Zürcher Hochschule
für Angewandte Wissenschaften

Soziale Arbeit
Institut für Delinquenz
und Kriminalprävention

Kompetenzzentrum
für Strafrecht und Kriminologie
Universität St.Gallen

Cybercrime gegen Privatpersonen in der Schweiz

Ergebnisse des Crime Survey 2022

Studie im Auftrag der Konferenz der kantonalen Polizeikommandanten KKPKS

Januar 2023

Prof. Dr. Nora Markwalder, Universität St. Gallen
Lorenz Biberstein, Institut für Delinquenz und Kriminalprävention
Prof. Dr. Dirk Baier, Institut für Delinquenz und Kriminalprävention

Inhaltsverzeichnis

1 Einleitung 4

2 Methode 6

3 Ergebnisse 7

3.1 Cybercrime im engeren Sinn 7

3.2 Cybermobbing 9

3.3 Folgen der Viktimisierung mit Cybercrime und Cybermobbing 11

3.4 Weitere Delikte digitaler Kriminalität 12

4 Zusammenfassung 15

Literatur 17

1 Einleitung

Der Kriminalitätsbereich Cybercrime gehört zu den Zukunftsthemen der Kriminologie. In Zeiten allgemein rückläufiger Kriminalität weist dieser gewöhnlich ansteigende Zahlen auf. Problematisch ist, dass es derzeit «keine einheitliche Beschreibung bzw. Definition von Cybercrime» gibt (Huber 2019, S. 28). Welche Phänomene unter Cybercrime zu fassen sind, ist damit nicht verbindlich geregelt, wenngleich für die polizeiliche Registrierung von sog. «digitaler Kriminalität» in der Schweiz mittlerweile ein eigenes Kategoriensystem in Anwendung ist (s.u.). Hinzu kommt, dass es sich um einen sehr dynamischen Bereich handelt, der den Entwicklungen der Informationstechnik folgt, so dass immer wieder neue Verhaltensweisen zu beobachten und zu klassifizieren sind und dass die Unterscheidung von Cybercrime und Offline-Delikten zunehmenden verschwimmt, insofern Offline-Delikte inzwischen häufig auch Cyberelemente enthalten. Meist erfolgt in der wissenschaftlichen Untersuchung des Phänomens Cybercrime eine Fokussierung auf Organisationen oder Unternehmen als Opfer von Cybercrime-Angriffen (vgl. für die Schweiz u.a. Baier et al. 2022); Privatpersonen stehen meist nur dann, wenn es um spezifische Formen von Cybercrime geht (z.B. Cybermobbing bei Jugendlichen, z.B. Külling et al. 2022, S. 60ff; Cyberbullying bei Erwachsenen, vgl. z.B. Baier/Biberstein 2022) im Mittelpunkt des wissenschaftlichen Interesses. Dies ist sicherlich auch damit zu begründen, dass Privatpersonen teilweise gar nicht feststellen, dass sie Opfer von Cybercrime geworden sind.

Viktimisierungsbefragungen zu diesem spezifischen Kriminalitätsbereich sind in der Schweiz noch selten und messen hauptsächlich Cybercrime im engeren Sinn, d.h. «Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten» (Bundeskriminalamt 2019, S. 3). Biberstein et al. (2016) haben auf Basis des Crime Survey 2015, einer schweizweiten Repräsentativbefragung, Raten bzgl. der Betroffenheit von Cybercrime ermittelt, wobei nur eine Frage nach der Cybercrime-Viktimisierung gestellt wurde, die beinhaltete, ob man «Übergriffe im Internet, z.B. Phishing, Viren oder Missbrauch der eigenen Website oder des E-Mails» erlebt hat (S. 18). Insgesamt 6.6 % der Befragten gaben an, mindestens einen entsprechenden Übergriff in den zurückliegenden fünf Jahren erlebt zu haben, Männer häufiger als Frauen. Im Vergleich der Altersgruppen wurde kein signifikanter Unterschied der Viktimisierungsrate festgestellt. «Am häufigsten wurden die befragten Personen Opfer von Phishing (35.9 %), gefolgt von Viren (35.7 %)» (ebd. S. 19). Die Anzeigequote bei Übergriffen im Internet lag bei nur 3.9 %, was die zweitniedrigste Anzeigequote aller untersuchten Delikte war. Es ist insofern davon auszugehen, dass Dunkel- und Hellfeld in diesem Phänomenbereich weit auseinanderklaffen und primär über Dunkelfeldbefragungen Erkenntnisse zu diesem Deliktfeld erarbeitet werden können. Baier et al. (2022, S. 30) berichten auf Basis von Befragungen, die 2015, 2018 und 2021 durchgeführt wurden, Cybercrime-Viktimisierungsraten in Bezug auf ein Jahr in Höhe von 10,6, 11,5 und 10,7 %. Demnach hat es im Dunkelfeld keine Zunahme von Cybercrime-Delikten gegeben, wobei einschränkend festzuhalten ist, dass die Raten aufgrund einer unterschiedlichen Erfassung nur bedingt kompatibel sind. Auch 2021 bildeten dabei Phishing-Attacken die häufigste Form von Cybercrime, gefolgt von Sexting-Übergriffen; Angriff mittels Viren spielten hingegen keine bedeutsame Rolle mehr.[1]

Eine weitere Form vom Cybercrime ist das Cyberbullying bzw. Cybermobbing. Hierbei handelt es sich um eine Aggressionsform, die im Wesentlichen darauf angelegt ist, dem Ansehen einer Person zu schaden bzw. diese psychisch zu schädigen, wofür Anrufe, SMS, E-Mails, WhatsApp-Nachrichten, Postings usw. genutzt werden. Smith et al. (2008, S. 376) definieren dieses Verhalten als «an aggressive intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time

[1] Neben schweizweiten Befragungsstudien finden sich auch regionale Studien zum Thema Cybercrime-Opfererfahrungen. So berichten Milani et al. (2022) für die Stadt Lugano hohe Fünfjahresprävalenzraten für Cybercrime von 35 % (Virusattacke, Internetbetrug und unbefugte Verwendung von persönlichen Daten).

against a victim who cannot easily defend him or herself». Häufiger vorkommende Formen des Cybermobbing sind das Verspotten, das Beleidigen, das Bedrohen und das Gerüchte Verbreiten. Zusätzlich werden sexuelle Formen des Cyberbullying unterschieden. Auf Basis von zwei Repräsentativbefragungen für die Schweiz haben Baier und Biberstein (2022) kürzlich ermittelt, wie verbreitet entsprechende Opfererfahrungen unter Erwachsenen sind und ob es im Vergleich der Jahre 2018 und 2021 zu einem Anstieg gekommen ist. Festgestellt wird, dass die Cybermobbingjahresprävalenz von 8,1 auf 11,7 % signifikant gestiegen ist. Männliche Befragte berichten signifikant häufiger von solchen Erfahrungen als weibliche Befragte. Mit zunehmendem Alter geht die Online-Viktimisierung signifikant zurück. Zudem zeigt sich, dass arbeitslose Befragte signifikant häufiger Cybermobbing erlebt haben. Für andere Merkmale (Sprachregion, Migrationshintergrund, Bildungsniveau, Einwohnergrösse des Wohnorts) ergab sich hingegen kein Zusammenhang mit Cybermobbing-Erfahrungen.

