheben. Zum einen erleichtert die remote Beratung den Zugang auch für ländliche Gebiete in der Bundesrepublik. Die gleichzeitige Beratung von Betroffenen und ihren zuständigen Fallbearbeiter*innen der psychosozialen Beratung senkt zum einen das Erfordernis, die technischen Berater*innen im Kontext Partnerschaftsgewalt umfänglich zu schulen. Zum anderen kann eine remote Beratungsstruktur Kosten senken, indem nicht überall, flächendeckend Gebäude für eine Vor-Ort-Beratung gemietet und betrieben werden müssen. Allerdings ist zu bedenken, dass Betroffene hier regelmäßig auf den Zugang zur Beratung über einen von einer Beratungsorganisation bereitgestelltes Endgerät angewiesen sind. Das heißt, dass dieses Modell nur dann trägt, wenn die Beratungsinfrastrukturen entsprechend flächendeckend und barrierearm ausgebaut sind sowie eine stabile Internetanbindung vorhanden ist.

Als zusätzliche Leistung ist hervorzuheben, dass die dokumentierten Fälle auch vom wissenschaftlichen Personal der Universität ausgewertet werden. Auf diese Weise wird sichergestellt, dass die Tech Clinic, das wissenschaftliche Personal, Beratungsorganisationen usw. hinsichtlich missbrauchter IT kontinuierlich auf dem Laufenden sind und hieraus sowohl präventive Maßnahmen bzgl. Sensibilisierung von Verbraucher*innen, aber auch in Richtung von Herstellern und Anbietern ableiten kann. Finanziert wird das Angebot aus öffentlichen Mitteln wie auch aus Spendengeldern. Studierende profitieren von der Teilnahme, da sie so theoretische Lehrinhalte praktisch anwenden können und zudem frühzeitig in die Forschung einbezogen werden.

Im deutschsprachigen Raum ist vor allem die **Kompetenzstelle gegen Cyber-Gewalt an Frauen der Stadt Wien** bekannt. Sie unterscheidet sich von den vorhergegangenen Beispielen unter anderem bzgl. der Art der Finanzierung: Im Fall der Kompetenzstelle gegen Cybergewalt an Frauen handelt es sich um ein Angebot der Stadt Wien. Dabei ist die Kompetenzstelle keine einzelne Einrichtung, sondern beschreibt die enge Zusammenarbeit zwischen Beratungsorganisationen (24-Stunden-Frauennotruf, Wiener Fachberatungsstellen und Frauenhäuser) mit einer zentralen Stelle mit Technikexpertise (CERT Wien).[23] IT-Fachkräfte der Stadt Wien unterstützen Beratende in den Einrichtungen bei der technischen Beratung. Die psychosozialen Beratenden können die IT-Fachkräfte kontaktieren, wenn sie vertiefte Expertise

[23] https://www.wien.gv.at/menschen/frauen/stichwort/gewalt/cyber-gewalt/kompetenzstelle.html

benötigen.[24] Somit können personelle und materielle Ressourcen im IT-Bereich der Stadt Wien auch für den Frauen-Gewaltschutz zugänglich gemacht werden. In manchen Fällen findet eine Video- oder Telefonberatung gemeinsam mit Klientin, Berater*in und IT-Sicherheitsexpert*in statt, wobei abgeklärt wird, ob technische Unterstützung durch das CERT Wien oder polizeiliche Beratung zur Beweissicherung erforderlich ist.

In Deutschland hat das Bundesland Baden-Württemberg eine **Koordinierungsstelle zu digitaler Gewalt** im sozialen Nahraum eingerichtet.[25] Der Verein Frauen helfen Frauen e.V. bietet im Rahmen der Koordinierungsstelle kostenlose Fortbildungen und individuelle Fallberatungen für Mitarbeiter*innen aus Beratungsstellen zu häuslicher und sexualisierter Gewalt sowie aus Frauenhäusern an. Die Fortbildungen werden online und in Präsenz, (drei Stunden bis Tagesseminar) zum Thema digitale Gewalt aus diversen Perspektiven angeboten (rechtliche, psychosoziale, technische oder politische Perspektive). Individuellen Fallberatungen finden online statt und sind für Mitarbeiter*innen, die Betroffene begleiten. Dort können technische Fragestellungen zu digitaler Gewalt erfragt werden und es wird auch Unterstützung angeboten, wenn Mitarbeitende bei der Begleitung von Betroffenen selbst nicht weiterkommen oder unsicher sind.

