

Hackerprofile: Cyberkriminalität und die Dunkle Triade der Persönlichkeit

Dissertation

der Mathematisch-Naturwissenschaftlichen Fakultät

der Eberhard Karls Universität Tübingen

zur Erlangung des Grades eines

Doktors der Philosophie

(Dr. phil.)

vorgelegt von

Mark T. Hofmann

aus Frankfurt am Main

Tübingen

2025

Gedruckt mit Genehmigung der Mathematisch-Naturwissenschaftlichen Fakultät der
Eberhard Karls Universität Tübingen.

Tag der mündlichen Qualifikation:

23.03.2026

Dekan:

Prof. Dr. Thilo Stehle

1. Berichterstatter/-in:

Prof. Dr. Martin Hautzinger

2. Berichterstatter/-in:

Prof. Dr. Dr. h.c. mult. Niels Birbaumer

3. Berichterstatter/-in:

Prof. Dr. Stephan Schwan

„Empathy is conditional for me, and I don't feel guilt. I understand emotion much more than I feel it.”

Auszug Hacker Interview (BH10, Z. 189-190)

Für meine Eltern.

Danksagung

Psychopathie, Narzissmus und Machiavellismus bei Hackern außerhalb des Strafvollzugs zu untersuchen, ist ein zeitgemäßes Thema, aber auch ein sehr schwieriges Vorhaben, das ohne das Vertrauen und die Unterstützung einer Reihe von Personen nicht möglich gewesen wäre.

Mein besonderer Dank gilt daher meinen Betreuern Prof. Dr. Martin Hautzinger und Prof. Dr. Dr. h.c. mult. Niels Birbaumer für ihre wissenschaftliche Begleitung, ihren kritischen Blick und das Vertrauen, meinen ganz eigenen Weg in diesem speziellen Forschungsfeld zu gehen. Sie haben mir wertvolle Impulse, Freiraum und Geduld geschenkt und auch ermutigt und darin bestärkt, neue Wege zu gehen, um neue Erkenntnisse zu generieren. Für die Chance und das Vertrauen, dieses Forschungsvorhaben in Form einer Dissertation umzusetzen, möchte ich mich bedanken!

Ebenfalls möchte ich meinen Eltern und meiner Familie danken. Zwei Dinge sollen Kinder von ihren Eltern bekommen, soll Goethe einmal gesagt haben: Flügel und Wurzeln. Ich möchte meinen Eltern für die Flügel und Wurzeln danken. Ihr Vertrauen, ihre Unterstützung und ihre Werte sind das Fundament, auf dem alles ruht.

Meiner Partnerin gilt mein tiefster Dank. Sie war das ‚Licht‘ nach Recherchen und Forschung im Darknet. Die Geduld, die sie mir entgegengebracht hat und ihr Glaube an mich haben diese Arbeit ermöglicht.

Kriminelle Hacker in Hacker-Foren agieren strikt anonym oder pseudonym. Es war zu Beginn des Forschungsvorhabens keineswegs klar, ob es überhaupt gelingen würde, auch Black Hat Hacker für eine Teilnahme an empirischen Studien zu gewinnen. Es war einer der ersten Versuche und ist gelungen. Obwohl ich und die meisten der untersuchten Probanden auf unterschiedlichen Seiten stehen, gilt mein Dank auch den Black Hat Hackern für das Vertrauen, mir einen seltenen Einblick in ihre Welt und Innenperspektive gewährt zu haben. Letztlich wäre diese Arbeit ohne sie nicht möglich gewesen.

Abstract

Wie unterscheiden sich kriminelle Black Hat Hacker und legal handelnde White Hat Hacker hinsichtlich Eigenschaften der Dunklen Triade (Psychopathie, Machiavellismus, Narzissmus)? In drei Studien im Sinne eines *Mixed Method Designs* wurde durch Kombination quantitativer und qualitativer Methoden ein klares Profil von Black Hat Hackern identifiziert, das sowohl zur Prävention als auch Strafverfolgung (Cyberprofiling) potentiellen Nutzen haben kann.

Studie 1 ist eine quantitative Inhaltsanalyse von Fahndungsplakaten des FBIs der meistgesuchten Hacker mit dem Ziel, valide demografische Daten zu erfassen.

Studie 2 ist eine quantitative Online-Befragung mit $N = 1.185$ Hackern, die u.a. in Hacker-Foren im Darknet unter Wahrung strengster Sicherheitsvorkehrungen rekrutiert wurden.

Studie 3 beinhaltet qualitative Leitfadeninterviews mit 18 Hackern, um die quantitativen Ergebnisse zu validieren, indem sie um die Innenperspektive der Hacker ergänzt werden.

Black Hat Hacker sind im Durchschnitt jung, männlich und gut qualifiziert. Es liegen mehrere Motive gleichzeitig vor, wobei Herausforderung ("Challenge") am häufigsten genannt wurde. Black Hat Hacker sind signifikant psychopathischer und machiavellistischer als White Hat Hacker. Insgesamt zeigte sich für Black Hat Hacker das Profil ‚machiavellistischer primärer Psychopathen‘, wobei sekundäre Psychopathie und Narzissmus moderater ausfallen. Hierin könnte der Grund liegen, warum sie kriminell handeln und auch wie es ihnen langfristig gelingt, dem Strafvollzug zu entgehen. Bei isolierter Betrachtung erhöhte Narzissmus leicht die Chance, White Hat Hacker zu sein.

Auch Rechtfertigungsstrategien und der Online Disinhibition Effect spielen eine Rolle, jedoch bei White Hats und Black Hats. Die Ergebnisse deuten darauf hin, dass White Hats und Black Hats (beide) ihre Hackerkarriere im Alter von 10-17 Jahren, oft durch *Cheating* und *Modding* in Computerspielen, eher im rechtlichen Graubereich beginnen. Die Dunkle Triade entscheidet damit weniger, wer Black Hat Hacker *wird*, sondern wer Black Hat Hacker *bleibt*.

Abstract

How do Black Hat Hackers and White Hat Hackers differ in terms of Dark Triad personality traits (Psychopathy, Machiavellianism, Narcissism)? In three studies (*Mixed Method Design*), a clear profile of Black Hat Hackers has been identified by combining quantitative and qualitative methods. The results may be useful for both crime prevention and law enforcement (Cyberprofiling).

Study 1 is a quantitative content analysis of FBI Cyber Most Wanted posters with the aim of obtaining valid demographic data.

Study 2 is a quantitative Online-Survey with $N = 1,185$ hackers who were recruited in hacker-forums on the Darknet, among other places, under strict security precautions.

Study 3 involves qualitative interviews with 18 hackers to validate the quantitative results and gain insights into hacker's inside-perspective.

On average, Black Hat Hackers are young, male, and well-qualified. Hackers reported multiple motives, with 'Challenge' being mentioned the most.

Black Hat Hackers are significantly more psychopathic and machiavellian than White Hat Hackers.

Overall, Black Hat Hackers were found to resemble the profile of 'machiavellian primary Psychopaths', with secondary Psychopathy and Narcissism being moderate. This could be the reason why they engage in criminal activity and also how they manage to avoid punishment long term. When examined in isolation, narcissism slightly increased the odds of being a White Hat Hacker. Moral justification strategies and the Online Disinhibition Effect also play a role among White Hats and Black Hats. The results suggest that White Hats and Black Hats (both) tend to start their hacking careers between the ages of 10-17, often through *Cheating* and *Modding* in video games, in a legal gray area.

The Dark Triad therefore does not determine who *becomes* a Black Hat Hacker, but who *remains* a Black Hat Hacker.

Inhaltsverzeichnis

	Seite
Abkürzungsverzeichnis	VIII
Abbildungsverzeichnis	IX
Tabellenverzeichnis	XI
1 Einführung	1
1.1 Überblick der Studien	1
1.2 Relevanz des Themas	5
1.3 Aufbau der Arbeit	7
2 Theoretischer Bezugsrahmen	8
2.1 Definition Cyberkriminalität	8
2.1.1 Arten von Cybercrime im engeren Sinne	11
2.2 Definitionen Hacker und Darknet	14
2.2.1 Ursprung des Hackerbegriffs	14
2.2.2 Black Hat Hacker und White Hat Hacker	15
2.2.3 Abgrenzung Darknet, Deepweb, Clearnet	18
2.2.4 Crime-As-a-Service-Strukturen und Dark Economy	21
2.3 Die Dunkle Triade	24
2.4 Psychopathie	25
2.4.1 Differenzierung subklinischer Psychopathie und ASPD	25
2.4.2 Operationalisierungen und Konzeptionalisierungen	26
2.4.3 Primäre und sekundäre Psychopathie	30
2.4.4 Neurobiologische Aspekte der Psychopathie	33
2.5 Narzissmus	35
2.6 Machiavellismus	38
2.7 Kurzskalen zur Erfassung der Dunklen Triade	40
3 Aktueller Forschungsstand	43
3.1 Die Dunkle Triade und Kriminalität	43
3.1.1 Gewaltkriminalität, Wirtschaftskriminalität und antisoziales Verhalten	43
3.1.2 Die Dunkle Triade und Cyberkriminalität	45
3.2 Cyberprofiling und die Dunkle Triade	50
3.3 Forschungsergebnisse zu Persönlichkeitsmerkmalen von Hackern	52
3.4 Cyberkriminologische Theorien	57
3.4.1 Einordnung in den Kontext kriminologischer Theorien	57
3.4.2 Der Online Disinhibition Effect	60

3.4.3	Die White Gloves Theorie	62
3.4.4	Der Labelling-Ansatz	63
3.4.5	Subkultur- und Lerntheorien	64
3.5	Fragestellungen der Arbeit	66
4	Studie 1: Quantitative Inhaltsanalyse der FBI Most Wanted Hacker	68
4.1	Zielsetzung, Forschungsfragen, Hypothesen	68
4.2	Forschungsdesign	71
4.2.1	Untersuchungsgegenstand und Zeitraum	71
4.2.2	Materialbeschaffung durch die Wayback Machine (Internet Archive)	72
4.2.3	Definition der Analyseeinheit und Auswahlinheit	76
4.2.4	Kategorien, Codebuch, Datenerhebung	79
4.2.5	Berechnung des Alters zur Tatzeit	81
4.3	Ergebnisse und Hypothesenprüfung	82
4.3.1	Deskriptive Statistiken: Geschlecht	82
4.3.2	Deskriptive Statistiken: Alter	82
4.3.3	Deskriptive Statistiken: Nationalitäten, Nachrichtendienstzugehörigkeit, Belohnung	83
4.4	Diskussion	87
4.4.1	Zusammenfassung und Bewertung der zentralen Befunde	87
4.4.2	Methodische Reflexion	92
5	Studie 2: Online-Befragung zur Dunklen Triade und Motiven von Hackern ...	94
5.1	Zielsetzung und Forschungsfragen	94
5.2	Herleitung der Hypothesen	98
5.3	Zugang zum Forschungsfeld	103
5.4	Fragebogenkonstruktion	105
5.4.1	Operationalisierung der Konstrukte	106
5.4.2	Programmierung der Endseite mit Darstellung der Ergebnisse	119
5.4.3	Pretest & Anpassungen	121
5.5	Rekrutierungsstrategie und Video	122
5.6	Rechtliche Aspekte, Ethik und besondere Sicherheitsvorkehrungen	127
5.7	Durchführung der Befragung	134
5.7.1	Die Rekrutierung von Hackern	134
5.7.2	Rücklaufstatistik und Plausibilitätscheck	148
5.8	Datenbereinigung	149
5.9	Beschreibung der Stichprobe	151
5.10	Ergebnisse und Hypothesenprüfung	155
5.10.1	Validität der Gruppenzugehörigkeit: Black Hats und White Hats	155
5.10.2	Statistische Analysen	157
5.10.3	Psychopathie	158

5.10.4 Machiavellismus	162
5.10.5 Narzissmus	166
5.10.6 Dunkle Triade (Gesamt)	169
5.10.7 Primäre und sekundäre Psychopathie (LSRP)	172
5.10.8 Quelle der Fähigkeiten	177
5.10.9 Der Online Disinhibition Effect	178
5.10.10 Motive von Hackern und Korrelationen mit Triademerkmale	181
5.10.11 Persönlichkeitsmerkmale und Angriffsmethoden	184
5.10.12 KI-Nutzung	185
5.11 Diskussion	186
5.11.1 Sonstige Felderfahrungen	186
5.11.2 Zusammenfassung und Bewertung der zentralen Befunde	192
5.11.3 Methodische Reflexion	204
6 Studie 3: Qualitative Interviews mit Hackern	208
6.1 Zielsetzung und Gütekriterien	208
6.2 Interviewleitfaden	210
6.3 Probandengewinnung	214
6.4 Durchführung der Interviews und Transkription	215
6.5 Auswertungsmethode	218
6.6 Ergebnisse	221
6.6.1 Einzelfallbeschreibungen	221
6.6.2 Fallübergreifende Gruppenvergleiche	231
6.7 Diskussion	263
6.7.1 Zusammenfassung und Bewertung der zentralen Befunde	263
6.7.2 Methodische Reflexion	265
7 Allgemeine Diskussion und Schlussfolgerungen	268
7.1 Zusammenführung der Ergebnisse	268
7.2 Praktische Relevanz und Ausblick	282
7.3 Methodische Reflexion	285
Literaturverzeichnis	288
Anhang	303

Abkürzungsverzeichnis

APT	Advanced Persistent Threat
ASPD	Antisocial Personality Disorder
BKA	Bundeskriminalamt
BSI	Bundesamt für Sicherheit in der Informationstechnik
DDoS	Distributed Denial of Service
DSM	Diagnostic and Statistical Manual of Mental Disorders
FBI	Federal Bureau of Investigation
HUMINT	Human Intelligence (menschliche Aufklärung)
ICD	International Classification of Diseases
IP	Internet Protocol
IT	Informations-Technologie
KI	Künstliche Intelligenz
LLM	Large Language Model
LSRP	Levenson Self-Report Psychopathy Scale
MACH	Machiavellismus-Subskala der Short Dark Triad
MO	Modus Operandi
NARC	Narzissmus-Subskala der Short Dark Triad
NATO	North Atlantic Treaty Organization
NPI	Narcissistic Personality Inventory
OpSec	Operational Security
OSINT	Open-Source Intelligence
PCL-R	Psychopathy Checklist Revised
PDF	Portable Document Format
PGP	Pretty Good Privacy Verschlüsselung
PKS	Polizeiliche Kriminalstatistik
PPI-R	Psychopathic Personality Inventory Revised
PSYCH	Psychopathie-Subskala der Short Dark Triad
SCPs	Slow Cortical Potentials
SD3	Short Dark Triad Skala (Jones & Paulhus, 2014)
TB	Terabyte
TOR	The Onion Router
TriPM	Triarchic Psychopathy Measure
URL	Uniform Resource Locator (Internetadresse)
VPN	Virtual Private Network