In der Schweizerischen Kriminalstatistik, also im Polizeilichen Hellfeld, wird der Bereich Cybercrime seit dem Berichtsjahr 2020 gesondert als «digitale Kriminalität» ausgewiesen.[2] Hierzu zählen Straftaten, die in den Telekommunikationsnetzen und insbesondere im Internet begangen werden. Die Zuordnung zum Bereich «digitale Kriminalität» erfolgt dabei über das Tatvorgehen, wobei keine neuen Straftatbestände entwickelt wurden; stattdessen wird bei bestehenden Straftaten geprüft, inwieweit sie digital verübt wurden. Derzeit werden 28 Straftaten zum Bereich «digitale Kriminalität» gezählt. Die fünf im Jahr 2021 häufigsten Delikte in diesem Bereich waren Betrug, Geldwäscherei, betrügerischer Missbrauch einer Datenverarbeitungsanlage, Pornografie und Erpressung. Bei Betrugsdelikten wurden schweizweit 17'232 Delikte mit Modus operandi «digitale Kriminalität» erfasst; dies sind 76,3 % aller registrierten Betrugsdelikte. Auch bei anderen, «klassischeren» Cybercrime-Delikten findet sich ein hoher Anteil digital verübter Straftaten (Datenbeschädigung 90,7 %, Unbefugte Datenbeschaffung 72,2 %, Unbefugtes Eindringen in ein Datenverarbeitungssystem 68,4 %). Laut Polizeilicher Kriminalstatistik haben sich die Geschädigtenzahlen zu diesen Delikten, aber ebenso bspw. zum Betrug, zwischen 2015 (der letzten Durchführung eines schweizweiten Crimesurvey) und 2021 deutlich erhöht – teilweise mehr als verdoppelt (vgl. Markwalder et al. 2023).

Anliegen des Crime Survey 2022 war es, auf Basis einer umfassenden Bevölkerungsbefragung aktualisierte Befunde zum Dunkelfeld der Cybercrime-Opfererfahrungen unter Erwachsenen in der Schweiz zu erarbeiten. Im Folgenden werden die zentralen Befunde vorgestellt.

[2] Vgl. https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht/polizei/digitale-kriminalitaet.html

2 Methode

Der Crime Survey 2022 stellt eine repräsentative Befragung der Schweizer Wohnbevölkerung im Alter von 16 bis 80 Jahre dar. Anhand eines nationalen Registers wurde eine Zufallsstichprobe von 41'316 Personen gezogen, geschichtet nach Kanton und Altersgruppe (vgl. für detaillierte Ausführungen zum methodischen Vorgehen Markwalder et al. 2023). Diese Personen wurden Anfang Mai 2022 angeschrieben, mit der Bitte, an einer Online-Befragung teilzunehmen. Dem Schreiben waren ein personalisierter Zugangscode sowie ein Unterstützungsschreiben der entsprechenden kantonalen Polizei beigelegt. Neben dem Einladungsschreiben wurden zwei Erinnerungsschreiben verschickt. Der Online-Fragebogen lag in den drei Sprachen Deutsch, Französisch und Italienisch vor. Er wurde, wie das gesamte Vorgehen im Projekt, von der Ethikkommission der Universität St. Gallen gutgeheissen (Referenznummer: HSG-EC-20220411).

Von den verschickten Einladungsschreiben wurden 715 retourniert, weil die adressierte Person nicht unter der Adresse erreicht werden konnte; diese Adressen werden als stichprobenneutrale Ausfälle betrachtet. Die bereinigte Stichprobe umfasst daher 40'601 Personen, von denen 15'519 verwertbare Angaben gemacht haben; dies entspricht einer Rücklaufquote von 38,2 %, was vor dem Hintergrund des Verzichts auf einen Einsatz von Anreizen als gut eingestuft werden kann. Die Zusammensetzung der Stichprobe entspricht insbesondere hinsichtlich der Kantonsverteilung nicht den Verteilungen in der Grundgesamtheit, dies, weil bevölkerungskleinere Kantone bewusst bei der Stichprobenziehung überrepräsentiert wurden. Für Datenauswertungen auf nationaler Ebene wurde daher ein Anpassungsgewicht berechnet, welches die Stichprobe entlang der Merkmale Kantonszugehörigkeit, Geschlecht und Altersgruppe an die Grundgesamtheit anpasst. Im Folgenden werden ausschliessliche Befunde der entsprechend gewichteten Stichprobe vorgestellt.

Die gewichtete Stichprobe lässt sich wie folgt beschreiben:

- 50,0 % der Befragten sind weiblich, 50,0 % männlich; Befragte mit der Geschlechtsangabe «divers» wurden entsprechend ihres im nationalen Register vermerkten Geschlechts kategorisiert.
- 32,7 % der Befragten haben ein Alter ab 16 bis 36 Jahre, 38,2 % ein Alter ab 37 bis 57 Jahre und 29,1 % der Befragten ab 58 Jahre (bis 80 Jahre) an.
- 20,0 % der Befragten berichten davon, keine Schweizer Staatsangehörigkeit zu besitzen; Befragte mit doppelter Staatsangehörigkeit wurden als Schweizer Bürger:innen kategorisiert.
- 71,1 % Befragte gehören zur deutschsprachigen Region der Schweiz, 24,7 % zur französischsprachigen Region und 4,2 % zur italienischsprachigen Region.
- In eher ländlichen Gemeinden (unter 5'000 Einwohner:innen) wohnen 33,3 % der Befragten, in kleinstädtischen Gemeinden (ab 5'000 bis unter 20'000 Einwohner:innen) 37,0 % und in städtische Gemeinden (ab 20'000 Einwohner:innen) 29,7 %.