Seit 2024 gibt es eine Webseite für Fachkräfte in Baden-Württemberg, die aktuelles Wissen und grundlegende Informationen für die Beratung zu digitaler Gewalt im sozialen Nahraum bereitstellt. Sie stellt u.a. Checklisten und Anleitungen zu neuesten technischen Entwicklungen für Fachkräfte zur Verfügung, die einen Zugang benötigen, um auf die Ressourcen zuzugreifen.[26]

Im Modellprojekt **InterAktion des bff** von 2022 wurde an zwei Standorten die Zusammenarbeit zwischen Frauen- und IT-Beratung erprobt. Besonderes Augenmerk lag dabei auf dem Grundsatz, der Klientin Entscheidungsfreiheit und Selbstwirksamkeitserfahrungen zu ermöglichen, auch in der Beratung durch eine*n IT-ler*in. Im Ergebnisbericht wurde zudem festgehalten, dass es wichtig ist, sich über die Ziele der technischen Unterstützung im Klaren zu sein: Geht es in erster Linie um Schadensbegrenzung oder Beweissicherung oder um die Vermittlung des souveränen Umgangs mit IT?[27] Insgesamt wurde nach der Laufzeit ein positives Resümee gezogen. So hat insbesondere der gewünschte Wissens- und Erfahrungsaustausch

---

[24] FHK-Fachinfo Digitale Gewalt, Seite 19 https://www.frauenhauskoordinierung.de/fileadmin/redakteure/Publikationen/Fachinformationen/2021-11-10_FHK-Fachinformation_DigitaleGewalt_2021-Nr02.pdf

[25] https://www.fhf-heidelberg.de/de/digitale-gewalt/koordinierungsstelle-digitale-gewalt/

[26] Vergleichbare Informationen finden Betroffene u.a. hier https://antistalking.haecksen.org/

[27] https://www.frauen-gegen-gewalt.de/de/broschueren-und-buecher/was-tun-gegen-geschlechtsspezifische-gewalt-kooperation-zwischen-fachberatung-und-it-als-l%C3%B6sungsansatz.html(S. 18) zuletzt abgerufen am 23.10.2024

gut funktioniert und die Vernetzung der Beratungsstellen mit Vertretern*innen aus den verschiedenen Bereichen der IT hat auch dazu geführt, die Problematik der digitalen Gewalt im sozialen Nahraum in die IT-Profession hineinzutragen.

Bis Mitte 2025 läuft das Modellprojekt **„IT-Beratung“ von Frauenhauskoordinierung.** Dabei wird erprobt, wie IT-Beratung wirksam für das Hilfesystem umgesetzt werden kann. Mit den Ergebnissen des Modellprojekts werden Empfehlungen an Bund und Länder erarbeitet, damit IT-Kompetenzzentren aufgebaut werden, die unter anderem Mitarbeitende des Hilfesystems technisch zu digitaler Gewalt beraten.

Die IT-Beratung steht für 17 Modellstandort-Frauenhäuser bundesweit zur Verfügung. Die Frauenhaus-Mitarbeitenden können sich per E-Mail, Telefon oder Videokonferenz beraten lassen. Es besteht auch die Möglichkeit, die Beratung gemeinsam mit der Betroffenen und der Frauenhaus-Mitarbeitenden durchzuführen, bei Bedarf auch mit Dolmetschen. Die IT-Beraterinnen unterstützen bei (Verdachts-)Fällen digitaler Ortung und Überwachung. Aber auch bei fallunabhängigen Fragen ist eine Beratung möglich. Die IT-Beraterinnen verfügen auch über Kenntnisse zu geschlechtsspezifischer Gewalt und dem Hilfesystem, was für die Beratung wichtig ist. Die IT-Beratung wird von den Modellstandorten als sehr hilfreich wahrgenommen und es besteht großer Bedarf an Verstetigung und Ausweitung.