Abbildungsverzeichnis

	Seite
<i>Abbildung 1.</i> <i>Mixed Method Design</i> nach Creswell & Plano Clark (2018).....	5
<i>Abbildung 2.</i> Screenshot Best Carding World (2025) (Darknet-Forum).....	10
<i>Abbildung 3.</i> Screenshot Darknet-Marktplatz Vortex (2025): Angebote der Dark Economy	22
<i>Abbildung 4.</i> Screenshot: Anonymer Auftragshacker (2025) (Darknet)	23
<i>Abbildung 5.</i> Korrelationen der Merkmale der Dunklen Triade untereinander	24
<i>Abbildung 6.</i> Mögliche Einflussfaktoren auf kriminelles Hacking.....	59
<i>Abbildung 7.</i> Anonymisierte Screenshots FBI Cyber Most Wanted	72
<i>Abbildung 8.</i> Screenshot <i>Wayback Machine</i> (2025), Archivierte Seite der Uni Tübingen	73
<i>Abbildung 9.</i> Screenshot <i>Wayback Machine</i> (2025): Archivierung der Cyber Most Wanted	74
<i>Abbildung 10.</i> Anzahl gesuchter Hacker im Zeitverlauf	75
<i>Abbildung 11.</i> Aufbau eines FBI-Fahndungsplakats (Analyseeinheit, anonymisiert)..	76
<i>Abbildung 12.</i> Histogramm: Alter der Hacker zur Tatzeit ($n = 123$).....	83
<i>Abbildung 13.</i> Deskriptive Statistik: Häufigkeiten der Nationalitäten ($n = 138$)	84
<i>Abbildung 14.</i> Deskriptive Statistik: Nationalitäten staatlicher Hacker ($n = 85$).....	85
<i>Abbildung 15.</i> Deskriptive Statistik: Häufigkeiten der FBI-Belohnungen ($n = 46$)	87
<i>Abbildung 16.</i> Durchschnittliches Profil eines typischen FBI Most Wanted Hackers ..	88
<i>Abbildung 17.</i> Übersicht der Variablen und Forschungsfragen	98
<i>Abbildung 18.</i> Screenshot Fragebogen: Operationalisierung der Hacker-Kategorie	107
<i>Abbildung 19.</i> Visualisierte 5-stufige Likert-Skala	110
<i>Abbildung 20.</i> Screenshot Sosci-Survey Fragebogen: Motivauswahl	116
<i>Abbildung 21.</i> Screenshot Fragebogen: Ergebnisdarstellung	120
<i>Abbildung 22.</i> QR-Link zum Rekrutierungsvideo	125
<i>Abbildung 23.</i> Beispiel Text- und Bildbeiträge zur Rekrutierung von Hackern.....	127
<i>Abbildung 24.</i> Screenshot Hacker-Forum DarknetArmy (2025) (Darknet).....	139
<i>Abbildung 25.</i> Screenshot Hacker-Forum CryptBB (2025).....	140
<i>Abbildung 26.</i> Screenshot Darknet-Netzwerk Pitch (2025)	141

<i>Abbildung 27.</i>	Screenshots Clearnet Hacker-Foren	142
<i>Abbildung 28.</i>	Screenshots Telegram-Hackergruppen	143
<i>Abbildung 29.</i>	Screenshot Login-Bereich: Targeting Reddit Hacker-Foren (Subreddits)	144
<i>Abbildung 30.</i>	Screenshot Bannerwerbung Imageboard 4chan (2025)	145
<i>Abbildung 31.</i>	Screenshot LinkedIn Probandengewinnung	147
<i>Abbildung 32.</i>	Histogramme Altersverteilung in Prozent	152
<i>Abbildung 33.</i>	Histogramm akademischer Abschluss in Prozent	153
<i>Abbildung 34.</i>	Visualisierung der Mittelwerte der Einzelitems: Psychopathie (SD3)	159
<i>Abbildung 35.</i>	Visualisierung der Mittelwerte der Einzelitems: Machiavellismus (SD3)	163
<i>Abbildung 36.</i>	Visualisierung der Mittelwerte der Einzelitems: Narzissmus (SD3) ...	167
<i>Abbildung 37.</i>	Prozentuale Häufigkeiten der Nennungen: Motive von Black Hat Hackern	181
<i>Abbildung 38.</i>	Darstellung der stärksten Korrelationen zwischen Triademerkmale und Hacking-Motiven.....	183
<i>Abbildung 39.</i>	Screenshot Dread (Darknet): Surveillance-Operation-Vorwurf und Doxxing.....	187
<i>Abbildung 40.</i>	Screenshot Reddit Hacking-Forum: OpSec-Paranoia	188
<i>Abbildung 41.</i>	Screenshot Dread (Darknet): Subforum <i>d/fraud</i>	190
<i>Abbildung 42.</i>	Ergebnisse der Mittelwertvergleiche durch <i>t</i> -Tests (LSRP).....	198
<i>Abbildung 43.</i>	Screenshot: Probandengesuch Hacker-Forum Breachform (2025) (Darknet)	215
<i>Abbildung 44.</i>	Übersicht empirischer Befunde zum Profil von Black Hat Hackern ...	269
<i>Abbildung 45.</i>	Effektgrößen der <i>t</i> -Tests nach Cohen (1988)	272
<i>Abbildung 46.</i>	Drei-Phasen-Modell der Hacker-Karriere	279

Tabellenverzeichnis

	Seite
Tabelle 1: Subskalen des NPI-40 nach Collani (2014)	36
Tabelle 2: Machiavellismus-Items aus Henning & Six (1997)	39
Tabelle 3: Kategorien des Codebuchs	79
Tabelle 4: Deskriptive Statistiken: Abstand Tat zu Haftbefehl, $n = 86$	81
Tabelle 5: Kreuztabelle Nachrichtendienstzugehörigkeit x Nationalität	86
Tabelle 6: Aufbau des Fragebogens	106
Tabelle 7: Transkript des Rekrutierungsvideos und methodische Überlegungen ...	125
Tabelle 8: Deskriptive Statistiken: Psychopathie-Mittelwerte (SD3-Subskala)	159
Tabelle 9: Deskriptive Statistiken: Machiavellismus-Mittelwerte (SD3-Subskala) ...	163
Tabelle 10: Deskriptive Statistik: Narzissmus-Mittelwerte (SD3-Subskala)	166
Tabelle 11: Alpha-Reliabilitäten der LSRP ($n = 897$)	172
Tabelle 12: Deskriptive Statistik: Prozentuale Häufigkeiten, Quelle der Hackingfähigkeiten (Mehrfachauswahl möglich)	177
Tabelle 13: Deskriptive Statistik: Online-Disinhibition Effect	179
Tabelle 14: Ausschnitt Codebogen Black Hats, Kategorie ‚Motive‘	220
Tabelle 15: Acht Prinzipien des <i>Moral Disengagements</i> nach Bandura (1999) bei Black Hat Hackern	235
Tabelle 16: Ausschnitt Codebogen: Zitate und Interpretationen	266

1 Einführung

1.1 Überblick der Studien

Manche Hacker nutzen ihre technischen Fähigkeiten im kriminellen Sinne (für Cyberangriffe), während andere Hacker ihre Fähigkeiten legal nutzen (für Cybersicherheit und Abwehr). Je nach Motiv, ob Hacker ihre Fähigkeiten in den Dienst der ‚dunklen Seite‘ oder ‚hellen Seite‘ stellen, haben sich die Begriffe *Black Hat Hacker* und *White Hat Hacker*¹ zur abgrenzenden Kategorisierung etabliert (z.B. Huber, 2019, S. 34; Kirwan & Power, 2013, S. 54).

Warum handeln die einen kriminell und die anderen nicht?

Das Ziel der vorliegenden Arbeit besteht darin, Black Hat Hacker und White Hat Hacker in Hacker-Foren im Clearnet und Darknet zu rekrutieren, um sie hinsichtlich Eigenschaften der Dunklen Triade miteinander zu vergleichen.

Hackerprofile sind in Bezug auf demografische Daten wie Alter und Geschlecht recht homogen (jung und männlich) (BKA, 2015b) und entstammen derselben Subkultur, die sich erst später ausdifferenzierte, wie Chiesa, Ducci & Ciappi (2009, S. 38) rekonstruieren. Zudem ähneln sich Black Hat Hacker und White Hat Hacker in ihren technischen Fähigkeiten, was eine Besonderheit dieses Deliktsbereiches ist. Wer die technischen Fertigkeiten besitzt, Sicherheitslücken auszunutzen, hätten auch die Fähigkeit, diese zu schließen und vice versa. Da beide Hackergruppen sich in Demografie, Subkultur und technischen Fähigkeiten ähneln, liegt die Vermutung nahe, dass sie sich im Sinne der Persönlichkeitspsychologie in *traits* (Persönlichkeitseigenschaften) unterscheiden könnten und Black Hats möglicherweise ‚dunklere‘ Persönlichkeitsdispositionen besitzen.

Bei der Erklärung antisozialen oder kriminellen Verhaltens spielt die Dunkle Triade eine besondere Rolle. Psychopathie, Machiavellismus und Narzissmus sind drei distinkte, aber sich überschneidende, interkorrelierte Konzepte, weshalb Paulhus & Williams (2002) den

¹ In Übereinstimmung mit der üblichen Praxis werden die englischsprachigen Begriffe *Hacker*, *Black Hat Hacker* und *White Hat Hacker* verwendet. Die Begriffe sind englischsprachig und daher geschlechtsneutral zu verstehen und beziehen sich nicht ausschließlich auf Männer, sofern nicht anders angegeben. In allen anderen Fällen wird zur besseren Lesbarkeit entweder das generische Maskulinum oder wenn möglich eine geschlechtsneutrale Bezeichnung (z. B. „Personen“) verwendet.

gemeinsamen Begriff der Dunklen Triade prägten. Seit der Bündelung zur Triade vor über 20 Jahren werden die drei Konstrukte häufig gemeinsam beschrieben und untersucht.

Als ‚Dunkle Triade‘ werden Psychopathie, Narzissmus und Machiavellismus nicht als Persönlichkeitsstörungen betrachtet, sondern als subklinische Persönlichkeitsmerkmale, die auf einem Kontinuum existieren und somit jede Person mehr oder weniger hohe Ausprägungen aufweist. Die Triade findet daher vor allem bei nicht-klinischen Populationen Anwendung, z.B. im Organisationskontext. Alle drei Komponenten der Dunklen Triade zeigen nach Paulhus & Williams (2002) negative Zusammenhänge mit Verträglichkeit (S. 559), sind also tendenziell sozial aversiv und gehen u.a. mit egozentrischen, manipulativen und empathielosen Verhaltensdispositionen einher. Externbrink & Keil (2018) bezeichnen dies als gemeinsamen „antisozialen Kern“ (S. 3), aufgrund der Verbindungen der Dunklen Triade mit antisozialem oder kriminellem Verhalten. Insbesondere Psychopathie wurde in zahlreichen Untersuchungen als valider Prädiktor identifiziert für eine Reihe von antisozialen Verhaltensweisen, Aggression, Kriminalität und Rückfälligkeit (zur Übersicht siehe: Douglas, Vincent, & Edens, 2019; Gillespie, Jones & Garofalo, 2023; Hemphill, Hare & Wong, 1998; Lykken, 1995, S. 3-12; Porter, Woodworth & Black, 2019). Jüngere Untersuchungen haben die Dunkle Triade auch im Zusammenhang mit Wirtschaftskriminalität untersucht (z.B. Amos, Longpré & Roos, 2024). Wenn Triadeeigenschaften und insbesondere Psychopathie eine erhebliche Rolle bei nahezu allen Formen der Gewalt- & Wirtschaftskriminalität spielen, scheint es lohnenswert, die Rolle der Dunklen Triade auch in Bezug auf Cyberkriminalität zu untersuchen. Obwohl Cyberkriminalität ein zunehmend bedeutsames Deliktsfeld ist, existiert kaum empirisches Wissen über Black Hat Hacker und insbesondere deren Persönlichkeitsprofile (Gaia, Sanders, Sanders, Upadhyaya, Wang, & Yoo, 2021, S. 25; Martineau, Spiridon, Aiken, 2023, S. 452; Selzer & Oelrich, 2021). Der Grund liegt unter anderem in der geringen Aufklärungsquote im Bereich Cybercrime (Huber & Pospisil, 2020, S. 130). Rüdiger (2023, S. 14) setzt Zahlen aus Befragungen der Bevölkerung, also wie viele Personen tatsächlich Opfer von Cyberkriminalität geworden sind, mit der offiziellen

polizeilichen Kriminalstatistik in Relation und leitet eine mögliche Dunkelfeldrate von etwa 1 zu 147 ab.

White Hat Hacker sind verhältnismäßig leicht zu finden, sie arbeiten in Cybersecurity-Abteilungen von Unternehmen oder bieten als sogenannte Penetrationstester selbstständig ihre Dienste an, gegen Bezahlung Sicherheitsmängel zu finden und zu beheben (Huber, 2019, S. 34). Der empirische Zugang zu Black Hat Hackern gestaltet sich weitaus schwieriger:

„Das Wissen um Täter im Bereich Cybercrime ist begrenzt. Es basiert häufig auf retrospektiven Studien angeklagter Cybercrime-Fälle sowie Surveys und halbstandardisierten Befragungen (entweder Face-to-Face oder online) zu selbstberichteter Delinquenz. Eine zunehmend von Forschern genutzte Methode der Datensammlung besteht in der Beobachtung bzw. Analyse von Diskussionsforen (auch im ‚Darknet‘)“ (BKA, 2015b, S. 4).

Dem Beispiel des Bundeskriminalamtes folgend, liegt der wesentliche Beitrag der vorliegenden Arbeit in der Rekrutierung dieser äußerst schwer erreichbaren Zielgruppe: Aktive Black Hat Hacker in Hacker-Foren im Darknet und Clearnet.

Das ‚Darknet‘ bezeichnet einen verborgenen Teil des Internets und ist über das Tor-Netzwerk erreichbar, das eine außerordentliche Verschlüsselung und Anonymisierung ermöglicht (Henkel, 2020, siehe auch Kapitel 2.2.3). Es ist einer der wenigen bisherigen Versuche, empirischen Zugang zu einer Population zu gewinnen, die bislang überwiegend im Verborgenen agiert und in der Forschung daher kaum direkt berücksichtigt wurde.