3 Ergebnisse

3.1 Cybercrime im engeren Sinn

In Anlehnung an die Studien von Dreißigacker und Riesner (2018) bzw. Müller et al. (2022) wurde die Viktimisierung mit Cybercrime-Delikten im engeren Sinn im Crime Survey 2022 wie folgt erhoben: «Im Folgenden geht es um Straftaten, die im Internet/den Sozialen Medien verübt werden und die sich gegen Ihren Internet-/Soziale-Medien-Zugang, Ihre Daten im Internet usw. richten.» Im Anschluss wurden verschiedene Delikte aufgeführt («Im Detail sind damit bspw. folgende Straftaten gemeint»), die in Tabelle 1 abgebildet sind. Zunächst sollte mitgeteilt werden, ob entsprechende Erfahrungen im Zeitraum 2017 bis 2022 gemacht wurden; wenn dies der Fall war, wurde eine Reihe an weiteren Fragen insbesondere in Bezug auf das zuletzt erlebte Delikt gestellt.

Die zentralen Ergebnisse zur Cybercime-Viktimisierung insgesamt lauten:

- 14,6 % der Befragten haben im Zeitraum 2017 bis 2022 mindestens ein Cybercrime-Delikt erlebt (Fünfjahresprävalenz; n = 2'114 von 14'437 Befragten mit gültiger Angabe); 6,6 % aller Befragten sind im genannten Zeitraum mehrfach viktimisiert worden (n = 951/14'437).
- In Bezug auf das Jahr 2021 gaben 6,2 % eine Viktimisierung mit Cybercrime-Delikten an (Einjahresprävalenz; n = 897/14'434).
- Die Anzeigerate bezogen auf das zuletzt erlebte Delikt beträgt 10,0 % (n = 203/2'033).[3] Von den Befragten, die das Erlebnis bei der Polizei gemeldet haben, gaben 26,5 % (n = 38/144) an, unzufrieden damit gewesen zu sein, wie die Polizei mit dem Vorfall umgegangen ist. Wenn Unzufriedenheit geäussert wurde, dann insbesondere wegen folgender Gründe: «Die Polizei konnte mir nicht helfen/das Problem wurde nicht gelöst» (n = 25) und «Die Polizei hat nichts/nicht genug gemacht, um mir zu helfen» (n = 10).

Zum zuletzt erlebten Delikt wurde erfragt, um welches Cybercrime-Delikt es sich konkret handelte.[4] Tabelle 1 zeigt, dass es sich bei 37,7 % der berichteten Delikte um das Hacking von E-Mail- oder Social-Media-Konten handelte. Am zweithäufigsten wurden Phishing-Attacken berichten (Daten ausspioniert). Der Datenverlust durch Viren usw. bzw. der Ransomwareangriff wurden deutlich seltener berichtet. 11,4 % gaben andere Delikte an, wobei sehr unterschiedliche Delikte, teilweise versuchte Delikte, angegeben wurden. Mittels der Frage nach der konkreten Form des zuletzt erlebten Cybercrime-Delikts lässt sich zudem eine Fünfjahresprävalenz für Einzeldelikte berechnen. Dabei ist allerdings anzumerken, dass die Raten eine Unterschätzung darstellen, weil Befragte, die mehrere Delikte erlebt haben, immer nur zu einem Delikt eine Angabe machten; wenn diese Befragten ein zweites, andere Delikt erlebt haben, müssten sie in die Berechnung der entsprechenden Fünfjahresprävalenzrate eingehen (und diese entsprechend erhöhen); da aber keine Angabe zu einem zweiten, dritten usw. erlebten Delikt vorliegen, kann dies bei der Berechnung der Raten nicht berücksichtigt werden. Wie Tabelle 1 zeigt, beträgt die Fünfjahresprävalenz beim Hacking von Konten 5,3 %; 3,7 % aller Befragten haben Phishing erlebt. Werden die Anzeigeraten für die Einzeldelikte betrachtet (ohne Abbildung), ergeben sich keine bedeutsamen Unterschiede: Die Anzeigerate variiert zwischen 6,4 % (Datenverlust durch Viren usw.) und 14,7 % (Ransomewareangriff).

[3] 33,5 % der zuletzt erlebten Delikte beziehen sich auf das Jahr 2022, 25,8 % auf das Jahr 2021, 12,8 % auf das Jahr 2020 und 27,9 % auf die Jahre 2017 bis 2019.

[4] Mehrfachantworten waren hier möglich, weil grundsätzlich ein Vorfall aus mehreren Delikten zusammengesetzt sein kann.

Tabelle 1: Fünfjahresprävalenzrate verschiedener Cybercrimedelikte (gewichtete Daten; n = 1'997)

Beschreibung im Fragebogen	Anteil in %	n	Fünfjahres-prävalenz
Mein Konto bei Sozialen Medien oder mein E-Mail-Konto wurde gehackt.	37.7	752	5.3
Meine vertraulichen Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern wurden durch gefälschte E-Mails oder Internetseiten ausspioniert.	26.7	533	3.7
Mein Onlinebanking wurde angegriffen/meine Kredit-/Debitkarteninformationen wurden online missbraucht.	22.2	443	3.1
Ich habe Datenverlust oder Datenbeschädigung durch Viren, Trojaner, Würmer erfahren.	14.5	290	2.0
Anderes	11.4	227	1.6
Der Zugang zu meinem Computer bzw. meinen mobilen Geräten wurde durch Schadsoftware gesperrt und ich wurde aufgefordert, Geld zu bezahlen, damit ich wieder auf alles zugreifen kann (sog. Ransomwareangriff).	9.8	195	1.4