Das Modellprojekt findet im Rahmen des BMFSFJ geförderten Projektes „Digitaler Gewalt handlungssicher begegnen“ statt.[28] In dem Projekt wird außerdem eine Fortbildungsreihe für Frauenhausmitarbeitende zu rechtlichen, psychosozialen, technischen und medienpädagogischen Aspekten digitaler Gewalt angeboten. Des Weiteren werden medienpädagogische Materialien für Mitarbeitende und Frauenhaus-Bewohner*innen entwickelt, die zielgruppengerecht zum Schutz vor digitaler Gewalt im Frauenhaus sensibilisieren.

Das Projekt **„Ein Team gegen digitale Gewalt“** des Berliner Instituts für Technik und Journalismus e.V. schult und berät Gewaltschutzeinrichtungen zum Thema digitale Ortung und Überwachung. Fachkräfte aus sozialen Berufen erwerben dabei das nötige Wissen, um unerwünschte Zugriffe auf Geräte und Accounts zu unterbinden. Anschließend können sie Ratsuchende bei der Absicherung ihrer Geräte begleiten. Die unterschiedlichen Formate werden abhängig von den Ressourcen der Auftragnehmenden gemeinsam geplant. Neben halb- und ganztägigen Fortbildungen bietet das Projekt eine Multiplikator*innen-Ausbildung an, bei der Personen innerhalb von sechs Monaten vertieftes Expert*innenwissen erlangen. Alle Inhalte können deutschlandweit in Präsenz und online vermittelt werden.

[28] https://www.frauenhauskoordinierung.de/arbeitsfelder/digitale-gewalt

4. Konzept für eine technische Anlaufstelle

Um die durch die Bedarfsanalyse und die Best-Practices gewonnenen Ergebnisse bestmöglich zusammenzufassen, wurden im Rahmen eines Präsenzworkshops in Kleingruppen zwei Modelle für die technische Anlaufstelle entwickelt. Dabei wurde zum einen die Perspektive der Beratungsorganisationen und zum anderen die Perspektive der Betroffenen eingenommen.

4.1 Technische Anlaufstelle für Berater*innen

Abbildung 6: Modell zur technischen Unterstützung von Beratenden

Beim Modell aus Sicht der Beratenden, wurde als Ausgangspunkt angenommen, dass psychosozialen Beratende im direkten Kontakt mit Klient*innen stehen. Ausgehend davon gewährleisten Beratungsorganisationen eine grundlegende Beratung zu digitaler Gewalt, im Sinne einer ersten Hilfe. Um die erste Hilfe sinnvoll zu gestalten, ist sowohl bei haupt- als auch bei ehrenamtlich tätigen Beratenden sinnvoll, diese durch ergänzende Schulungen für den Bereich der digitalen Gewalt zu sensibilisieren und Wissen über die verschiedenen digitalen Gewaltformen und mögliche Unterstützungsoptionen zu vermitteln. Wie diese Kenntnisse vermittelt werden können und welche unterschiedlichen Optionen dafür zur Verfügung stehen, ist den Best Practices zu entnehmen (vgl. Kapitel 3).

Im Modell muss dabei auf die unterschiedlichen Praxiserfahrungen aus den Beratungsorganisationen zurückgegriffen werden. So ist zu berücksichtigen, dass bei hauptamtlich Beratenden in Fachberatungsstellen und Frauenhäusern angesichts von Unterfinanzierung ein zeitlicher und personeller Mangel besteht, der den Kompetenzaufbau zu digitaler Gewalt in den Einrichtungen massiv bremst. Hier braucht es zusätzliche Ressourcen in den Einrichtungen, damit sie grundlegende technische Beratung gewährleisten können.

Im Bereich der ehrenamtlichen Opferhilfe des WEISSEN RINGS besteht aufgrund von dessen finanzieller Unabhängigkeit von staatlichen Mitteln das Problem des zeitlichen und personellen Mangels weniger. Die Motivation zur Weiterbildung und Teilnahme an Seminaren, die grundlegende Inhalte zu digitaler Gewalt und deren Erkennung vermitteln, ist im Ehrenamt groß. Eine direkte technische Beratung der Betroffenen durch Mitarbeitende des WEISSEN RINGS selbst ist hingegen nicht umsetzbar.