Es soll ein *Mixed Method Design* nach Creswell & Plano Clark (2018) verwendet werden, um sich diesem schwierigen Forschungsfeld aus drei verschiedenen Perspektiven anzunähern. In drei Studien werden quantitative und qualitative Methoden so kombiniert, dass sich die methodischen Stärken und Schwächen im Sinne der „Methodentriangulation“ (Flick, 2004, S. 42) gegenseitig kompensieren, um ein klares Profil von Black Hat Hackern zu erlangen. White Hats stellen in gewisser Weise die Kontrollgruppe dar, wobei das Hauptinteresse darin

besteht, ein klares Profil von Black Hat Hackern (in Hacker-Foren im Clear- und Darknet) zu gewinnen.

Studie 1 ist eine quantitative Inhaltsanalyse der Cyber Most Wanted Fahndungsplakate des FBI von 2010 bis 2024. Durch die inhaltsanalytische Auswertung der demografischen Informationen zu Alter, Nationalität und Geschlecht soll sich der Frage, *wer* Black Hat Hacker sind, angenähert werden. Der Vorteil der Methode ist, dass hier behördlich validierte Informationen zu soziodemografischen Daten gewonnen werden können und der Forschungsgegenstand (FBI-Fahndungsplakate) nicht reaktiv ist und das Vorgehen nicht auf einer Selbstauskunft der Täter basiert. Nachteil ist, dass neben formellen, demografischen Daten mit dieser Methodik keine inhaltlichen Dimensionen wie Motive, moralische Überzeugungen oder Einstellungen erhoben werden können.

Studie 2 ist eine quantitative Online-Befragung, bei der Hacker in Hacker-Foren und durch gezieltes Targeting direkt rekrutiert werden. Mittels *t*-Tests für unabhängige Stichproben soll geprüft werden, ob sich Black Hats und White Hats signifikant hinsichtlich Psychopathie, Narzissmus und Machiavellismus und weiterer Merkmale unterscheiden. Es soll eine hohe und möglichst repräsentative Fallzahl je Hackergruppe erreicht werden. Ziel ist also das Messen, Quantifizieren und die Prüfung der Hypothesen.

Studie 3 soll die quantitativen Ergebnisse durch qualitative Interviews validieren, erklären und vertiefen, indem Hacker selbst zu Wort kommen, um einen tieferen Einblick in die Innenperspektive der Hacker zu gewinnen, der über psychometrische Messinstrumente, Likert-Skalen und reine Zahlenwerte hinausgeht. Creswell & Plano Clark (2018) bezeichnen diese Reihenfolge des Vorgehens - erst quantitativ zu messen, dann qualitativ zu validieren - als „explanatory sequential design“ (Creswell & Plano Clark, 2018, S. 77). Durch die Kombination von drei Methoden in drei Studien soll der Untersuchungsgegenstand aus verschiedenen Perspektiven betrachtet werden, um so ein klares Bild der Profile und Motive von Hackern zu gewinnen (siehe Abbildung 1).

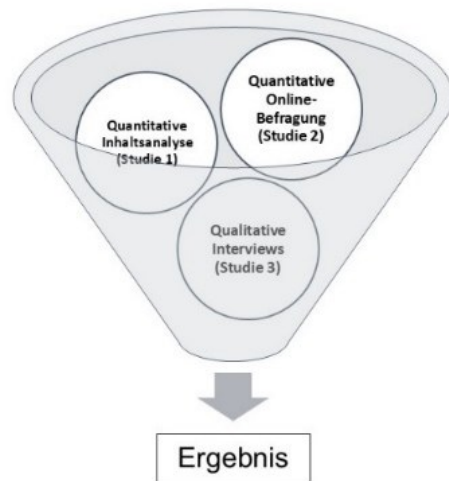


Abbildung 1. *Mixed Method Design* nach Creswell & Plano Clark (2018)

Quelle: Eigene Darstellung.

1.2 Relevanz des Themas

Der jährliche Schaden durch Cyberangriffe auf deutsche Unternehmen wurde 2023 auf 148,2 Milliarden Euro geschätzt (Bitkom, 2023, S. 9; BKA, 2024, S. 23). Statista (2025c) beziffert die globalen Schäden durch Cyberangriffe für das Jahr 2025 mit 10,29 Billionen Euro (engl. trillion). Diese Summe entspricht mehr als dem doppelten des Bruttoinlandsprodukts Deutschlands des Jahres 2024 von 4,33 Mrd. Euro (Statistisches Bundesamt, 2025a). Dass Cyberkriminalität eine zunehmend bedeutsame Bedrohung darstellt, steht außer Frage, doch worin liegt die praktische Relevanz, die Dunkle Triade, Profile und Motive von Black Hat Hackern zu untersuchen?

Cybercrime ist kein rein technisches Problem, sondern die Mehrzahl der Cyberangriffe und Sicherheitsverstöße (Data Security Breaches) gehen auf menschliche Fehler zurück (z.B. Liginlal, Sim & Khansa, 2009, S. 221). Sowohl auf der Seite der Täter als auch der Opfer sind es letztlich psychologische Motivatoren und Faktoren, die einen wichtigen Teil des Phänomens ausmachen. Die Relevanz der Forschungsfrage soll anhand von drei Dimensionen verdeutlicht werden:

Erstens wird damit eine Forschungslücke geschlossen. Die Psychopathieforschung hat ihren historischen Ursprung im forensischen Bereich (Benning, Venables & Hall, 2019, S. 585) und befasste sich zunehmend mit Psychopathie im Wirtschaftskontext (z.B. Mullins-Sweatt, Glover, Derefinko, Miller & Widiger, 2010). Psychopathie im Zusammenhang mit Cyberkriminalität zu untersuchen, schließt eine Forschungslücke und erscheint angesichts der Zahlen und KI-getriebenen Zukunftsszenarien zeitgemäß.

Zweitens kann ein Verständnis der Persönlichkeitsmerkmale von Hackern in Bezug auf die Entwicklung von Präventionsansätzen relevant sein (Kirwan & Power, 2013, S. 22). Das Dunkelfeld im Deliktsbereich der Cyberkriminalität ist groß (BKA, 2024, S. i), das bedeutet, nur wenige Fälle kommen überhaupt zur Kenntnis der Strafverfolgungsbehörden. Huber & Pospisil (2020, S. 112) weisen darauf hin, dass sich die digitalen Spuren über die ganze Welt verteilen können, weshalb herkömmliche Ermittlungsmethoden hier an ihre Grenzen stoßen. Erschwerend kommt hinzu, dass Täter in Ländern residieren, die nicht an Deutschland ausliefern (siehe World Cybercrime Index: Bruce, Lusthaus, Kashyap, Phair & Varese, 2024). Daher folgern Huber & Pospisil (2020) „Die Cybercrime-Prävention muss international eine hohe Priorität einnehmen“ (S. 112). Nach Chiesa et al. (2009, S. 122) beginnen Hacker bereits im Alter von 11-12 Jahren ihre Fähigkeiten zu entwickeln. In diesem jungen Alter besteht noch Hoffnung zur Intervention, um angehende Hacker zu überzeugen, eine Karriere als White Hat anzustreben. Doch woran sind potentielle Black Hat Hacker zu erkennen? Erst durch ein klares Bild der Profile, Persönlichkeitsmerkmale und Motive wird „selektive Prävention“ (Bürger & Kaess, 2024, S. 405) überhaupt erst möglich.

Drittens kann ein besseres Verständnis der Profile der Täter potentiell auch bei der Aufklärung von Straftaten helfen. Profiling beschreibt die „Idee, das Verhalten von Tätern und den psychosozialen Kontext von Straftaten als Informationsquelle zur Unterstützung der Verbrechensaufklärung zu nutzen“ (Musolff, 2002, S. 3). Das *Offender Profiling* (Täterprofiling) ist eine Technik, die nach Musolff (2002, S. 1) bislang u.a. bei Ermittlungen zu Mordserien und Sexualstraftaten eingesetzt wurde. Mit einem besseren Verständnis der Profile und Motive von Black Hat Hackern besteht Hoffnung, dass Profiling-Ansätze langfristig

auch im Cyberspace Anwendung finden könnten und einen Beitrag zur Verbrechensaufklärung leisten können (Huber, 2019, S. 64-65; Martineau et al., 2023, S. 452). Chiesa et al. (2009) schließen daraus:

„To understand computer attacks, we need the joint know-how of computer security experts, who can tell us exactly ‘what’ has happened and ‘how’, and criminal profiling skills to explain ‘why’ the attack was carried out and what kind of attacker we’re dealing with - the ‘who’“ (S.12).

Das ‚Wie‘ und das ‚Was‘ sind technische Fragestellungen, aber das ‚Wer‘ (Profile) und ‚Warum‘ (Motive) sind psychologische Aspekte. In einem besseren Verständnis der Motive und Profile von Black Hat Hackern liegt die Relevanz der Studien in diesem Feld.

1.3 Aufbau der Arbeit

Nach der Einführung (Kapitel 1) liefert Kapitel 2 die nötigen theoretischen Fundamente, Definitionen und Konzeptionalisierungen zur Dunklen Triade, Cyberkriminalität, Darknet und White Hat- und Black Hat Hackern. Kapitel 3 fasst den aktuellen Forschungsstand zu den Profilen und Persönlichkeitsmerkmalen von Hackern zusammen und ordnet dies in den Kontext cyberkriminologischer Theorien ein. Basierend darauf werden die konkreten Forschungsfragen und relevanten Dimensionen abgeleitet, worin Black Hats und White Hats sich unterscheiden könnten. Das Forschungsdesign, Instrumente, Ergebnisse und Diskussion der drei Studien werden in Kapitel 4, 5 und 6 vorerst einzeln dargestellt. Kapitel 7 liefert im Sinne der „Methodentriangulation“ (Flick, 2004, S. 42) eine gemeinsame Diskussion der Ergebnisse, setzt die Studien also in Beziehung zueinander und diskutiert Limitation, Reflexion, praktische Relevanz und Anwendbarkeit der Ergebnisse und Implikationen für künftige Forschung.

2 Theoretischer Bezugsrahmen

2.1 Definition Cyberkriminalität

Cybercrime ist ein vager, diffuser Sammelbegriff für zahlreiche unterschiedliche Taten, doch Hacking, der Online-Drogenhandel und das Teilen kinderpornografischer Inhalte unterscheiden sich stark in Bezug auf das Vorgehen der Täter (*Modus Operandi*), die Profile und Motive. Außer, dass diese Delikte direkt oder indirekt etwas mit Computertechnologie oder dem Internet als Kommunikationsmedium zu tun haben, gibt es kaum Gemeinsamkeiten. Der Begriff ‚Cyberkriminalität‘ sollte daher zunächst definiert und abgegrenzt werden. Die Definition im Rahmen dieser Arbeit orientiert sich an der üblichen Definition der Strafverfolgungsbehörden und der Forschung.

Das Bundeskriminalamt und die PKS unterscheiden *Cyberkriminalität im engeren Sinne* und *Cyberkriminalität im weiteren Sinne* (BKA, 2024, S. i). Diese Begriffe zur Abgrenzung und Definition finden auch in wissenschaftlichen Publikationen und Lehrbüchern Anwendung (z.B. Huber & Pospisil, 2020, S. 111; Plank, 2020, S. 18-19).

Cyberkriminalität im weiteren Sinne beschreibt „Delikte, die lediglich unter Nutzung von Informationstechnik begangen werden und bei denen das Internet vorwiegend Tatmittel ist“ (BKA, 2024, S. i). Die Taten wären also auch in der physischen, realen Welt möglich (z.B. Drogenhandel) und das Internet stellt nur das Medium dar. Das Internet und IT-Infrastruktur sind bei *Cybercrime im weiteren Sinne* zwar Kommunikationsmedium, ohne aber selbst Angriffsobjekt zu sein (Dreißigacker, Skarczynski, Bergmann & Wollinger, 2020, S. 320). Zu dieser Kategorie von *Cybercrime im weiteren Sinne* zählt vor allem der Online-Handel mit jeglicher Art von illegalen Gütern, wie falschen Papieren, Drogen, Waffen etc. (siehe zur Übersicht z.B.: Henkel, 2020, S. 175; Wernert, 2021, S. 38). Cyberkriminelle haben für den Vertrieb einen neuen Kanal identifiziert, weshalb Wernert (2021) vom „Tatmittel Internet“ (S. 38) spricht, und Kirwan & Power (2013) nutzen die Metapher des „old wine in new bottles“.

So wie auch legale Geschäftsmodelle sich digitalisiert haben (Dating wird zu Online-Dating, Shopping wird zu Online-Shopping und Banking wird zu Online-Banking), haben sich auch

die analoge Kriminalität und antisoziale Phänomene zunehmend digitalisiert. So wird auch Stalking immer öfter zu Cyberstalking, Mobbing zu Cybermobbing, und auch Romance-Scams könnte man nach Thiel (2020, S. 244) als die digitalisierte Version des Heiratsschwindels bezeichnen.

Im englischen Sprachraum wird *Cybercrime im weiteren Sinne* als *cyber-enabled crime* bezeichnet (z.B. Interpol, 2021). Die Hauptforschungsfrage der vorliegenden Arbeit zielt auf Hacker ab. Der Online-Drogenhandel ist zwar der *Cyberkriminalität im weiteren Sinne* zuzuordnen, doch auch im allgemeinen Sprachgebrauch würde man Täter dieses Deliktsbereiches nicht als ‚Hacker‘ bezeichnen. *Cybercrime im weiteren Sinne* wird im Rahmen dieser Arbeit vollständig ausgeschlossen, da das Forschungsinteresse Hackern gilt, also Tätern im Bereich *Cybercrime im engeren Sinne*. Damit sind Delikte gemeint, die durch das Internet und Computertechnologie überhaupt erst möglich geworden sind (z.B. Dreißigacker et al., 2020, S. 320) und die es „in keiner Variante offline gibt“ (Huber, 2019, S. 22), wie z.B. Viren, Phishing, Trojaner oder Schadsoftware. Der englische Begriff für diese Art der ‚echten Cyberkriminalität‘ ist „cyber-dependent crime“ (Interpol, 2021, S. 10), da IT-Systeme selbst Zielscheibe sind und nicht nur Medium. Hacking ist ohne die entsprechende Technologie analog nicht möglich, weshalb Kirwan & Power (2013) diese Taten „internet-specific crimes“ (S. 3) nennen. Wenn im Rahmen der vorliegenden Arbeit und Studien von ‚Cyberkriminalität‘ ohne weitere Zusätze gesprochen wird, ist damit ausnahmslos die direkte Form der *Cyberkriminalität im engeren Sinne* gemeint, im Sinne der Definition des BKAs: „Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten“ (BKA, 2019, S. 3).