Um zu prüfen, ob sich das Risiko, Opfer von Cybercrime-Delikten zu werden, zwischen verschiedenen Bevölkerungsgruppen unterscheidet, wurde eine binär-logistische Regressionsanalyse berechnet, in die verschiedene Merkmale gleichzeitig eingeschlossen wurden. Tabelle 2 berichtet die Ergebnisse; Koeffizienten über 1 indizieren, dass ein Merkmal das Risiko der Opferwerdung erhöht (Fünfjahresprävalenz), Koeffizienten unter 1, dass ein Merkmal dieses Risiko senkt. Von Bedeutung sind dabei jene Koeffizienten, die als signifikant ausgewiesen werden. Insgesamt gibt es nur wenig signifikante Beziehungen, was bedeutet, dass das Risiko der Opferwerdung kaum mit sozio-demografischen Merkmalen variiert; oder anders ausgedrückt: Opfer von Cybercrime kann mehr oder weniger jeder werden, typische Opfermerkmale lassen sich bei diesem Delikt eher nicht identifizieren. Es gilt primär, dass Personen der ältesten Altersgruppe am seltensten eine Viktimisierung berichten (und Personen der mittleren Altersgruppe an häufigsten)[5] und dass Personen aus höheren Einkommensgruppen[6] bzw. mit höherer Bildung[7] häufiger Opfer werden, möglicherweise weil sie entsprechende Delikte häufiger registrieren (aufgrund höherer Bildung) oder weil sie attraktivere Ziele (höheres Einkommen) darstellen. In der französischsprachigen Schweiz liegt die Viktimisierungsrate zudem höher als in der deutschsprachigen Schweiz; in der italienischsprachigen Schweiz liegt sie niedriger.[8]

[5] Die Fünfjahresprävalenzraten lauten: 16 bis 36 Jahre 14,9 %, 37 bis 57 Jahre 17,0 %, 58 bis 80 Jahre 11,4 %.

[6] Die Viktimisierungsrate der untersten Einkommensgruppe (weniger als 2'500 CHF) liegt bei 11,2 %, der höchsten Einkommensgruppe (über 7'500 CHF) bei 16,8 %. Von allen Befragten gehören 45,5 % zur Gruppe mit dem höchsten Einkommen, 6,1 % zur Gruppe mit dem geringsten Einkommen (vgl. Markwalder et al. 2023).

[7] Unterschieden wurden Personen mit niedriger/mittlerer Bildung (62,1 % der Stichprobe) und Personen mit hoher Bildung (Matur/Abitur oder Studium; 37,9 % der Stichprobe). Befragte mit niedriger/mittlerer Bildung erlebten zu 13,2 % Cybercrime im Zeitraum 2017 bis 2022, Befragte mit hoher Bildung zu 16,9 %.

[8] Die Raten lauten: deutschsprachige Schweiz 14,0 %, französischsprachige Schweiz 17,1 %, italienischsprachige Schweiz 11,0 %.

Tabelle 2: Sozio-demografische Merkmale als Einflussfaktoren von Cybercrime-Viktimisierung (Fünfjahresprävalenzrate; binär-logistische Regression; abgebildet Exp(B); gewichtete Daten)

		Fünfjahresprävalenz	
Geschlecht	männlich	1.070	
Alter	16-36 Jahre	Referenz	
	37-57 Jahre	1.149	*
	58-80 Jahre	0.733	***
Staatsangehörigkeit	Ausland	0.839	*
Sprachregion	Deutschsprachige Schweiz	Referenz	
	Französischsprachige Schweiz	1.282	***
	Italienischsprachige Schweiz	0.741	*
Gemeindegrösse	ländlich (unter 5000 Einwohner)	Referenz	
	kleinstädtisch (unter 20000 Einwohner)	0.978	
	städtisch (ab 20000 Einwohner)	0.965	
Bildung	hoch	1.197	**
Monatliches Haushalts-Nettoeinkommen	weniger als 2500 CHF	Referenz	
	weniger als 5000 CHF	1.320	*
	weniger als 7500 CHF	1.394	*
	mehr als 7500 CHF	1.529	**
N		**12041**	
Nagelkerkes R^2		**0.018**	

* p < .05, ** < .01, *** p < .001

3.2 Cybermobbing

Neben Cybercrime im engeren Sinn wurde spezifisch nach dem Erleben von Cybermobbing gefragt. Im Fragebogen wurde dieser Fragekomplex wie folgt eingeleitet: «Im Folgenden geht es um Beleidigungen, Belästigungen usw., die über das Internet/die Sozialen Medien ausgeführt werden.» Auch hier wurden zusätzlich verschiedene Einzeldelikte aufgeführt, damit die Befragten eine konkretere Vorstellung erhalten, welche Übergriffe gemeint sind («Im Detail sind damit bspw. folgende Verhaltensweisen gemeint»; vgl. Tabelle 3). Neben der Fünfjahresprävalenz (Viktimisierung im Zeitraum 2017 bis 2022) wurden wiederum Fragen zum zuletzt erlebten Delikt gestellt, wobei hier auch – im Unterschied zu Cybercrime im engeren Sinn – nach der Täterschaft gefragt wurde, weil davon ausgegangen werden konnte, dass zumindest teilweise die Täter:innen bekannt sind.

Werden wiederum zunächst die Gesamtraten betrachtet, zeigt sich folgendes Bild zum Cybermobbing:

- 3,0 % der Befragten haben im Zeitraum 2017 bis 2022 mindestens einmal Cybermobbing erlebt (n = 440/14'824); in zwei von drei Fällen handelt es sich dabei um Mehrfachopfer, insofern die Mehrfachopfer-Gesamtrate 2,0 % beträgt (n = 293/14'824).
- In Bezug auf das Jahr 2021 gaben 1,4 % eine Cybermobbing-Viktimisierung an (n = 211/14'824).
- Die Anzeigerate bezogen auf das zuletzt erlebte Delikt beträgt 5,2 % (n = 22/432).[9] Von den Befragten, die das Erlebnis bei der Polizei gemeldet haben, gaben 78,3 % (n = 15/19) an, unzufrieden damit gewesen zu sein, wie die Polizei mit dem Vorfall umgegangen ist. Als Grund wurde dabei häufiger genannt «Die Polizei konnte mir nicht helfen/das Problem wurde nicht gelöst».

[9] 38,1 % der zuletzt erlebten Cybermobbing-Delikte beziehen sich auf das Jahr 2022, 22,7 % auf das Jahr 2021, 14,0 % auf das Jahr 2020 und 25,2 % auf die Jahre 2017 bis 2019.

Bei den Cybermobbing-Delikten handelt es sich zu 62,0 % um Beleidigungen, Beschimpfungen usw. (Tabelle 3); in 37,1 % wurden Gerüchte verbreitet.[10] Werden auf Basis der Angaben Fünfjahresprävalenzen berechnet, so ist erneut darauf hinzuweisen, dass diese Unterschätzungen darstellen, gerade vor dem Hintergrund des hohen Anteils an mehrfach viktimisierten Personen. Im Zeitraum 2017 bis 2022 haben daher mindestens 1,7 % Beleidigungen usw. über Internet/Soziale Medien erfahren, mindestens 1,0 % das Verbreiten von Gerüchten. Für die verschiedenen Subdelikte von Cybermobbing gilt dabei ebenfalls, dass die Anzeigerate nicht bedeutsam zwischen 4,7 % (Beleidigungen usw.) und 9,4 % (Blossstellen) variiert.