Ergänzend zu der „ersten Hilfe“ durch die psychosoziale Beratung, werden deshalb technische Anlaufstellen vorgeschlagen. Diese sollen dann zum Einsatz kommen, wenn Beratende an die Grenzen ihrer Kenntnisse stoßen oder ein Fall technologisch komplex ist. Diese kann optional als Vor-Ort-Beratung angeboten werden, wenn das Anleiten per Videokonferenz oder Telefon nicht oder nur schwer möglich ist oder besondere technische Expertise erforderlich wird. Die Kompetenzen der technischen Anlaufstellen sollen von der akuten Schadensbegrenzung, z.B. hinsichtlich Gerätestatus, Informationsabfluss oder Datensicherung, bis hin zur Spurensicherung und digitaler Forensik reichen. Zusätzlich führt die technische Beratung eine Vorfallsdatenbank, um bspw. neue Angriffsvektoren zu erkennen, zu systematisieren und das Wissen in zukünftige Fallberatungen einzubringen.

Eine Koordinierungsstelle dient als vermittelnde Stelle zwischen den bestehenden Beratungsorganisationen und den technischen Anlaufstellen. Die Koordinierungsstelle ist dafür zuständig, den Wissens- und Erfahrungsaustausch zwischen Beratungsorganisationen, der technischen Beratung und der Koordinierungsstelle zu organisieren. Das kann beispielsweise in Evaluationstreffen und über die generelle Vernetzung der beteiligten Beratungseinheiten erfolgen. Durch den Austausch wird den Beratungsstellen und Frauenhäusern Einblick in aktuelle sicherheitstechnische Problemstellungen und deren Bedeutung für digitale Gewalt gegeben. Gleichermaßen lernt das technische Personal die Beratungstechniken und den Umgang mit Betroffenen kennen. Außerdem organisiert die Koordinierungsstelle Fortbildungen für Beratungsorganisationen. Ziel soll ein gemeinsamer Wissensaustausch auf Augenhöhe zu den genannten Punkten sein.

Neben Fortbildungen und Evaluationstreffen, ist die praxisgerechte Aufbereitung von Informationen ein Bestandteil des Wissensaustauschs. Die Entwicklung von Anleitungen und Checklisten für Beratende, sowie Informationsmaterialien für Betroffene wurde demnach als Anforderung formuliert. Besonders auffällige oder sich häufende Schemata von digitaler Gewalt können in dieser Form pseudonymisiert aufbereitet, in leichte „nicht technische“ Sprache überführt und den Bedarfsträgern bereitgestellt werden. Die langfristige Systematisierung der Fälle soll ebenfalls zum geregelten, aktuellen Wissensaustausch der einzelnen Instanzen beitragen und in die oben genannten Aspekte mit einfließen.

Im Sinne der Qualitätssicherung ist die Koordinierungsstelle zuständig für die Auswahl des technischen Personals. Auswahlgespräche, regelmäßige Evaluationen und das Einholen von Feedback von Betroffenen zum Beratungsprozess tragen dabei zu einer konstant hohen Beratungsqualität sowie der generellen Gestaltung eines sicheren Raumes für Beratende und Bertoffene bei.