Auch in den Ausformulierungen der zugrundeliegenden Strafnormen liegt ein Unterschied zwischen *Cybercrime im engeren-* und *im weiteren Sinne*. Der Online-Drogenhandel ist ein Verstoß gegen das Betäubungsmittelgesetz, unabhängig davon, ob die Transaktion im Darknet oder analog abgewickelt wurde. Das Internet oder Computer sind in diesem Fall also *kein* wörtlicher Bestandteil der betreffenden Gesetzesformulierungen. Wernert (2021, S. 35) weist darauf hin, dass bei *Cyberkriminalität im engeren Sinne* Computer oder andere IT-

Elemente wörtlich Teil der Strafnormen sind, wie das z.B. bei § 263a StGB (**Computer**betrug) oder § 303b StGB (**Computers**abotage) der Fall ist.

Während bei Hacking oder dem Drogenhandel eine klare Zuordnung und Abgrenzung möglich ist, stellt das ‚Carding‘, also der Kreditkartenbetrug, eine Ausnahme bzw. einen Grenzfall dar. Theoretisch wäre Kreditkartenbetrug auch in der analogen Welt möglich, weshalb Huber & Pospisil (2020) Carding der *Cyberkriminalität im weiteren Sinne* zuordnen. Im Sinne der genannten Definitionen müssten beim Carding theoretisch zwei Phasen unterschieden werden: Die Phase 1, das Abfangen von Kreditkartendaten durch Phishing oder das Hacken von Firmendatenbanken, wäre *Cyberkriminalität im engeren Sinne*, also Hacking in seiner reinsten Form. Wenn diese Daten im Anschluss jedoch auf Darknet-Marktplätzen zum Kauf angeboten oder gekauft werden, wäre dies *Cyberkriminalität im weiteren Sinne*. Die Praxis und ein Blick in die einschlägigen Hacker-Foren im Clear- und Darknet zeigen jedoch, dass Carding, Hacking und Phishing untrennbar miteinander verwoben sind. Fast alle Hacker-Foren haben ein Unterforum, welches sich ausschließlich dem Thema *Carding* widmet. Der Handel mit gestohlenen Kreditkartendaten und der Austausch darüber ist in manchen Hacker-Foren wie z.B. bei Best Carding World (Darknet, siehe Abb. 2) die Hauptaktivität.

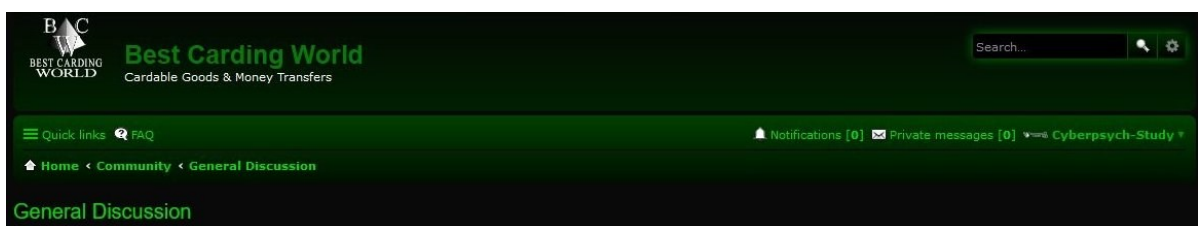


Abbildung 2. Screenshot Best Carding World (2025) (Darknet-Forum)

Für viele Hacker könnte das Carding auch einen Einstieg in die Cyberkriminalität bieten. Aus den genannten Gründen wird das Carding hier der *Cyberkriminalität im engeren Sinne* zugerechnet, ansonsten wird *Cybercrime im weiteren Sinne*, wobei das Internet nur als Medium genutzt wird, strikt ausgeschlossen.

An diese strikte Differenzierung von *Cybercrime im engeren- und weiteren Sinne* halten sich interessanterweise auch Täter: Die Hacker-Foren im Darknet werden von Administratoren moderiert. Die meisten Beiträge müssen also erst von Moderatoren autorisiert werden, bevor sie für andere Nutzer sichtbar werden. Grundregel ist hierbei, dass nur hackingbezogene Beiträge geduldet werden (was aber auch das *Carding* einschließt). Insbesondere werden in den reinen Hacker-Foren keinerlei kinderpornografische Inhalte in jeglicher Form geduldet und auch keine Diskussionen über Drogen oder Waffen. Hier ziehen auch Hacker eine klare inhaltliche und moralische Grenze. Damit ist festzuhalten, dass nicht nur die Strafverfolgungsbehörden und Forschung eine Grenze ziehen zwischen *Cybercrime im engeren-* und *Cybercrime im weiteren Sinne*, sondern auch Hacker selbst.

2.1.1 Arten von Cybercrime im engeren Sinne

Die Strafnormen zu Cyberkriminalität, wie § 202b StGB (Abfangen von Daten) oder § 263a StGB (Computerbetrug), sind sehr allgemeine Formulierungen und fassen verschiedene Angriffsmethoden zusammen, wobei das Abfangen von Daten durch sehr unterschiedliche Angriffsmethoden geschehen kann. Einige relevante Formen seien hier exemplarisch genannt, wobei die Liste keinen Anspruch auf Vollständigkeit erhebt.

Keylogger haben meistens die äußere Erscheinungsform eines USB-Sticks; werden sie jedoch an einen Computer angesteckt, wird im Hintergrund unbemerkt ein Programm ausgeführt, das ab diesem Zeitpunkt alle Tastatureingaben aufzeichnet und mit dem Angreifer teilt, um so Zugangsdaten zu Systemen oder dem Online-Banking auszuspähen (z.B. Kirwan & Power, 2013, S. 110).

Bei sogenannten *Man-in-the-middle-Angriffen* handelt es sich z.B. um kompromittierte öffentliche WLANs in Cafés, Flughäfen oder Hotels, bei denen ein Angreifer probiert, sensible Daten abzufangen (Conti, Dragoni & Lesyk, 2016).

Der wohl bekannteste, relevanteste und auch am weitesten verbreitete Angriffsvektor ist das *Phishing*, also E-Mails, die z.B. simulieren, von der eigenen Bank zu stammen, und auf eine

gefälschte Website leiten, die Nutzer unter Zeitdruck und Emotion auffordert, Zugangsdaten einzugeben (z.B. Kirwan & Power, 2013, S. 113-116).

Social Engineering beschreibt das Ausnutzen der „Schwachstelle Mensch“ (Huber, 2019, S. 32), indem Personen am Telefon aufgefordert werden, ihre Zugangsdaten preiszugeben, indem jemand beispielsweise behauptet, der Microsoft-Support oder ein Mitarbeiter der Bank zu sein.

Auch *DDoS-Angriffe* sind ein beliebtes Werkzeug im Methodenarsenal krimineller Hacker. DDoS-Angriffe sind bildlich gesprochen Überlastungsangriffe, wobei die Abkürzung DDoS für *Distributed-Denial-of-Service* steht (siehe z.B. BSI, 2025b). Das Ziel besteht darin, Internetseiten der Opfer lahmzulegen. Das technische Wirkprinzip eines DDoS-Angriffs lässt sich an einem alltäglichen Beispiel verdeutlichen. Beginnt der Vorverkauf für Karten eines beliebten Konzertes, probieren oft tausende Nutzer simultan, auf eine bestimmte Internetseite zuzugreifen. Der massenhafte, simultane Zugriff kann in einigen Fällen dazu führen, dass die Seite durch Überlastung kollabiert. In Fällen gezielter DDoS-Angriffe führen Hacker diesen Effekt künstlich herbei, indem sie sogenannte *Botnetze* instrumentalisieren, um massenhafte automatisierte Anfragen zeitgleich an eine bestimmte Webseite zu senden.

Laut Tavakkoli, Çetin, Ekmekcioglu, Savaş, ErKay (2025, S. 63-64) konnten seit dem Ukrainekrieg verstärkt pro-russische DDoS-Angriffe festgestellt werden, d.h. diese Angriffsform sei zu einem Mittel der geopolitischen Kriegsführung geworden.

Malware ist ein zusammengesetztes Wort aus engl. *malicious* (schädlich) und *Software*, also eine übergeordnete Kategorie für Schadsoftware jeglicher Art (Kirwan & Power, 2013, S. 79-84). Beispiele für *Malware* sind Viren, Würmer, Spyware oder Trojaner.

Ransomware ist die bekannteste und wahrscheinlich destruktivste Art der Malware und gemäß Daten des Bundeskriminalamtes aktuell das Hauptrisiko für die meisten Unternehmen (BKA, 2025a, S. 2). *Ransomware* ist Erpressungssoftware, die Dateien oder Netzwerke verschlüsselt, was zum Stillstand in Unternehmen führen kann, um dann eine

Lösegeldforderung in Form von Kryptowährung (meist Bitcoin) zu stellen (siehe z.B. Dreißigacker et al., 2020, S. 322). Nach Wernert (2021) sind *Ransomware-Angriffe* (Cybererpressungen) zu einem „Massenphänomen im Bereich Cybercrime“ (S. 164) geworden. Während dies für Unternehmen einen Produktionsstillstand bedeuten kann, kann ein Stillstand in Krankenhäusern potentiell Gesundheit oder Menschenleben gefährden (Al-Qarni, 2023; Neprash et al., 2022). Ausgelöst durch das Öffnen eines Anhangs oder Klicks auf einen Link, probieren Ransomware-Akteure, ihre Zugriffsrechte in einem Netzwerk immer mehr auszuweiten und schließlich Stillstand der Systeme durch Verschlüsselung zu erreichen. Metaphorisch ließe sich das Geschäftsmodell *Ransomware* als ‚Daten-Geiselnahme‘ klassifizieren. Häufig drohen Hacker zusätzlich damit, die sensiblen Daten des Unternehmens (falls das Unternehmen beschließt, nicht zu zahlen) im Darknet zu veröffentlichen; man spricht hier von *Double Extortion*, also einer Zweifach-Erpressung (z.B. Kerns, Payne & Abegaz, 2022). Gerade bei Banken, Versicherungen oder Krankenhäusern geht es um hochsensible Finanz- oder Gesundheitsdaten, die unter keinen Umständen im Darknet landen sollten. Dieser drohende Vertrauensverlust erhöht den Druck auf die gehackten Unternehmen noch weiter. Erst nachdem das Lösegeld (engl. *ransom*) in Form von Bitcoin oder anderen Kryptowährungen gezahlt wurde, geben die Kriminellen die Systeme wieder frei (so zumindest das Versprechen). Die Lösegeldforderung wird dabei an die Unternehmensgröße angepasst.

Nach Wernert (2021, S. 30) sei insbesondere bei Cybercrime gegen Unternehmen aus zwei Gründen von einer niedrigen Bereitschaft zu Strafanzeigen auszugehen: entweder aus Sorge vor Imageverlusten oder weil das Eindringen in die Firmensysteme gar nicht bemerkt wurde. Dass Taten tatsächlich unbemerkt bleiben, ist z.B. bei Spionage nicht ausgeschlossen, da hier seitens der Angreifer keine Notwendigkeit besteht, Opfer über den Angriff zu informieren. Gerade die Firmen, die sich entschieden haben, das Lösegeld in Ransomware-Erpressungen zu zahlen, kommunizieren dies selten nach außen. Würde man nur die mediale Außendarstellung von Firmen bei Cybervorfällen betrachten, dürfte Ransomware kein

lukratives Geschäftsmodell sein. Dies steht aber im Missverhältnis zu den wahren Einnahmen der Ransomware-Gruppierungen (BKA, 2025a).

Die genannten Arten von *Cybercrime im engeren Sinne* sind Beispiele ohne Anspruch auf Vollständigkeit. Das Ziel dieses Kapitels bestand darin, die Begriffe *Cybercrime im engeren Sinne*, durch Praxisbeispiele zu ergänzen. Bei der Betrachtung einzelner Angriffsmethoden wird auch deutlich, warum die Mehrzahl der Cyberangriffe auf menschliche Fehler zurückgehen (Liginlal et al., 2009, S. 221). Das Öffnen einer Phishing-E-Mail, das Anstecken eines USB-Sticks, der auf dem Flur oder Firmenparkplatz gefunden wurde, das Herausgeben von Zugangsdaten am Telefon, das ungeschützte Verbinden mit dem Hotel-WLAN, das Öffnen von Anhängen, welche Malware enthalten, sind allesamt menschliche Fehler. Diese Beispiele zeigen, dass Cyberkriminalität auf der Seite der Täter und Opfer nicht nur ein technisches, sondern auch ein psychologisches/verhaltensbezogenes Phänomen darstellt.

2.2 Definitionen Hacker und Darknet

2.2.1 Ursprung des Hackerbegriffs

Hören Menschen heutzutage das Wort ‚Hacker‘, assoziieren sie es wahrscheinlich mit Cyberkriminellen in Gestalt von Teenagern in schwarzen Kapuzenpullovern, entsprechend dem medialen Klischee. Hacking ist heute negativ konnotiert, war ursprünglich aber sogar *positiv* besetzt (Huber, 2019, S. 33; Kirwan & Power, 2013, S. 53). In der Zeit des *ARPANET* und zu Beginn der technologischen Entwicklung der Digitalisierung mit Computern entstand nach Chiesa et al. (2009, S. 33) im universitären Umfeld der USA (u.a. dem MIT) eine sogenannte Hacker-Subkultur. Das *Jargon File*, welches manchmal auch *Hackers Dictionary* genannt wird, spiegelt diese Zeit und beschreibt die damalige Hacker-Subkultur und deren *Slang* (Chiesa et al., 2009, S. 33; Jargon File, 1992). Hierin wird Hacking u.a. beschrieben als „intellectual challenge of creatively overcoming or circumventing limitations“ (Jargon File, 1992, S. 199). Demnach beschrieb Hacking damals neben technischer Versiertheit vor allem eine Geisteshaltung, die sich durch Neugierde, Kreativität, Grenzenlosigkeit und Interesse an

innovativer Problemlösung beschreiben lässt. Ein Hack war also „das Finden einer kreativen Lösung zu einem technischen Problem“ (Huber, 2019, S.33).