Tabelle 3: Fünfjahresprävalenzrate verschiedener Cybermobbingdelikte (gewichtete Daten; n = 411)

Beschreibung im Fragebogen	Anteil in %	n	Fünfjahresprävalenz
Jemand hat mich online verspottet, beleidigt, beschimpft oder bedroht.	62.0	255	1.7
Jemand hat online Gerüchte über mich verbreitet oder schlecht über mich geredet.	37.1	152	1.0
Anderes	15.2	62	0.4
Jemand hat private Nachrichten, vertrauliche Informationen, Fotos oder Videos von mir ins Internet gestellt bzw. im Internet versendet, um mich blosszustellen oder lächerlich zu machen.	13.6	56	0.4
Jemand hat Fotos/Videos von mir verschickt, auf denen ich nackt zu sehen bin oder mich zu sexuellen Handlungen aufgefordert (z.B., dass ich mir vor der Web-Cam ausziehe)	11.3	47	0.3

Auf die Frage, ob die Tatperson bekannt war, gaben 15,3 % der Befragten an, dass sie die Tatperson nicht gesehen haben, 46,2 % kannten die angreifende Person nicht. Dies bedeutet, dass nur etwa ein Drittel (38,5 %) der Befragten angaben, Angaben zur Tatperson machen zu können (n = 169). Am häufigsten wurden von diesen «andere Personen» als Täter:in benannt (ehem. Schulkolleg:innen, Bekannte), gefolgt von «Schüler:in, Student:in, «eng:er Freund:in», «(damalig:er) Ex-Freund:in», «Person aus Nachbarschaft» und «Arbeitskolleg:in». Weitere Personengruppen (z.B. häusliches Umfeld, Vorgesetzte, Lehrer:in) wurden kaum benannt.

Auch in Bezug auf das Cybermobbing wurde mittels binär-logistischen Regressionsanalysen geprüft, inwieweit verschiedene sozio-demografische Gruppen stärker bzw. weniger stark belastet sind (Fünfjahresprävalenz). Die Ergebnisse sind in Tabelle 4 dargestellt, wobei sich auch bei diesem Delikt nur wenige Zusammenhänge zeigen. Mit zunehmendem Alter sinkt das Risiko, Opfer von Cybermobbing zu sein.[11] Eine ausländische Staatsangehörigkeit steht mit geringerer Viktimisierung in Verbindung.[12] Zudem zeigt sich, dass ein höheres Einkommen mit selteneren Erfahrungen mit Cybermobbing einhergeht.[13]

[10] Auch hier waren Mehrfachantworten möglich.
[11] Die Fünfjahresprävalenzraten lauten: 16 bis 36 Jahre 4,8 %, 37 bis 57 Jahre 2,3 %, 58 bis 80 Jahre 1,8 %.
[12] Befragte mit Schweizer Staatsangehörigkeit weisen eine Prävalenzrate von 3,1 % auf, Befragte mit ausländischer Staatsangehörigkeit eine Rate von 2,4 %.
[13] Die Viktimisierungsrate der untersten Einkommensgruppe (weniger als 2'500 CHF) liegt bei 5,7 %, der höchsten Einkommensgruppe (über 7'500 CHF) bei 2,6 %.

Tabelle 4: Sozio-demografische Merkmale als Einflussfaktoren von Cybermobbing-Viktimisierung (Fünfjahresprävalenzrate; binär-logistische Regression; abgebildet Exp(B); gewichtete Daten)

		Fünfjahresprävalenz	
Geschlecht	männlich	1.039	
Alter	16-36 Jahre	Referenz	
	37-57 Jahre	0.562	***
	58-80 Jahre	0.411	***
Staatsangehörigkeit	Ausland	0.691	*
Sprachregion	Deutschsprachige Schweiz	Referenz	
	Französischsprachige Schweiz	0.853	
	Italienischsprachige Schweiz	0.843	
Gemeindegrösse	ländlich (unter 5000 Einwohner)	Referenz	
	kleinstädtisch (unter 20000 Einwohner)	1.160	
	städtisch (ab 20000 Einwohner)	1.001	
Bildung	hoch	1.102	
Monatliches Haushalts-Nettoeinkommen	weniger als 2500 CHF	Referenz	
	weniger als 5000 CHF	0.649	*
	weniger als 7500 CHF	0.469	***
	mehr als 7500 CHF	0.483	***
N		**12357**	
Nagelkerkes R^2		**0.027**	

* p < .05, ** < .01, *** p < .001

3.3 Folgen der Viktimisierung mit Cybercrime und Cybermobbing

Anliegen des Crime Survey 2022 war in erster Linie, Prävalenzraten zu verschiedenen Delikten zu erarbeiten, um das Dunkelfeld der Kriminalität aufzuhellen. Es ging in der Befragung weniger darum, Zusammenhänge zwischen verschiedenen Merkmalen, so z.B. mögliche Folgeerscheinungen von Viktimisierungserfahrungen, zu prüfen. Aus diesem Grund wurde nur eine begrenzte Anzahl an Merkmalen für entsprechende Auswertungen erfasst. Unter Verwendung von zwei Merkmalen soll im Folgenden geprüft werden, inwieweit Cybercrime- bzw. Cybermobbing-Viktimisierungen folgenreich für die psychische Konstitution der Opfer sind. Im Fragebogen wurde einerseits mittels der Frage «Ganz allgemein gefragt: Wie zufrieden sind Sie mit Ihrem Leben?» die Lebenszufriedenheit erhoben (Antwortvorgaben: 0 = gar nicht zufrieden, 10 = vollumfänglich zufrieden). Andererseits wurde das Sicherheitsgefühl mit der Frage «Wie sicher fühlen Sie sich, wenn Sie nach Einbruch der Dunkelheit allein in Ihrer Wohngegend zu Fuss unterwegs sind?» ermittelt (Antwortvorgaben: 1 = sehr unsicher, 4 = sehr sicher).