4.2 Technische Anlaufstelle für Betroffene

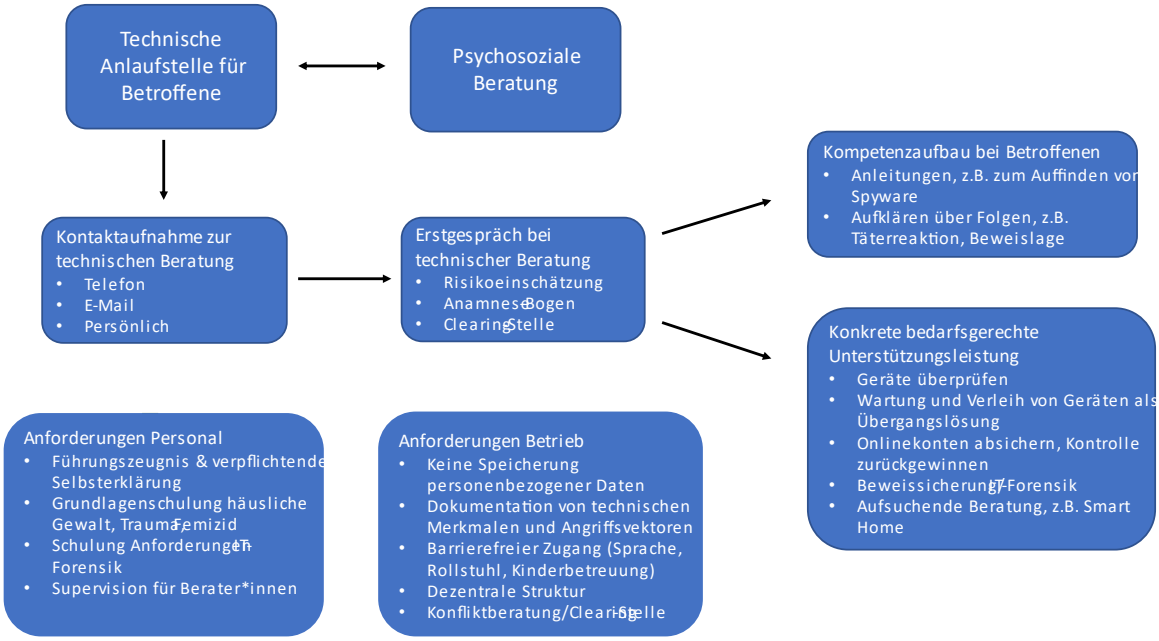

Abbildung 7: Modell zur technischen Unterstützung von Betroffenen

Das Modell, das sich primär an Betroffene wendet, soll dezentral organisiert werden. Betroffene von digitaler Partnerschaftsgewalt sollen damit auch die Möglichkeit erhalten, sich direkt an eine technische Anlaufstelle zu wenden. Die im Folgenden vorgestellte Struktur für das zweite Modell lässt sich unmittelbar an die im ersten Modell vorgeschlagene „Technische Anlaufstelle“ anschließen, um Synergien auszunutzen. Zu beachten sind hier die Anforderungen an den barrierearmen Zugang. Diese umfassen sowohl die Kontaktaufnahme via E-Mail und Telefon als auch die persönliche Vorsprache. Dazu soll gewährleistet sein, dass die Einrichtungen auch für Menschen mit Behinderung zugänglich sind. Zudem soll die verwendete Sprache bei Bedarf niedrigschwellig sein, um sicherzustellen, dass die Betroffenen die erarbeitete Lösung verstehen und nachvollziehen können sowie mit einem Zuwachs an Autonomie aus der Beratung gehen. Auch soll Beratung in unterschiedlichen Sprachen möglich sein.

Das Leistungsspektrum umfasst die Überprüfung potenziell kompromittierter Geräte und Konten. Angelegt an das Vorgehen von WESNET soll auch ein Bestand an Leihgeräten aufgebaut werden, um Betroffene im Fall einer Übergangszeit mit den erforderlichen

Kommunikationsmitteln ausstatten zu können. Des Weiteren sollen auch Fachleute für IT-Forensik beteiligt werden, um die Beweissicherung anzuleiten und zu unterstützen. Da zunehmend vom Smart Home als Angriffsvektor auszugehen ist[29], soll in Fällen, bei denen Geräte nicht transportiert werden können oder das kompromittierte Gerät nicht von der Betroffenen identifiziert werden kann, auch ein IT-Service eingerichtet werden, der Betroffene zu Hause aufsucht und bei diesen Herausforderungen begleitet und unterstützt.

Hinsichtlich des IT-Personals soll ein Führungszeugnis vorgelegt und eine verpflichtende Selbsterklärung unterzeichnet werden, um den Schutz der Betroffenen zu gewährleisten und den Gefahren von Missbrauch der Machtposition als technische*r Berater*in frühzeitig vorzubeugen. Das technische Personal ist auf die Beratungen durch die verpflichtende Teilnahme an Grundlagenschulungen zu häuslicher Gewalt, Trauma und Mehrfachdiskriminierung vorzubereiten. Auch sollen die spezifischen Anforderungen an die IT-Forensik im komplexen Handlungsfeld der digitalen Gewalt in einer weiteren Schulung vermittelt werden. Um den besonderen Herausforderungen bei der Unterstützung von Gewalt Betroffener zu begegnen, kann das technische Personal jederzeit auf ein Supervisionsangebot zurückgreifen. Eine enge Zusammenarbeit mit Angeboten der psychosozialen Beratung vor Ort soll zudem eine wechselseitige Verweisungsstruktur und auf die jeweiligen Bedarfe der Betroffenen ausgerichtete Hilfestellung gewährleisten.