Früher war der Begriff eher positiv besetzt und erst durch begriffliche Abgrenzung, wie *Cracker*, wurde auf das kriminelle Hacking hingewiesen (Chiesa et al., 2009, S. 34). Heute ist das Verhältnis andersherum: Der Hackerbegriff ist heute negativ konnotiert und erst durch den sprachlichen Zusatz des *Ethischen Hackings* oder *White Hat Hackings* weist man auf die konstruktive oder legale Seite des Hackings hin. Nach Chiesa et al. (2009) neigt die gesellschaftliche Wahrnehmung eher zu Extremen: „Society's (sic!) representation [...] either demonize them or turn them into legends“ (S. 33).

Sprachlich haben sich verschiedene Begriffe etabliert, um Hacker zu kategorisieren, u.a. nach dem Niveau der technischen Fähigkeiten, Motivation oder Angriffsform (Übersicht: Kirwan & Power, 2013, S. 56-57). Im Rahmen dieser Arbeit geht es vor allem um motivationale Faktoren, also die Frage, warum manche Personen sich entscheiden, Straftaten zu begehen, während andere ihre Fähigkeiten im legalen Sinne einsetzen. Deshalb werden im Rahmen dieser Arbeit die Begriffe ‚White Hat Hacker‘ und ‚Black Hat Hacker‘ verwendet. Das ist nicht nur eine moralische, sondern auch rechtliche Abgrenzung, da z.B. Penetrationstester autorisiert und im Sinne der jeweiligen Organisationen agieren. Black Hats hacken hingegen unautorisiert (Huber, 2019, S. 34). Kirwan & Power (2013, S. 54) weisen jedoch darauf hin, dass es Fälle gibt, in denen White Hats *unautorisiert* in ein Unternehmensnetzwerk eindringen und danach die gefundene Sicherheitslücke dem Unternehmen melden. Gerade aufgrund dieser Grenzfälle ist eine klare Begriffsdefinition nötig.

2.2.2 Black Hat Hacker und White Hat Hacker

Huber (2019, S. 32) definiert Hacking als „das Eindringen ein Computersystem“. Das beschreibt also erst einmal nur eine technische Fähigkeit, unabhängig vom Zweck des Eindringens. Während Black Hats Sicherheitslücken suchen, um diese auszunutzen, probieren White Hats ebenfalls Schwachstellen zu identifizieren, aber nicht, um diese auszunutzen, sondern um Unternehmen zu helfen, diese Lücken zu schließen. Alternativ

werden diese Hacker auch als „ethical hacker“ (Chiesa, Ciappi & Ducci, 2009, S. 239) bezeichnet. Gelegentlich wird der Begriff der ‚Gray Hat Hacker‘ für eine dazwischenliegende Kategorie verwendet, die manchmal auch als „Hacktivist“ (BKA, 2015a, S. 1) bezeichnet werden. Gray Hats brechen zwar auch das Gesetz, da sie sich unautorisiert Zugang zu Systemen verschaffen, allerdings aus ideologischen oder aktivistischen Gründen (Huber, 2019, S. 34-35). Das bekannte Hackerkollektiv Anonymous hat in der Vergangenheit z.B. die Terrororganisation IS angegriffen (Martins, 2017). Fälle wie dieser werfen zwar moralisch hochinteressante Fragestellungen auf, diese Hackerkategorie ist jedoch schwer operationalisier- und abgrenzbar und soll ausgeschlossen werden, da Gray Hats sich weniger eindeutig der ‚hellen‘ oder ‚dunklen‘ Seite des Hackings zuordnen lassen.

In Anlehnung an die Definition von Kerschull (2023, S. 4), Huber (2019, S. 34) und Kirwan & Power (2013, 53-55) werden Black Hat Hacker und White Hat Hacker im Rahmen der Studien wie folgt definiert:

Black Hat Hacker sind Personen, die bewusst und unautorisiert Taten im Bereich von *Cybercrime im engeren Sinne* zum Schaden von Unternehmen, Einzelpersonen oder Institutionen begehen oder kürzlich (innerhalb der letzten 12 Monate) begangen haben (als Einzelperson oder Teil einer Gruppe) mit dem Motiv, sich selbst zu bereichern oder anderen destruktiven, egoistischen Motiven. Auch staatliche Akteure und Hacker, die im Auftrag von Nachrichtendiensten andere Staaten ausspionieren oder hacken, sind Black Hat Hacker, selbst wenn sie im Sinne des Strafrechts ihres Heimatlandes keine Straftat begehen, sondern ihren Dienst ausführen.

In Abgrenzung dazu werden White Hats wie folgt definiert:

White Hat Hacker sind Programmierer, Sicherheitsforscher, IT-Spezialisten, Ethische Hacker oder Penetrationstester, also Personen, die Hackingfähigkeiten haben oder auch aktiv Schwachstellen in Systemen suchen, jedoch nicht mit dem Ziel diese auszunutzen, sondern die Cybersicherheit von Unternehmen oder Institutionen zu verbessern. Sie handeln autorisiert und verantwortungsvoll, hätten aber grundsätzlich die Fähigkeit und das Know-How ein Black Hat Hacker zu sein.

Die Definitionen sind so allgemein wie nötig und so spezifisch wie möglich. Natürlich ließe sich das ‚Hacking‘ viel feinteiliger nach der Art der Delikte, Fähigkeitslevel oder Strafnormen differenzieren. Aus forschungsökonomischen Gründen ist es jedoch sinnvoll, die Definition

zu Black Hats recht breit zu halten, um möglichst viele Personen einzuschließen, da die Rekrutierung von Probanden ohnehin schwierig ist.

Im Folgenden sollen einige Grenzfälle aufgezeigt werden und wie diese im Rahmen der Arbeitsdefinitionen klassifiziert werden würden.

Es gibt beispielweise eine Reihe von Hackern, die die Seiten wechseln, das prominenteste Beispiel war Kevin Mitnick († 2023). Mitnick war Cyberkrimineller und wurde nach seiner Haftstrafe ein gefragter Sicherheitsexperte (Kirwan & Power, 2013, S. 51). Es ist davon auszugehen, dass es einige White Hat Hacker gibt, die ihre Fähigkeiten in der Jugend zu kriminellen Zwecken genutzt oder sich in ethischen und rechtlichen Grenzbereichen ausprobiert haben. Deshalb ist in der Definition das zeitliche Kriterium enthalten: „begehen oder *kürzlich (innerhalb der letzten 12 Monate)* begangen haben“.

Es gibt außerdem eine Reihe von Kindern und Jugendlichen, die Cyberstraftaten aus Unwissenheit oder mangelnder Medienkompetenz begehen, weshalb viele Präventionsprogramme hier ansetzen (Aiken, Davidson & Amann, 2016). Aus diesem Grund ist in der Definition zu Black Hats das Kriterium der *Bewusstheit* enthalten, um nur Black Hats einzuschließen, die wissentlich gegen Gesetze verstoßen.

Das Hauptkriterium der Definition zu Black Hat Hackern ist die *Kriminalität*. In diesem Zusammenhang ist die kriminologische Theorie des Etikettierungsansatzes zu nennen, welche nach Mentzel & Schröder 2015, S. 36) besagt, dass Kriminalität nicht einfach ‚gegeben‘ ist, sondern erst durch die Selektion der Polizei entsteht, die somit entscheidet, wem das Label ‚kriminell‘ zugeschrieben wird. Ob ein Verhalten als kriminell oder nicht kriminell gesehen und verfolgt wird, kann sich im Zeitverlauf ändern und nach Huber (2019, S. 23) zwischen Ländern sehr unterschiedlich gesehen werden. Im Zusammenhang mit Cyberkriminalität ist dies erwähnenswert, da es sich um einen neueren Deliktsbereich handelt. Wernert (2021, S. 36) weist darauf hin, dass von staatlicher Seite erst 2007 durch ein Strafrechtsänderungsgesetz auf Cyberkriminalität reagiert wurde.

Die oben genannte Definition des Bundeskriminalamtes zu *Cybercrime im engeren Sinne* stellt damit eine deutsche bzw. westliche Perspektive dessen dar, wer als Black Hat Hacker klassifiziert wird. Cyberangriffe gegen westliche Unternehmen werden zum Teil von Nachrichtendiensten geopolitischer Kontrahenten gelenkt, gefördert oder zumindest toleriert; der Fachbegriff hierfür sind „nation-state-sponsored cyberattacks“ (Holt, Griffith, Turner, Greene-Colozzi, Chermak & Freilich, 2023, S. 825). Ein Hacker, welcher im Ausland residiert und Cyberangriffe gegen Unternehmen oder Einzelpersonen ausführt, würde als Black Hat Hacker im Rahmen der Studien definiert werden, selbst wenn sein Verhalten möglicherweise im Heimatland *nicht* als kriminell angesehen wird. Ein Mitarbeiter eines ausländischen Geheimdienstes, der Cyberangriffe gegen deutsche, kritische Infrastruktur ausführt, begeht im Heimatland keine Straftat, wohl aber im Sinne des deutschen Staates, in dem die Opfer ansässig sind. Die Definition, was kriminell und unautorisiert ist, orientiert sich also am Ansässigkeitsstaat der Opfer, nicht der Täter.

Beim Sampling sollen möglichst Probanden ausgewählt werden, die eindeutig Black Hat Hacker sind (z.B. Cracker in Darknet-Foren) oder eindeutig White Hat Hacker (z.B. Penetrationstester). Möglichst ausgeschlossen werden sollen Gray Hat Hacker und andere uneindeutige Fälle.

Es sei zudem erwähnt, dass sich die Kategorien theoretisch nicht ausschließen. Manche Black Hat Hacker haben ggf. einen normalen Job und eine bürgerliche Fassade, das heißt, sie arbeiten offiziell in der Cybersicherheit oder IT-Abteilungen und nutzen privat oder am Wochenende die Fähigkeiten, um sich selbst zu bereichern.

Wer *Cyberkriminalität im engeren Sinne* innerhalb der letzten 12 Monate begangen hat, soll als Black Hat Hacker definiert werden.

2.2.3 Abgrenzung Darknet, Deepweb, Clearnet

Im Rahmen dieser Arbeit werden Black Hat Hacker vor allem in Hacker-Foren im Clear- und Darknet rekrutiert. Doch was genau versteht man unter dem Darknet und wie gelangt man dorthin?

Es wird auf eine technische Erklärung der Anonymisierungsmechanismen im Darknet verzichtet, da dies eigenständige Bücher füllt; die Begriffe Clearnet, Deepweb und Darknet sollen jedoch kurz erläutert und voneinander abgegrenzt werden.

Das *Clearnet* stellt nach Henkel (2020, S. 175) den sichtbaren Teil des Internets dar, also Webseiten, die über Suchmaschinen wie *Google* auffindbar sind und sich über normale Browser öffnen lassen. Die Seite *www.uni-tuebingen.de* ist somit gemäß der Definition Bestandteil des Clearnets, da sie über Google auffindbar ist und mit Browsern wie Firefox, Safari, Chrome oder dem Internet Explorer zugänglich. Synonyme für das *Clearnet* sind das *Surface Web* oder *Visible Web* (Henkel, 2020, S. 175). Schon die Begriffe ‚sichtbar‘, ‚klar‘ und ‚Oberfläche‘ verdeutlichen, dass die beiden Wesensmerkmale des Clearnets die Sichtbarkeit und Auffindbarkeit sind.

Die öffentlich sichtbare Website der Universität Tübingen stellt jedoch nur einen Bruchteil der Datenströme dar. Laut ZDV (2025) übertragen insgesamt 45.000 Nutzer der Universität Tübingen 70 TB Daten am Tag. Die meisten dieser Datenströme sind aber nicht öffentlich einsehbar, sondern z.B. vertrauliche E-Mail-Kommunikation, Datenbanken im Hintergrund, das Intranet und alles, was sich passwortgeschützt hinter einem Login verbirgt. Das ist Teil des *Deepwebs*, also dem ‚tiefen‘, nicht öffentlich auffindbaren Teil des Internets unter der Oberfläche. Es sind nach Henkel (2020, S. 175) Seiten, die zwar über normale Browser aufrufbar sind, aber nicht über Google auffindbar. Im Online-Banking wäre das Clearnet die öffentliche Webseite der Bank. Die Seiten hinter dem Login, in denen der persönliche Kontostand und alle Transaktionen sichtbar sind, sind Teil des Deepwebs. Anhand der Beispiele soll deutlich werden, dass die meisten Daten des Deepwebs nicht deswegen geschützt und nicht sichtbar sind, weil sie illegal wären, sondern weil sie schlicht vertraulich sind. Das Deepweb ist ein Oberbegriff für alle Daten unter der sichtbaren Oberfläche des Internets.

Das Darknet ist somit nach Haider (2023, S. 527) nur ein kleiner Teil des Deepwebs. Seiten im Darknet sind nicht über ‚normale‘ Browser aufrufbar, sondern nur über dedizierte Software, wie das Tor-Netzwerk (Wernert, 2021, S. 95). Seiten im Darknet werden deshalb *Hidden*

Services genannt und enden auch nicht auf *.de* oder *.com*, sondern auf *.onion*. Zum Aufruf solcher *.onion-Links* braucht es den Tor-Browser, wobei TOR die Abkürzung ist für „The Onion Router“ (The Tor Project, 2025; Wernert, 2021, S. 96). Die Metapher der Zwiebel ist eine Anspielung auf die technologische Funktionsweise der Anonymisierung im Darknet. Die wahre Identität, also die IP-Adresse² eines Nutzers, wird im Sinne mehrerer Zwiebelschichten verborgen (Wernert, 2021, S. 95). Ruft ein Nutzer eine Internetseite im Clearnet auf, kann der Seitenbetreiber die IP-Adresse als Zahlenfolge sehen. Strafverfolgungsbehörden könnten über eine Abfrage der IP-Adresse beim Telekommunikationsanbieter (Internet-Provider) den Klarnamen und die Wohnanschrift des Nutzers herausfinden. Diese Form der einfachen IP-basierten Deanonymisierung funktioniert so im Darknet nicht, denn die Anfrage eines Users wird über mehrere Knotenpunkte umgeleitet (Wernert, 2021, S. 95). Die IP-Adresse, die letztlich bei dem *Hidden Service* ankommt, hat mit der wahren IP-Adresse des wahren Nutzers nichts mehr zu tun. Aufgrund dieser zwiebelschichtigen Anonymität und Verschlüsselung wird im Darknet erstaunlich offen über Hacking, Drogenhandel und alle möglichen anderen Arten der Kriminalität gesprochen und gehandelt. Beahlt wird mit anonymen oder pseudonymen Kryptowährungen (Haider, 2023, S. 527), d.h. auch hier ist eine Aufdeckung der wahren Identität nur umständlich möglich, wenn überhaupt. Hacker (auch White Hats) betonen gerne, dass es falsch sei, das Darknet per se als kriminell darzustellen, da der Wunsch nach Anonymität an sich kein Verbrechen ist und es positive Anwendungsbeispiele gibt. Henkel (2020, S. 179) betont, dass digitale Anonymität für viele kritische Journalisten oder Dissidenten in autoritären Staaten überlebensnotwendig sein kann, und verweist auch auf die Rolle des Tor-Netzwerks beim arabischen Frühling (S. 179). Es gibt auch andere positive Beispiele, aber es sind seltene Ausnahmen. Owen und Savage (2016) haben über sechs Monate selbst einen Server im Tor-Netzwerk betrieben, um den Datenverkehr überwachen können. Sie haben über 80.000 Hidden Services im Darknet entdeckt, wovon die Mehrzahl eindeutig kriminellen Aktivitäten zuzuordnen war.