Tabelle 5 stellt Ergebnisse von OLS-Regressionen vor, die sowohl den Einfluss von Cybercrime-/Cybermobbing-Erfahrungen als auch den Einfluss verschiedener sozio-demografischer Merkmale gleichzeitig auf die beiden Folgevariablen prüft. Die abgebildeten Koeffizienten können Werte zwischen 0 und +1 bzw. -1 annehmen; je grösser der Koeffizient ausfällt, umso stärker erhöht (positive Werte) bzw. senkt (negative Werte) ein Merkmal die Lebenszufriedenheit bzw. das Sicherheitsgefühl. Entscheidend in Tabelle 5 sind die Koeffizienten zur Cybercrime- bzw. Cybermobbing-Viktimisierung: Diese fallen negativ und signifikant aus und haben in etwa die gleiche Höhe. Das Erleben beider Formen der Viktimisierung reduziert damit in bedeutsamer Weise die Lebenszufriedenheit und das Sicherheitsgefühl. Die Stärke der Koeffizienten ist gleichwohl als gering einzustufen.

Jenseits dieser Befunde zeigt sich, dass männliche Befragte etwas weniger mit ihrem Leben zufrieden sind als weibliche Befragte, aber ein deutlich höheres Sicherheitsgefühl aufweisen. Ältere Befragte sind zufriedener mit ihrem Leben; hinsichtlich des Sicherheitsgefühls gilt, dass sich die mittlere Altersgruppe etwas sicherer fühlt als die jüngste Altersgruppe, die älteste Altersgruppe aber das geringste Sicherheitsgefühl äussert. Weitere erwähnenswerte Befunde ergeben sich mit Blick auf die Gemeindegrösse: Mit zunehmender Gemeindegrösse wird weniger Lebenszufriedenheit und ein geringeres Sicherheitsgefühl angegeben. Höher gebildete sowie Befragte mit höherem Einkommen fühlen sich signifikant sicherer; zudem steigt mit dem Einkommen auch die Lebenszufriedenheit.

Tabelle 5: Zusammenhänge zwischen Cybercrime- und Cybermobbing-Viktimisierung und möglichen Folgen (OLS-Regressionen; abgebildet: Beta-Koeffizienten; gewichtete Daten)

		Lebenszufriedenheit		**Sicherheitsgefühl nach Einbruch der Dunkelheit allein in Wohngegend**	
Geschlecht	männlich	-.03	**	.22	***
Alter	16-36 Jahre	Referenz		Referenz	
	37-57 Jahre	.08	***	.03	**
	58-80 Jahre	.22	***	-.03	**
Staatsangehörigkeit	Ausland	-.01		-.01	
Sprachregion	Deutschsprachige Schweiz	Referenz		Referenz	
	Französischsprachige Schweiz	-.04	***	-.01	
	Italienischsprachige Schweiz	-.04	***	-.01	
Gemeindegrösse	ländlich (unter 5000 Einwohner)	Referenz		Referenz	
	kleinstädtisch (unter 20000 Einwohner)	-.03	**	-.08	***
	städtisch (ab 20000 Einwohner)	-.05	***	-.12	***
Bildung	hoch	.01		.14	***
Haushalts-Nettoeinkommen	weniger als 2500 CHF	Referenz		Referenz	
	weniger als 5000 CHF	.11	***	.02	
	weniger als 7500 CHF	.21	***	.06	***
	mehr als 7500 CHF	.33	***	.10	***
Fünfjahresprävalenz Cybercrime		-.06	***	-.04	***
Fünfjahresprävalenz Cybermobbing		-.06	***	-.05	***
N		**11756**		**11884**	
korr. R^2		**0.085**		**0.096**	

* p < .05, ** < .01, *** p < .001

3.4 Weitere Delikte digitaler Kriminalität

Im Rahmen des Crime Surveys 2022 wurden neben Cybercrime- und Cybermobbing-Viktimisierung weitere Viktimisierungen mit strafbarem Verhalten erhoben. Bei einigen wenigen Delikten wurde mittels einer Nachfrage zum zuletzt erlebten Vorfall der Ort des Übergriffs erhoben. Dabei wurde, neben anderen standardisiert präsentierten Ortsangaben, auch der Ort «Im Internet / in den Sozialen Medien» erhoben. Dies ermöglicht, in vergleichbarer Form, wie dies in der Schweizerischen Polizeilichen Kriminalstatistik geschieht, nicht nur Delikte auszuweisen, die genuine Cyberdelikte darstellen, sondern auch solche, bei denen die Tatausübung gleichwohl digital erfolgt (sog. Cyberdelikte im weiteren Sinn[14]). Ein

[14] Für die Unterscheidung zwischen cyber-enabled crimes (im weiteren Sinn) und cyber-dependent crimes (im engeren Sinn) vgl. u.a. Caneppele et al. (2019).

Beispiel wären Betrugsdelikte, die mittlerweile zum Grossteil über Internet/Soziale Medien verübt werden. Allerdings wurde im Crime Survey 2022 bei Betrugsdelikten oder Erpressungen keine Nachfrage nach dem Ort gestellt, weshalb der Anteil digital verübter Delikte nicht berechnet werden kann; beim Betrug wurden allerdings verschiedene Subdelikte erhoben, so dass zumindest Online-Anlagebetrug als eine Form des digitalen Betrugs betrachtet werden kann.

Wie Tabelle 6 zeigt, lassen sich zu fünf weiteren Delikten Fünfjahresprävalenzraten zu digital erlebten Delikten berechnen. Da diese auf den Angaben zum zuletzt erlebten Delikt beruhen, ist auch hier wieder zu beachten, dass es sich um Unterschätzungen handelt. Die höchste Prävalenzrate zeigt sich beim Online-Anlagebetrug: Insgesamt 4,8 % aller Befragten bestätigten, dass sie in den Jahren 2017 bis 2022 erlebt haben, dass sie jemand online zu Geldanlagen auf gefälschten Anlageplattformen überreden wollte. Ebenfalls eine höhere Rate findet sich beim Stalking: 3,4 % aller Befragten haben digital ausgeführte Stalking-Handlungen in den letzten fünf Jahren erlebt. Von digital ausgeübten sexuellen Belästigungen berichten 1,3 % der Befragten, digital ausgeführten Drohungen 0,8 %, von digital ausgeführten Hate-Crime-Handlungen 0,6 %.