Zu Beginn der Beratung soll auf Grundlage eines vorab erarbeiteten Anamnesebogens eine Ersteinschätzung zu dem Fall erfolgen. Erst danach und mit informiertem Einverständnis der Betroffenen werden die nächsten Schritte eingeleitet. Neben der Überprüfung, Beweissicherung und Wiederherstellung, ist Kompetenzaufbau bei den Ratsuchenden ein wesentliches Ziel der Beratung. Diese sollen befähigt werden, grundlegende Schritte zum Ausschluss von Fremdzugriffen auf die eigenen Geräte und Accounts zur Kontenüberprüfung und Wiederherstellung zu verstehen und selbst anwenden zu können. In besonderem Maße ist darauf zu achten, dass sie jederzeit über die Konsequenzen der technischen Maßnahmen informiert werden. Im Konfliktfall steht den Betroffenen eine Beschwerdestelle zur Verfügung.

Es sollen keine personenbezogenen Daten der Betroffenen gespeichert werden, die über das für die Beratung erforderliche Maß hinausgehen. Diese werden spätestens mit dem Abschluss der Beratung gelöscht. Langfristig erhoben und verarbeitet werden nur die technologischen, den konkreten Vorfall betreffenden Daten. Es soll sukzessive eine Vorfallsdatenbank aufgebaut werden, welche Aufschluss über Angriffe und über die Angriffsvektoren gibt, und so

[29] Brown, A., Harkin, D., & Tanczer, L. (2024). Safeguarding the 'Internet of Things' (IoT) for Victim-Survivors of Domestic and Family Violence (DFV): Anticipating Exploitative Use and Encouraging Safety-by-Design. Violence Against Women. https://journals.sagepub.com/doi/10.1177/10778012231222486

einerseits wichtige Hinweise für die Prävention gibt, aber auch Grundlage für den Dialog mit Herstellern von Produkten mit Missbrauchspotential ist.

Die beiden erarbeiteten Modelle können als komplementär zueinander betrachtet werden. Die zentrale Koordinierungsstelle mit dem Fokus auf Unterstützung der Beratenden und die dezentralen technischen Anlaufstellen für Betroffene ergänzen sich. Auf diese Weise ist sowohl die schnelle und barrierearme Unterstützung für Betroffene gesichert, als auch der langfristige Kompetenzaufbau bei Beratungsorganisationen. Zudem könnte die anvisierte „Koordinierungsstelle“ Aufgaben wie das Führen von Auswahlgesprächen, die Erstellung des Anamnesebogens, die Einrichtung der Clearingstelle, das Erstellen von Informations- und Hilfsmaterial sowie das Angebot der Supervision übernehmen. Aus Perspektive der IT-Sicherheit ist mit dem dadurch verfolgten kooperativen Ansatz auch sichergestellt, dass das Lagebild auf einem aktuellen Stand ist und bislang nicht in den einschlägigen Statistiken erhobene Vorfälle erfasst werden können. Dies schafft die erforderliche Grundlage für präventive sowie ggf. regulatorische Maßnahmen.

5. Fazit

Durch den Workstream erfolgte die erste gemeinsame quantitative Bedarfserhebung von institutionellen Bedarfsträgern. Die Ergebnisse der Bedarfserhebung zeigen die große Diskrepanz zwischen der Zunahme von digitalen Gewaltfällen und den fehlenden Strukturen im Hilfesystem für adäquate Beratung zu digitaler Gewalt. Die Best Practices zeigen Wege auf, wie das Hilfesystem gestärkt werden kann.

Das vorgeschlagene Konzept adressiert viele der zentralen Herausforderungen im Umgang mit digitaler Gewalt im sozialen Nahraum. Es zielt darauf ab, Beratungsorganisationen zu entlasten, Betroffene zu unterstützen, Expertise bei Berater*innen aufzubauen und Betroffene zu empowern.