² Die IP-Adresse ist eine eindeutige Identifikationsnummer eines Gerätes.

Während mehrerer Jahre Analysen und Recherche im Darknet und monatelanger Probandengewinnung in Hacker-Foren im Rahmen dieser Arbeit wurde deutlich, dass das Darknet ein dunkler Ort ist und fast nichts, was dort besprochen oder gehandelt wird, legal ist. Eine Ausnahme ist die *.onion*-Seite *Bible4u* im Tor-Netzwerk, auf der es tatsächlich lediglich die Bibel zu lesen gibt, da es Länder gibt, in denen das Mitführen einer Bibel zu Verfolgung führen kann. Das Darknet zum Lesen der Bibel zu nutzen, dürfte eine seltene Ausnahme darstellen und ändert nichts an der Regel, dass die Anonymität im Darknet primär deswegen geschätzt wird, weil dort Cyberkriminalität und andere Formen der schwersten Kriminalität praktiziert und diskutiert werden.

Zusammenfassend lässt sich festhalten: Das Clearnet ist der sichtbare Teil des Internets, das Deepweb der verborgene Teil unter der Oberfläche, und das Darknet ist der dunkle Teil des Deepwebs (Übersicht: Henkel, 2020).

2.2.4 Crime-As-a-Service-Strukturen und Dark Economy

Das Darknet und die mehrschichtig-strukturierte Anonymität des Tor-Netzwerks bilden die technische Grundlage für eine florierende Wirtschaft auf der ‚dunklen Seite‘: „Gemeinsamer Nenner der meisten Bedrohungen im Cyberraum ist die Underground Economy. Sie ist die Gesamtheit aller kriminellen Plattformen und Marktplätze und nimmt daher eine zentrale Rolle im Phänomenbereich ein“ (BKA, 2025a, S. 10). Über sogenannte *Phishing Kits* lassen sich eigene Phishing-Angriffe auch für weniger technisch versierte Akteure leicht realisieren (BKA, 2025a, S. 14). Sogenannte *Initial Access Broker* verkaufen gestohlene Zugangsmöglichkeiten in Unternehmensnetzwerke (BKA, 2025a, S. 10). Ransomware-Akteure können diese Zugänge kaufen und über *Loader* and *Dropper* ihre eigene Schadsoftware im anzugreifenden Netzwerk platzieren (BKA, 2025a, S. 16). *Counter-Antivirus-Services* bieten teils im Abomodell die Möglichkeit, eigene Malware daraufhin zu überprüfen, ob sie von gängigen Virenschutzprogrammen tatsächlich unerkannt bleibt (BKA, 2025b). *Krypto-Exchange-Dienste* werden dann zur Geldwäsche missbraucht (BKA, 2025a, S. 29), um es in Fiat-Währungen auszuzahlen oder direkt in anderen Darknet-Marktplätzen auszugeben. Anhand der Beispiele des Bundeskriminalamtes wird deutlich, dass die

Beschreibung einer ‚Dark Economy‘ dabei nicht metaphorisch gemeint ist, sondern es sich tatsächlich um eine hochprofessionelle, arbeitsteilige Wirtschaftsform handelt.

Die Tatsache, dass die Dark Economy eine Infrastruktur darstellt, in der Akteure Hacking-Dienstleistungen extern einkaufen können, hat wichtige Implikationen für die Definition von Hackern und den Umgang mit Hackern, die sich derartiger Angebote bedienen. Es geht dabei um die Frage, ab welchem Grad der Fremdleistung einem Hacker das ‚Hackersein‘ abzusprechen wäre. Metaphorisch ausgedrückt, geht es um die Frage, ob jemand, der eine Backmischung zum Brotbacken nutzt, noch als Bäcker zu definieren wäre. Abbildung 3 zeigt beispielhaft zwei angebotene Dienstleistungen eines Darknet-Marktplatzes.

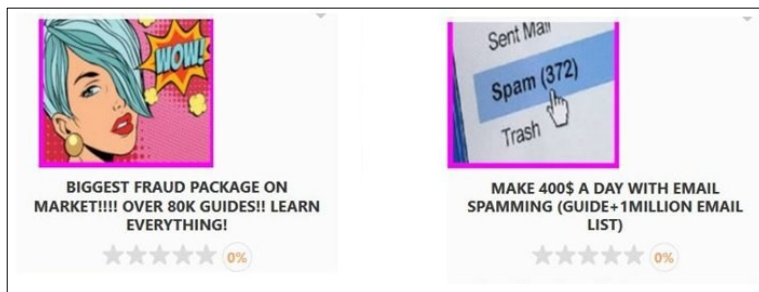
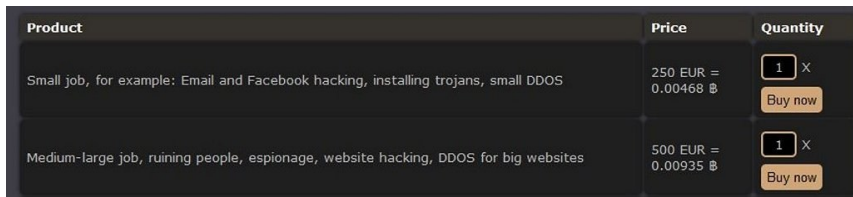


Abbildung 3. Screenshot Darknet-Marktplatz Vortex (2025): Angebote der Dark Economy

Die Abbildung 3 zeigt z.B. ein ‚Phishing-Kit‘, also eine Sammlung von Ressourcen, das alles enthält, um eigene Phishing-Kampagnen autonom durchzuführen. Dies wären in der Metapher des Bäckers Rezepte oder fertige Backmischungen. Wäre das Interesse dieser Arbeit, Hacker nach dem Niveau ihrer Fähigkeiten zu kategorisieren, von *Script Kiddies* bis Profis (siehe Kirwan & Power, 2013, S. 56), müsste man diese Täter mit niedrigem technischem Fertigniveau ausschließen. Das Interesse und Kategorisierungsmerkmal dieser Arbeit ist aber *nicht* das Level der technischen Fähigkeiten, sondern die Richtung des Motivs (Black Hats vs. White Hats). Selbst wenn ein Hacker Werkzeuge aus dem Darknet für die Angriffe verwendet, ist er/sie selbst die ausführende Person.

Abbildung 4 zeigt ein noch weitergehendes Beispiel eines Auftragshackers. Auf der Darknet Seite des Dienstleisters ist es möglich, Hacking als externe Dienstleistung zu buchen, z.B. werden DDoS-Angriffe für 250,00 € (zahlbar in Form von Bitcoin) angeboten.



Product	Price	Quantity
Small job, for example: Email and Facebook hacking, installing trojans, small DDOS	250 EUR = 0.00468 ₿	1 X Buy now
Medium-large job, ruining people, espionage, website hacking, DDOS for big websites	500 EUR = 0.00935 ₿	1 X Buy now

Abbildung 4. Screenshot: Anonymer Auftragshacker (2025) (Darknet)

In der Metapher des Backens wäre dies keine Backmischung oder kein Rezept mehr, sondern schlicht der Akt, ein Brot zu kaufen. Der Bäcker ist darin der Anbieter der Dienstleistung, aber nicht der Kunde, der diese Leistung kauft.

Wenn jemand sich also Anleitungen, Dienstleistungen oder Werkzeugen der Dark Economy bedient, um damit selbst *Cyberkriminalität im engeren Sinne* zu begehen, ist er/sie als Black Hat zu definieren. Erst wenn jemand Hacking als Dienstleistung bucht, ohne jegliches eigenes Zutun, wäre die Person nicht mehr als Black Hat zu klassifizieren.

Dieselbe Abgrenzung und Definition gilt auch für die zunehmende Nutzung künstlicher Intelligenz, auf die auch das Bundeskriminalamt im Bundeslagebild Cybercrime (BKA, 2024, S. 24) hinweist. Nutzt ein Hacker Generative künstliche Intelligenz zur Recherche oder Unterstützung der eigenen Angriffe, indem die KI z.B. Anleitungen gibt („Rezepte“) oder Quellcode generiert („Backmischungen“), ist die Person trotzdem ein Black Hat Hacker. Erst wenn die Generative KI vollständig selbst das Brot backt (ergo: eigenständig Cyberangriffe ausführt), müsste man hinterfragen, inwiefern die auftraggebende Person selbst als Hacker zu definieren wäre. Stand 2025 ist es möglich, KI als unterstützendes Werkzeug einzusetzen, wobei vollständig automatisierte Angriffe (noch) ein Zukunftsszenario sind (BKA, 2024, S. 24; BSI, 2024, S. 11).

2.3 Die Dunkle Triade

Psychopathie, Narzissmus und Machiavellismus sind distinkte, aber ähnliche Persönlichkeitskonstrukte, welche moderat miteinander korrelieren (siehe Abb. 5).

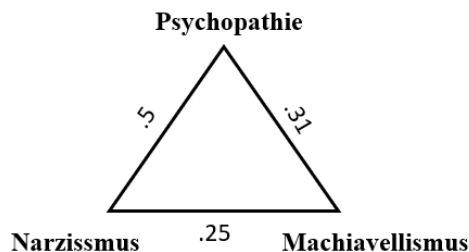


Abbildung 5. Korrelationen der Merkmale der Dunklen Triade untereinander

Quelle: Paulhus & Williams, 2002, S. 559. $N = 245$, signifikant bei $p < .001$, zweiseitig.

Zusätzlich fanden Paulhus & Williams (2002) für alle Triademerkmale negative Korrelationen unterschiedlicher Stärke mit der Big-5 Persönlichkeitsdimension der Verträglichkeit ($r = -.36$ für Narzissmus, $r = -.47$ für Machiavellismus und $r = -.25$ für Psychopathie) (S. 560). Diese geringe soziale Verträglichkeit, welche Paulhus & Williams (2002) als „common core of disagreeableness“ (S. 561) beschrieben, führte dazu, dass Psychopathie, Machiavellismus und Narzissmus zur Dunklen Triade gebündelt wurden und häufig gemeinsam als solche untersucht werden.

Buckels, Jones und Paulhus (2013) schlugen vor, die Dunkle Triade um Charaktersadismus zu ergänzen und somit zu einer Tetrade auszuweiten. Während manche Forscher für eine Ausweitung zur Tetrade plädieren, haben Andere angezweifelt, ob es sich tatsächlich um drei unterschiedliche Persönlichkeitseigenschaften handelt. Hauptkritikpunkt ist nach Gillespie & Garofalo (2024, S. 81) die Frage, ob das breite Konstrukt der Psychopathie nicht bereits narzisstische und machiavellistische Tendenzen mit abdeckt. Eine Meta-Analyse von Vize, Lynam, Collison & Miller (2018, S. 101) fand starke Überschneidungen zwischen Psychopathie & Machiavellismus, während Narzissmus sich unterschied. Auch Miller, Hyatt,

Maples-Keller, Carter & Lynam (2017, S. 439) hinterfragen daher, ob eine Unterscheidung von Psychopathie und Machiavellismus überhaupt sinnvoll ist.

Bisher hat sich jedoch weder eine Kürzung der Dunklen Triade auf zwei Merkmale noch die Ausweitung auf vier Merkmale durchgesetzt. Es ist daher sinnvoll, die drei Konstrukte gemeinsam zu untersuchen, aber separat zu messen und zwischen den Konstrukten zu unterscheiden (Paulhus & Williams, 2002). Im folgenden Kapitel werden daher die unterschiedlichen Konzeptionalisierungen und Operationalisierungen der einzelnen Konstrukte vorgestellt.

2.4 Psychopathie

2.4.1 Differenzierung subklinischer Psychopathie und ASPD

Grundsätzlich wird Psychopathie in den durchzuführenden Studien und im Rahmen der Arbeit als subklinisches Persönlichkeitsmerkmal betrachtet und untersucht. Sie soll daher inhaltlich und begrifflich von der antisozialen und dissozialen Persönlichkeitsstörung, abgegrenzt werden. Als Bestandteil der Dunklen Triade wird Psychopathie nicht im Sinne einer Taxonomie, sondern als kontinuierlich verteiltes Persönlichkeitsmerkmal betrachtet und auch in nicht-klinischen Kontexten, z.B. unter Führungskräften, untersucht. Frandrup (2023, S. 4) betont, „dass die Wirtschaftspsychologie [...] negative Persönlichkeitsmerkmale nicht als Krankheitsbilder betrachte[t], sondern sich mit deren Ausprägungen im subklinischen Bereich beschäftig[t]“.

Zwischen der subklinischen *Psychopathy*, der antisozialen (bzw. dissozialen) Persönlichkeitsstörung und Soziopathie bestehen wichtige Unterschiede. In den sogenannten ‚Diagnosebibeln‘, also den etablierten Klassifikationssystemen für psychische Störungen (ICD und DSM), stellt Psychopathie keine eigene Kategorie dar (Sarkar, Clark & Deeley, 2011, S. 191). Hautzinger & Thies (2009, S. 137) betonen, dass die Begrifflichkeiten häufig fälschlicherweise synonym verwendet werden. Die begriffliche Distinktion ist jedoch wichtig.

Bedeutsame Unterschiede zwischen Psychopathie und der ASPD und der dissozialen Persönlichkeitsstörung liegen sowohl in den zugrundeliegenden Definitionskriterien, als auch der Ätiologie. Während Psychopathie nach Hautzinger & Thies (2009, S. 137) vor allem das innere Erleben beschreibt, also Aspekte wie Empathie- oder Furchtlosigkeit, wird die dissoziale Persönlichkeitsstörung (ICD), bzw. ASPD (DSM), primär durch äußerlich beobachtbares Verhalten definiert. Auch Lykken (2019, S. 23) hebt deshalb kritisch hervor, dass die DSM-Klassifikationskriterien vor allem beobachtbare Verhaltensmerkmale (z.B. Kriminalität) im Sinne einer Checkliste aufführt. Nur rund ein Drittel der Personen mit der Diagnose einer ASPD fällt auch in die Kategorie der Psychopathie (Coid & Ullrich, 2010, S. 426). Psychopathie wird aus diesem Grund teilweise als „Unterform der antisozialen Persönlichkeitsstörung“ (Briken & Tozdan, 2018, S. 199) bezeichnet. Die Definitionsmerkmale der ASPD beziehen sich auf die Verhaltensebene, bilden aber die emotionalen Defizite nicht in dem Maße ab wie Psychopathie (Hautzinger & Thies, 2009, S. 137; Lykken 2019, S. 23).