Tabelle 6: Fünfjahresprävalenzrate «digitale Kriminalität» bei verschiedenen Delikten (gewichtete Daten)

Delikt	Beschreibung im Fragebogen	Fünfjahres-prävalenz	Fünfjah-resprä-valenz di-gitale Kri-minalität	n
Betrug/ Online-Anlage-betrug	Jemand möchte Sie Online zu Geldanlagen auf gefälschten Anlageplattformen überreden	Betrug: 18.3	**Anlagebe-trug: 4.8**	710/14725
Stalking	Im Folgenden geht es um das sog. Stalking, d.h. dass eine Person (z.B. Ex-Partner:in, Be-kannt:er, Fremd:er) Sie wiederholt belästigt oder verfolgt hat.	5.0	**3.4**	511/15048
sexuelle Belästigung	Es gibt Leute, die aus sexuellen Gründen manchmal andere Menschen in einer anstössi-gen oder belästigenden Art ansprechen, an-schreiben, anfassen oder berühren oder sich vor ihnen entblössen.	10.7	**1.3**	194/15061
Drohungen	Manchmal bedrohen einen andere Leute in einer beängstigenden Art und Weise.	10.7	**0.8**	123/14875
Hate Crime	Wurden Sie Opfer irgendeiner Straftat oder ir-gendeines Übergriffs, wie beispielsweise einer Beleidigung, wegen Ihrer Hautfarbe, Ihrer Her-kunft/Nationalität/Sprache, Ihres Geschlechts, Ihrer sexuellen Orientierung, Ihrer politischen Weltanschauung, Ihrer Religion, Ihrer Behinde-rung oder Erkrankung, Ihres körperlichen Ausse-hens, Ihres sozialen Status/Ihrer finanziellen Si-tuation, Ihres Berufs oder Ihres Alters?	6.6	**0.6**	86/14703

Bei den Delikten «sexuelle Belästigung», «Drohungen» und «Hate Crime» wurde der Anteil digitaler Kriminalität auf Basis der Ortsangabe «Im Internet / in den Sozialen Medien» zum zuletzt erlebten Vorfall bestimmt. Beim «Stalking» wurden die Angaben «unerwünscht E-Mails, SMS, Chat-Nachrichten usw. geschrieben» und «mich im Internet/den sozialen Medien verfolgt» als Antworten auf die Frage zum letzten Vorfall «In welcher Weise wurde das Stalking ausgeführt?» herangezogen. Beim Betrug gab es keine Nachfrage nach dem Tatort; hier wurde als ein mögliches online Betrugsdelikt aber explizit der «Online-Anlagebetrug» aufgeführt (wiederum bezogen auf den letzten erlebten Betrugsvorfall).

Zusätzlich in Tabelle 6 dargestellt ist die Prävalenzrate der verschiedenen Delikte ohne Berücksichtigung des Tatorts. So gilt, dass 10,7 % der Befragten im Zeitraum 2017 bis 2022 irgendeine Form sexueller Belästigung erlebt haben; 18,3 % der Befragten haben irgendeine Form des Betrugs erlebt. Das Verhältnis der beiden Raten gibt dann Aufschluss darüber, in welchem Deliktsbereich der Anteil digital

verübter Delikte besonders hoch ausfällt. Dies ist vor allem beim Stalking der Fall: Zwei von drei Befragten, die Stalking erlebt haben, haben dies auf digitalen Wegen erlebt (3,4 von 5,0 %). Bei Drohungen und Hate Crime ist dieser Anteil deutlich geringer, d.h. diese Delikte scheinen sich noch mehrheitlich in der Offline-Welt zuzutragen (oder werden, wenn sie dort ausgeführt werden, als entsprechende Delikte erlebt). Die Auswertungen unterstreichen anhand der fünf Deliktsbereiche, dass digitale Kriminalität kein klar abgegrenztes Phänomen darstellt, sondern dass verschiedene Delikte zunehmend digital ausgeführt werden. Dies ist bei zukünftigen Viktimisierungsbefragungen noch stärker zu berücksichtigen und durch entsprechende Nachfragen sichtbar zu machen.

4 Zusammenfassung

Die Ergebnisse haben gezeigt, dass Erfahrungen digitaler Kriminalität in der Bevölkerung keine Seltenheit darstellen. Jeder siebte Befragte (14,6 %) berichtet Viktimisierungen mit Cybercrime im engeren Sinn; dieser Anteil liegt deutlich höher als in im Crime Survey 2015, wo 6,6 % der Befragte solche Erlebnisse berichteten (Biberstein et al. 2016). Dabei fällt der Anstieg sogar noch stärker aus, als die beiden Zahlen dies aufzeigen, da im Crime Survey 2015 Cybermobbing in die Prävalenzrate eingeht, im Crime Survey 2022 hingegen nicht. Es lässt sich damit klar feststellen, dass Cybercrime auch im Dunkelfeld ein zunehmendes Problem darstellt. Dabei zeichnen sich gewisse Verschiebungen ab: Während in der Befragung 2015 Phishing und Viren noch gleichermassen bedeutsame Formen der Cybercrime-Viktimisierung darstellten, findet sich im Jahr 2022, dass Schäden durch Viren deutlich seltener genannt wurden; am häufigsten kommt hingegen das Hacking von E-Mail- und Social-Media-Konten vor. Erklärbar ist dies möglicherweise damit, dass die Menschen verstärkt für die Virenthematik sensibilisiert sind und Vorkehrungen treffen; und im gleichen Masse, wie Soziale Medien für die Menschen relevant werden (verbunden mit der Eröffnung entsprechender Konten), werden diese zu Zielen von Cyberangriffen.

Ein Grossteil dieser Kriminalität verbleibt dabei im Dunkelfeld. Zwar erhöht sich die Anzeigerate im Vergleich zu 2015, wo sie 4,0 % betrug (Baier et al. 2022, S. 29), auf mittlerweile 10,0 %; dies bedeutet aber, dass weiterhin neun von zehn Delikten nicht der Polizei zur Kenntnis gelangen. Cybermobbing wird zudem weiterhin kaum angezeigt – die Anzeigerate beträgt hier 5,2 %. Diesbezüglich hat sich zudem ein wichtiger Handlungsbedarf ergeben: Auch wenn die Fallzahlen aufgrund der geringen Anzeigerate gering sind, fällt auf, dass acht von zehn Befragten, die Erlebnisse von Cybermobbing zur Anzeige gebracht haben, nicht zufrieden damit sind, wie die Polizei in der Folge damit umgegangen ist.