Laut Lykken (2019, S. 23) lassen sich die psychopathische Furcht- und Empathielosigkeit zum Teil auf genetische Ursachen zurückführen; es besteht demnach auch ein zentraler Unterschied in der Ätiologie. Psychopathen zeigen strukturelle Defizite in den für Empathie und Emotion relevanten Hirnregionen, z.B. der Amygdala (Yang & Raine, 2019). Ist das antisoziale Verhalten wiederum nicht angeboren, sondern Ergebnis eines Lernprozesses (z.B. durch Erziehung, Subkultur oder das soziale Umfeld), fällt dies eher in die Kategorie der ASPD und wird manchmal auch als Soziopathie bezeichnet (Lykken, 2019, S. 23).

2.4.2 Operationalisierungen und Konzeptionalisierungen

Patrick (2019, S. 9) betont, dass es sich bei Psychopathie um ein weit gefasstes und mehrdimensionales und komplexes Konstrukt handelt. Bis heute konkurrieren unterschiedliche Modelle miteinander, die sich primär darin unterscheiden, welche Aspekte zu Psychopathie zählen und welche nicht. Bereits Skeem & Cooke (2010) wiesen darauf hin, dass darüber diskutiert wird, ob Kriminalität ein definitorischer Teil des Psychopathiekonstruktes ist oder eher als sekundäre Folge betrachtet werden sollte.

In der Gesamtbetrachtung der Literatur zur Historie der Erforschung sowie der Begriffsgenese (z.B. Schütte & Blickle, 2017; Brooks, Fritzon, Watt, 2020, S. 3-4; Brooks & Fritzon, 2020) lassen sich im Rückblick vier bedeutsame Entwicklungsstufen rekonstruieren, die zum heutigen Forschungsstand führten: Die Begriffsprägung durch Pinel im frühen 19. Jahrhundert, die erste Beschreibung durch Cleckley im Jahr 1941 (siehe Neuauflage: Cleckley, 1950/2015), die Operationalisierung durch Hare (1991) und die aktuelle, zunehmende Erforschung im Kontext der Wirtschaft und anderen nicht-klinischen Kontexten.

Im frühen 19. Jahrhundert (im Jahr 1806) beschrieb Pinel Psychopathie als „*manie sans délire*“ (zitiert nach Patrick, 2019, S. 4, Hervorhebung im Original). Auch in Lehrbüchern von 1912 finden sich Beschreibungen der sogenannten „psychopathischen Minderwertigkeiten“ (Elsenhans, 1912/1920, S. 413), „die nicht als normal bezeichnet werden, die aber doch auch noch nicht als Zeichen von Geisteskrankheit gelten können“ (S. 413). Obwohl der Begriff also bereits 1806 erwähnt wurde, existierte keine ausführliche Definition oder Beschreibung, welche Symptome oder Persönlichkeitsmerkmale charakteristisch wären.

Der amerikanische Psychiater Hervey Cleckley kritisierte, dass Psychopathie zwar in den Fachbüchern der damaligen Zeit erwähnt wird, die Kapitel darüber jedoch „often short, and sometimes vague or half-hearted“ (Cleckley, 1950/2025, S. 32) verfasst sind. Für ihn ist der Psychopath daher der „forgotten man of psychiatry“ (Cleckley, 1950/2015, S. 32). Cleckley blickte auf Jahre der Erfahrung mit Psychopathie zurück, die er an seinen Patienten aus allen Lebensbereichen beobachten konnte. Er nutzte zur Beschreibung des Konzeptes die Metapher der „Mask of Sanity“ (Cleckley, 1950/2015, Titel). Die *Maske der Vernunft* steht für eine angepasste Fassade, welche einen dunklen Persönlichkeitskern verbirgt. Aus seinen Fallstudien leitete Cleckley 16 Merkmale ab. Mit Kapiteln wie „The Psychopath as Businessman“ (Cleckley, 1950/2015, S. 214) beschrieb Cleckley auch Fallstudien angesehener Berufsgruppen, also nach heutigem Verständnis „Successful Psychopathy“ (Brooks et al., 2020, S. 23). Er vertrat somit einen Ansatz, der Psychopathie als „personality-based“ (Benning et al., 2019, S. 585) betrachtet. Für Cleckley war Gewaltkriminalität lediglich eine mögliche sekundäre Folge, aber kein definitorisches Merkmal (Schütte & Blickle, 2017,

S. 92). Cleckley beschrieb Psychopathie zwar ausführlich, aber operationalisierte sie nicht, - entwickelte also keine Skala, die Personen einen konkreten Zahlenwert zuordnet.

Der kanadische Kriminalpsychologe Robert D. Hare brachte den nächsten bedeutsamen Meilenstein der Psychopathieforschung durch die Entwicklung der Psychopathy-Checklist (PCL, später PCL-R, siehe Hare, 1991). Erstmals war Psychopathie damit operationalisierbar. Die Faktorstruktur des Instrumentes der PCL-R lässt sich durch zwei übergeordnete Faktoren beschreiben. Während Faktor 1 interpersonelle und affektive Aspekte beinhaltet, wie z.B. oberflächlichen Charme, pathologisches Lügen, Manipulation, Mangel an Empathie und Reue, bezieht sich Faktor 2 auf den Lebensstil und antisoziales Verhalten, z.B. Stimulationsbedürfnis, Impulsivität, ein parasitärer Lebensstil und Kriminalität (zur Übersicht: Hare & Neumann, 2008, S. 220, Abb. 2). Die Kriminalität ist für Hare (2005) also Teil von Psychopathie (S. 75-76). Hare ist selbst Kriminalpsychologe und hat somit nicht nur Cleckleys Auffassung von Psychopathie messbar gemacht, sondern auch selbst die Richtung verändert. Die PCL-R wurde an und mit männlichen (gewalt-)kriminellen Gefängnisinsassen entwickelt (Brooks et al., 2020, S. 14-15; Skeem & Cooke, 2010). PCL-R-Scores zeigen starke Korrelationen mit Kriminalität und Rückfälligkeit (Douglas et al., 2019, S. 682 ff.). Die Psychopathieprävalenz in der Allgemeinbevölkerung liegt bei 0,6 bis 1 % (Coid, Yang, Ullrich, Roberts & Hare, 2009). Unter Gefängnisinsassen ist die Psychopathieprävalenz nach Hare (2005, S. 76) deutlich höher und liegt bei durchschnittlich 20 %. Daher wurde Psychopathie lange Zeit fast ausschließlich mit Gewaltkriminalität in Verbindung gebracht und auch überwiegend im forensischen Kontext untersucht (Babiak, Neumann & Hare, 2010, S. 175). Robert D. Hares PCL-R Skala wurde nicht nur zum „gold standard psychopathy assessment“ (Brooks & Fritzon, 2020, S. 137), sondern zunehmend als „operational Definition“ (Pastwa-Wojciechowska, Kaźmierczak, Błażek, 2012, S. 119) für Psychopathie verwendet. Psychopathie war, was die PCL-R misst. Es ist jedoch keineswegs unproblematisch das Konstrukt mit dessen Messung gleichzusetzen, denn hierbei sollte die Generalisierbarkeit kritisch hinterfragt werden, ob die PCL-R tatsächlich Psychopathie als Persönlichkeitsdisposition bei allen Altersgruppen, Nationalitäten und Geschlechtern

beschreibt oder ausschließlich die spezielle Subgruppe der männlichen, gewaltkriminellen Psychopathen. Skeem & Cooke (2010, S. 433) resümierten daher: "Indeed, the field is in danger of equating the PCL-R with the theoretical construct of psychopathy". Alpers & Eisenbarth (2008, S. 8) kritisieren die mangelnde Differenzierung zwischen Handlungen und Persönlichkeitsdispositionen. Da die PCL-R u.a. auf Aktenanalyse basiert, ist sie nicht gut geeignet für die Forschung an und mit nicht-forensischen Populationen (Alpers & Eisenbarth, 2008, S. 13).

Nach der Etablierung der PCL-R als Standardverfahren, kann der nächste bedeutsame Meilenstein daher in der Entwicklung alternativer Messinstrumente gesehen werden, die besser für die Forschung außerhalb des Strafvollzugs geeignet sind (Brooks & Fritzon, 2020, S. 109). Levenson, Kiehl, & Fitzpatrick (1995) entwickelten anhand der PCL-R Items die Levenson Self-Report Psychopathy Scale (LSRP), bestehend aus 26 Items. Während Hare (1991) zwischen Faktor 1 und Faktor 2 differenziert, unterscheiden Levenson und Kollegen zwischen *primärer & sekundärer Psychopathie*. Nach Lykken (1995, S.132) ist primäre Psychopathie ein Ausdruck von Hares PCL-R Faktor 1, während sekundäre Psychopathie Hares Faktor 2 ähnelt. Die LSRP wurde jedoch nicht an Gefängnisinsassen entwickelt, sondern an einem Sample von Studenten, mit dem Ziel, ein Instrument für die Untersuchung von Psychopathie in nicht-forensischen Stichproben bereitzustellen (Levenson et al., 1995). Bis heute ist die LSRP eine häufig eingesetzte Skala in empirischen Untersuchungen, insbesondere außerhalb des Strafvollzugs (Brooks & Fritzon, 2020, S. 119). Patrick (2006) beschrieb diese Entwicklung mit den Worten „Back to the Future: Cleckley as a Guide to the Next Generation of Psychopathy Research“ (S. 605), um damit auszudrücken, dass die moderne Psychopathieforschung wieder dichter bei Cleckleys persönlichkeitsbasiertem Ansatz ist, als bei Hares Konzeptionalisierung mit Fokus auf Gewaltkriminalität (Brooks & Fritzon, 2020, S. 108). Auch Lilienfeld und Andrews (1996) entwickelten mit dem Psychopathic Personality Inventory (PPI) eine häufig genutzte alternative Operationalisierung von Psychopathie, ebenfalls primär für die Untersuchung von Psychopathie als subklinisches Merkmal im Wirtschaftskontext oder der Allgemeinbevölkerung (Skeem, Polaschek, Patrick

& Lilienfeld, 2011, S. 102). Die überarbeitete Version (PPI-R) besteht aus den übergeordneten Faktoren der *furchtlosen Dominanz* und *egozentrischen Impulsivität* (Lilienfeld & Widows, 2005; dt. Version von Alpers & Eisenbarth, 2008). *Kalthertzigkeit* wird häufig als eigene Dimension oder dritter Faktor beschrieben (Alpers & Eisenbarth, 2008, S. 14; Benning, Patrick, Hicks, Blonigen & Krueger, 2003; Skeem et al., 2011, S. 102).

Die Autoren Patrick, Fowles & Krueger (2009) entwickelten ein ähnliches Konzept von Psychopathie, bestehend aus den Komponenten der *Meanness* (Gemeinheit), *Boldness* (Kühnheit) und *Disinhibition* (Enthemmung), sowie das dazugehörige Messinstrument der TriPM zur Erhebung von Psychopathie. Collison, Miller & Lynam (2021, S. 115) betonen die Ähnlichkeit der Faktoren der TriPM zu den Faktoren der PPI-R: *Kühnheit* ist ähnlich zu dem, was Lilienfeld und Widows (2005) als *furchtlose Dominanz* bezeichnen, die Enthemmung ist dicht an der *egozentrischen Impulsivität*, und der dritte Faktor der *Gemeinheit* ist der *Kalthertzigkeit* ähnlich. Die Instrumente der LSRP, PPI-R und das TriPM bieten eine alternative Operationalisierung von Psychopathie zur Untersuchung in non-forensischen Populationen, was zu einer wachsenden Zahl an Publikationen zu „Successful Psychopathy“ (z.B. Benning et al., 2019, S. 585) oder „Corporate Psychopathy“ (Babiak et al., 2010, S. 174) führte.

2.4.3 Primäre und sekundäre Psychopathie

Der kleinste gemeinsame Nenner fast aller Betrachtungsweisen ist eine Differenzierung zweier distinkter Faktoren: „Nearly all theoretical models and empirical studies of subtypes have posited a distinction between primary and secondary psychopathy“ (Hicks & Drislane, 2019, S. 299).

Lykken (1995, S. 156) und auch bereits Karpman (1941) unterschieden begrifflich die Subtypen der *primären Psychopathie* und der *sekundären Psychopathie*. Für diese beiden Facetten nutzt Patrick (2019) die Metapher der „two contrasting ‚faces‘ of psychopathy“ (S. 4). Diese beiden Seiten der Psychopathie unterscheiden sich nicht nur durch unterschiedliche Eigenschaften, sondern nach Hicks & Drislane (2019, S. 300) auch durch unterschiedliche

ätiologische Ursachen. Die primäre Psychopathie ist nach Lykken (1995, S. 225) überwiegend durch Furcht- und Empathielosigkeit gekennzeichnet. Auch in anderen Betrachtungsweisen wird mit unterschiedlichen Begriffen dieselbe dahinterliegende Wirklichkeit beschrieben: Hare (1991) nennt diese Seite ‚Faktor 1‘, Lilienfeld und Widows (2005) beschreiben sie als *furchtlose Dominanz*, Cleckley (1950/2015) spricht von dem Fehlen von Nervosität, und Patrick et al. (2009) nennen diesen Faktor *Kühnheit* (engl. *boldness*). Im Gegensatz dazu sind charakteristische Attribute für sekundäre Psychopathie nach Lykken (1995) die Impulsivität, Aggressivität und auch eine defizitäre Selbstkontrolle (S. 226). Der Kriminalpsychologe Hare (1991) nennt diese Seite der Psychopathie ‚Faktor 2‘, Lilienfeld und Widows (2005) beschreiben dies als *egozentrische Impulsivität*, Cleckley (1950/2015) spricht von fehlender Selbstkontrolle und Patrick et al. (2009) beschreiben diesen Faktor als *Enthemmung* (engl. *disinhibition*). Trotz einiger Unterschiede sind auch das verschiedene sprachliche Formulierungen einer ähnlichen dahinterliegenden Realität.