Vor dem Hintergrund des eingangs geschilderten Forschungsstandes ist ein Ergebnis der Auswertungen überraschend: Der Anteil an Befragten, die Cybermobbing erlebt haben, fällt mit 3,0 % im Zeitraum 2017 bis 2022 eher gering aus. Eine Erklärung hierfür zu finden, ist schwierig. Auch die Studie von Baier und Biberstein (2022) basiert auf bevölkerungsrepräsentativen Stichproben, beinhaltet also auch ältere Befragte, die dieses Delikt seltener erleben. In der Studie von Baier und Biberstein (2022) gaben zuletzt 11,7 % der Befragten Cybermobbing-Erfahrungen an – und dies bezogen auf die letzten zwölf Monate. Möglicherweise wurden im Crime Survey 2022 vor allem schwerere Delikte berichtet; ein Hinweis hierfür ist der hohe Mehrfachviktimisiertenanteil, der andeutet, dass Befragte eher dann Delikte angegeben haben, wenn sie häufiger waren (und damit in der Summe auch schwerer). Ein deutlicher Unterschied zu Baier und Biberstein (2022) ist, dass Cybermobbing 2022 mit einem Item abgefragt wurde, nicht mit drei Items, wobei die Inhalte letztlich aber sehr ähnlich waren. Methodische Aspekte, die das Antwortverhalten von Befragten beeinflussen, könnten daher ebenfalls ausschlaggebend für die Diskrepanzen sein. Dies bedeutet, dass Fragen möglichst wenig geändert werden sollten, um Vergleichbarkeit zu anderen oder zu früheren Studien zu gewährleisten.

Nochmals zu erwähnen sind schliesslich die Befunde der multivariaten Auswertungen. Diese haben einerseits gezeigt, dass die Cybercrime- bzw. Cybermobbing-Opferwerdung kaum mittels sozio-demografischen Merkmalen vorhergesagt werden kann. Es finden sich zwar einige Unterschiede zwischen Befragtengruppen, die aber nicht immer einheitlich bei den beiden betrachteten Delikten ausfallen; zudem ist die erklärte Varianz der Modelle eher gering, was verdeutlicht, dass sozio-demografische Merkmale keinen substanziellen Einfluss haben. Cyber-Viktimisierungen können mehr oder weniger jeden treffen bzw. es müssten andere Merkmale, bspw. die Online-Routineaktivitäten, erfasst und geprüft werden. Cyberdelikte scheinen somit mehr von situativen Faktoren abhängig zu sein, weshalb sich in diesem Kontext auch ein Blick auf situative Präventionsmassnahmen wie etwa das Erschweren der Tatbegehung oder Reduktion des Gewinns durch einen besseren Schutz der Tatobjekte lohnen kann (Clarke/Mayhew 1980). Andererseits konnte mittels multivariater Auswertungen belegt werden, dass

Cyber-Viktimisierungen als Formen krimineller Opfererfahrungen ernstzunehmen sind. Sie reduzieren die Lebenszufriedenheit und ebenso das Sicherheitsgefühl im öffentlichen Raum (als im Offline-Raum). Die Zusammenhänge sind nicht sehr stark, aber signifikant. Opfer von Cybercrime und Cybermobbing benötigen mit Blick auf die Verarbeitung dieser Delikte mithin Unterstützung.

Literatur

Baier, D., Biberstein, L. (2022). Cyberbullying-Erfahrungen Erwachsener in der Schweiz vor und während der Covid-19-Pandemie. Kriminalistik 76, 506-509.

Baier, D., Biberstein, L., Markwalder, N. (2022). Kriminalitätsopfererfahrungen der Schweizer Bevölkerung. Entwicklungen im Dunkelfeld 2011 bis 2021. Zürich: Zürcher Hochschule für Angewandte Wissenschaften.

Biberstein, L., Killias, M., Walser, S., Iadanza, S., Pfammater, A. (2016). Studie zur Kriminalität und Opfererfahrungen der Schweizer Bevölkerung. Analysen im Rahmen der schweizerischen Sicherheitsbefragung 2015. Lenzburg: Killias Research & Consulting.

Bundeskriminalamt (2019). Cybercrime. Bundeslagebild 2018. Wiesbaden.

Caneppele, S., Aebi, M.F. (2019. Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. Policing: A Journal of Policy and Practice 13, 66-79.

Clarke, R.V., Mayhew, P. (Eds.) (1980). Designing out Crime. London: HMSO

Dreißigacker, A., Riesner, L. (2018). Private Internetnutzung und Erfahrungen mit computerbezogener Kriminalität. Ergebnisse der Dunkelfeldstudien des Landeskriminalamtes Schleswig-Holstein 2015 und 2017. Forschungsbericht Nr. 139 Hannover: Kriminologisches Forschungsinstitut Niedersachsen.

Huber, E. (2019). Cybercrime. Eine Einführung. Wiesbaden: Springer.

Külling, C., Waller, G., Suter, L., Willemse, I., Bernath, J., Skirgaila, P., Streule, P., Süss, D. (2022). JAMES – Jugend, Aktivitäten, Medien – Erhebung Schweiz. Zürich: Zürcher Hochschule für Angewandte Wissenschaften.

Markwalder, N., Biberstein, L., Baier, D. (2023). Opfererfahrungen und sicherheitsbezogene Einschätzungen der Schweizer Bevölkerung. Ergebnisse des Crime Survey 2022.

Milani, R., Caneppele, S., Burkhardt, C. (2022). Exposure to Cyber Victimization:Results from a Swiss Survey. Deviant Behavior 43, 228-240.

Müller, P., Dreißigacker, A. Isenhardt, A. (2022). Cybercrime gegen Privatpersonen. Ergebnisse einer repräsentativen Bevölkerungsbefragung in Niedersachsen. KFN-Forschungsberichte Nr. 168. Hannover: KFN.

Smith, P.K., Mahdavi, J., Carvalho, M., Fisher, S., Russell, S., Tippett, N. (2008). Cyberbullying: Its nature and impact in secondary school pupils. Journal of Child Psychology and Psychiatry 49, 376-385.

Zürcher Hochschule
für Angewandte Wissenschaften

Universität St. Gallen
Kompetenzzentrum für Strafrecht und Kriminologie
Bodanstrasse 3
CH-9000 St.Gallen
https://www.unisg.ch/de/universitaet/schools/law/forschung/sk-hsg

Departement Soziale Arbeit
Institut für Delinquenz und Kriminalprävention
Pfingstweidstrasse 96
Postfach 707
CH-8005 Zürich
www.zhaw.ch/sozialearbeit