Hicks & Drislane (2019, S. 300) nutzen metaphorisch die Worte ‚kalt‘ und ‚heiß‘, um das unterschiedliche Temperament und Wesensmerkmal der Subtypen zu verdeutlichen: Während primäre Psychopathen kühle Strategen sind, sind sekundäre Psychopathen eher emotional überhitzt und agieren unüberlegt, impulsiv und aggressiv.

Eine Destinktion von (mindestens) zwei Faktoren ist ratsam, da das Psychopathiekonstrukt multidimensional ist, sodass je nachdem, welche Facetten wie stark ausgeprägt sind, völlig unterschiedliche Profile und ‚Karrieren‘ im Ergebnis entstehen können. Die Höhe eines PCL-R Scores an sich ist wenig aussagekräftig, da die Profile und Folgen sehr unterschiedlich ausfallen können, je nachdem, welche Merkmale wie stark ausgeprägt sind. So kann Psychopathie die gesellschaftliche Karriereleiter nach ganz oben führen, möglicherweise bis hin zur Präsidentschaft der USA (Lilienfeld, Waldman, Landfield, Watts, Rubenzer & Faschingbauer, 2012). Doch auch der umgekehrte Weg eines gesellschaftlichen Abstieges bis ins Gefängnis ist möglich (zu Psychopathie und Kriminalität siehe Porter et al., 2019). Benning et al. (2003, S. 346) weisen darauf hin, dass *furchtlose Dominanz* (PPI-R Faktor 1) vor allem mit Intelligenz, Bildung und sozialer Kompetenz verbunden ist, während die

egozentrische Impulsivität (PPI-R Faktor 2) eher mit antisozialem Verhalten, Alkohol- oder Drogenmissbrauch einhergeht. Dass die beiden PPI-R Faktoren in der Konsequenz mit sehr unterschiedlichen Verhaltensweisen korrelieren, stützt die Annahme, „dass Psychopathie aus zwei oder mehr distinkten Faktoren besteht“ (Schütte & Blickle, 2017, S. 92).

Zur sprachlichen Abgrenzung der unterschiedlichen 'Karrieren' haben sich die Begriffe „Criminal Psychopaths“ (Kiehl & Hoffmann, 2011, S. 355) einerseits und „Corporate Psychopathy“ (Babiak et al., 2010, S. 174) oder „Successful Psychopathy“ (z. B. Benning et al., 2019, S. 585) andererseits etabliert. Die Psychopathieprävalenz unter Führungskräften liegt bei ca. 3-6 % (Babiak et al., 2010, S. 184). Die deutlich höhere Prävalenz unter Führungskräften und CEOs, verglichen mit dem Referenzwert von 1 %, ist ein empirisch gut abgesicherter Befund (z.B. Babiak et al., 2010; Boddy, 2014; Jonason, Slomski & Partyka, 2012). Verglichen mit gewaltkriminellen Psychopathen zeigen die Psychopathen im Wirtschaftskontext jedoch ein völlig unterschiedliches Psychopathieprofil. Erfolgreiche Psychopathie ist eher durch hohe Ausprägungen bei primärer Psychopathie (Furchtlosigkeit) gekennzeichnet, aber gleichzeitig in sekundärer Psychopathie (Impulsivität) gemäßigt (Benning et al., 2019, S. 597). Kriminelle Psychopathie und insbesondere Gewaltkriminalität wird wiederum eher mit sekundärer Psychopathie assoziiert (Douglas et al., 2019, S. 697). Schon Dutton (2014) resümierte, dass es bei Psychopathiemerkmalen nicht um den Summenscore gehe, sondern um „Ausprägung und der Art ihrer Kombination“ (S. 39).

Wie wären Hacker in diesem Kontext einzuordnen, und welche Implikationen hat das für die Methodik? Sollten Black Hat Hacker tatsächlich höhere Psychopathie-Scores aufweisen, ergibt sich die Frage, ob sie eher der Gruppe der erfolgreichen oder der kriminellen Psychopathen zuzuordnen wären. Die Abgrenzung (kriminell *oder* erfolgreich) wird dem Bereich der Cyberkriminalität nicht gerecht. Nach dem, was man bisher über Täterprofile weiß, sind Black Hat Hacker überdurchschnittlich intelligent und stammen aus allen sozialen Schichten, im Schnitt eher aus der Mittelschicht (BKA, 2015b). Bedenkt man gleichzeitig die geringen Aufklärungsquoten, Milliardenprofite und die hohe Dunkelfeldquote (BKA, 2025a; Rüdiger, 2023, S. 14; Wernert, 2021, S. 30), kann man Black Hat Hacker durchaus auch als

erfolgreich klassifizieren. Cyberkriminelle sind nicht entweder kriminell *oder* intelligent/erfolgreich, sondern beides. Daher ergibt sich die Fragestellung, ob Black Hat Hacker eher dem Profil primärer Psychopathie entsprechen würden (ähnlich den Wirtschaftspsychopathen) oder eher dem Profil sekundärer Psychopathie (ähnlich den gewaltkriminellen Psychopathen).

Eine Differenzierung nach zwei Faktoren erscheint in Anbetracht der Unterschiede jedenfalls sinnvoll. Für die Fragebogenkonzeption bedeutet das konkret, dass Psychopathie mit einem Instrument erhoben werden sollte, welches eine Differenzierung zwischen Subskalen der primären & sekundären Psychopathie erlaubt.

2.4.4 Neurobiologische Aspekte der Psychopathie

Auch innerhalb der Neurobiologie wurde Psychopathie ausführlich untersucht. Bei der Ätiologie der Kriminalität - also der Ursachenforschung - spielt Furchtlosigkeit eine bedeutsame Rolle. Ist das Angestempfinden grundsätzlich defizitär, fehlt auch die Furcht vor Strafe und damit die abschreckende Wirkung. Doch die emotionale Empathie mit anderen Menschen und Furcht sind zentrale, hemmende Faktoren, die Kriminalität verhindern können, aber bei primärer Psychopathie fehlen. Die Unterschiede lassen sich auch neuronal nachweisen und zeigen sich z.B. in strukturellen Defiziten in der Amygdala und dem präfrontalen Kortex (Yang & Raine, 2019). Heute wird angenommen, dass die Ursachen für die Furchtlosigkeit primärer Psychopathen angeboren sind (z.B. Douglas et al., 2019, S. 696). Vergleichsstudien mit Patienten mit Hirnschäden haben geholfen diejenigen Hirnareale zu identifizieren, die bei der Erklärung psychopathischer Merkmale besonders relevant sein könnten. Nach Glenn & Raine (2014) zeigen z.B. Patienten, die einen Hirnschaden im Bereich des ventromedialen präfrontalen Kortex erlitten haben, in Folge dessen Persönlichkeitseigenschaften und Verhalten, „that most closely resemble psychopathic traits“ (S. 87). Auch Patienten mit Schäden im Bereich der Amygdala haben im Anschluss Schwierigkeiten, Emotionen in Gesichtern zu erkennen, ähnlich wie es bei Psychopathie der Fall ist (Glenn & Raine, 2014, S. 92-93). Neben anderen Hirnregionen spielt insbesondere

die Amygdala eine zentrale Rolle bei der Emotionsverarbeitung und vor allem bei Furcht- bzw. Angstreaktionen (LeDoux, 2007). Es bestehen Korrelationen zwischen Psychopathie und einer verminderten Größe der Amygdala und einer geringeren Aktivierung der Amygdala bei emotionalen Reizen, verglichen mit Kontrollgruppen (zur Übersicht: Yang & Raine, 2019, S. 383 ff.).

Birbaumer et al. (2005) führten Experimente zur Angstkonditionierung durch, in denen sie psychopathische Straftäter mit einer Kontrollgruppe verglichen. Sie konnten experimentell zeigen, dass Psychopathen im Gegensatz zur Kontrollgruppe keine signifikante Aktivierung der Amygdala und keine konditionierten Hautleitfähigkeitsreaktionen zeigten. Birbaumer et al. (2005) folgern daraus eine „dissociation of emotional and cognitive processing“ (S. 799). In Bezug auf die Angst vor Strafe bedeutet das, dass Täter zwar kognitiv verstehen, dass eine Strafe droht, dies aber nicht mit den ‚normalen‘ emotionalen Reaktionen, wie Furcht oder Hemmung, einhergeht. Auch Glenn & Raine (2014, S. 71) betonen die Bedeutung der Konditionierbarkeit von Angst für Moral, gewissenhaftes Verhalten und damit auch die Wahrscheinlichkeit von kriminellem Verhalten.

Die typische Interpretation ist das Fehlen von Angst, wobei Hosker-Field, Gauthier & Book (2016) mit der „Fear Enjoyment Hypothesis“ (S. 278) eine andere Interpretation vorschlagen (siehe auch: Hofmann, Mokros & Schneider, 2024). Vielleicht empfinden Psychopathen Angst, aber eben nicht als negative Emotion, sondern eher als ‚reizvollen Kick‘. Nach dem Ansehen eines Videos als Stimulus für Angst bewerteten Personen mit höheren Psychopathie-Scores das Empfinden positiver und beschrieben Angst mit positiveren Worten (Hosker-Field et al., 2016). Die Fear-Enjoyment-Hypothese konnte im Kern auch von Hofmann et al. (2023) bestätigt werden. Diese Interpretation passt zu der Beschreibung von Hackern durch Chiesa et al. (2009): „Hackers don’t mind running risks; they feel it’s part of the ‘game’. They feel excited, enjoying the adrenalin rush caused by fear of being discovered and love of the ‘forbidden’“ (S. 183).

Gerade in den qualitativen Interviews ist es daher lohnenswert genauer nachzufragen, ob Black Hats keine Angst vor Konsequenzen empfinden oder die latente Gefahr, erwischt

werden zu können, vielleicht sogar als positive Emotion empfunden wird (*Thrill Seeking* Motiv).

Noch aufschlussreicher wäre eine direkte Messung der Hirnaktivität oder der elektrodermalen Aktivität bei Hackern. Dies würde jedoch persönliche Treffen voraussetzen, die aufgrund der Tatsache, dass (nicht-inhaftierte) Black Hats in Hacker-Foren weltweit verteilt leben und um ihre Identität besorgt sind, wahrscheinlich außerhalb des Strafvollzugs nicht realisierbar wären.

2.5 Narzissmus

Subklinischer Narzissmus ist wahrscheinlich die mittlerweile bekannteste Komponente der Dunklen Triade. Lange Zeit wurden dunkle Persönlichkeitsfacetten im Alltag und Organisationskontext eher unterschätzt, wobei die wachsende Zahl der populärwissenschaftlichen Artikel und Beiträge zu vermeintlich narzisstischen Chefs und toxischen Beziehungen ein Indikator dafür sein könnte, dass das Pendel mittlerweile in die entgegengesetzte Richtung ausgeschlagen ist. Unliebsame Führungskräfte oder Ex-Beziehungspartner pauschal als narzisstisch zu klassifizieren, kann auch ein Weg sein, die eigene Verantwortung auszublenken und Schuld zu externalisieren. Ursprünglich stammt der Begriff ‚Narzissmus‘ aus einer Geschichte der griechischen Mythologie: Der junge Narziss ist durch einen Fluch derart von sich selbst eingenommen, dass er beim Versuch, die Spiegelung seines Gesichts in der Oberfläche eines Tümpels zu küssen, das Gleichgewicht verliert und dabei ertrinkt (siehe z.B. Externbrink & Keil, 2018, S. 8). Narziss ist also, im Sinne der mythologischen Symbolik, an Selbstliebe erstickt. Narzissmus soll im Rahmen der Arbeit jedoch deutlich von der *Narzisstischen Persönlichkeitsstörung* abgegrenzt werden, da Narzissmus als Bestandteil der Dunklen Triade ebenfalls als subklinische Eigenschaft gesehen wird (Furtner, 2017, S. 5). Mit Narzissmus wird also „nicht die geistige Krankheit einer Person bezeichnet, sondern eine [...] stetig verteilte, subklinische Variante, die alle Personen auszeichnet, nur eben mehr oder weniger stark“ (Schwarzinger, 2020, S. 39).

Mit dem Instrument des *NPI* wurde von Raskin & Hall (1979) ein Messinstrument geschaffen, um Narzissmus als subklinisches Persönlichkeitsmerkmal zu erheben. Es wurde später von Raskin & Terry (1988) zur NPI-40 weiterentwickelt und zum „Goldstandard“ der Narzissmus-Messung“ (Schwarzinger, 2020, S. 39). Die NPI-40 besteht aus 40 Aussagenpaaren, wobei ein Satz jeweils eine narzisstische Einstellung repräsentiert und ein Satz die nicht-narzisstische Variante darstellt. Je Frage soll eine der dichotomen Antwortoption ausgewählt werden. Wie oft jemand die narzisstische Antwortvariante gewählt hat, wird zu einem Summenscore (der somit von 0-40 reichen kann) aufaddiert. Anhand der Funktionsweise des Messinstrumentes wird deutlich, dass Narzissmus keine Schwarz-Weiß-Kategorisierung darstellt, sondern eine stetig verteilte Variable bzw. ein Kontinuum. Jedem Menschen ließe sich somit ein mehr oder weniger hoher Narzissmus-Score zuweisen. Die genaue Faktorstruktur des Instruments wird uneinheitlich gesehen und ist Bestandteil aktueller Diskussionen.

Die Wesensmerkmale des Narzissmus werden jedoch durch die Beschreibungen der Subskalen deutlich. Collani (2014, S. 2) benennt in der deutschsprachigen, angepassten Version des NPI-40 die sechs Subskalen:

Tabelle 1: Subskalen des NPI-40 nach Collani (2014, S. 2)

(1) AUT	Autoritätsanspruch
(2) ÜBERH	Überheblichkeit, Selbstfälligkeit
(3) EINZIG	Überlegenheitsgefühl, Einzigartigkeit
(4) ANGEB	Angeberei
(5) MANIP	Manipulationsneigung, Ausbeutung
(6) ANSPR	Anspruchsdenken

Typische narzisstische Merkmale sind nach Raskin & Terry (1988) u.a. ein starkes Bedürfnis nach Anerkennung durch andere Menschen, das Gefühl, anderen überlegen zu sein, ausgeprägte persönliche Eitelkeit, Ausbeutung, eine hohe Anspruchshaltung und Selbstgefälligkeit. Je nachdem, welche Facetten wie stark ausgeprägt sind, wird häufig zwischen *grandiosem Narzissmus* vs. *vulnerablen Narzissmus* unterschieden (z.B. Miller,

Gentile, Wilson & Campbell, 2013). Während sich der *grandiose Narzissmus* durch dominantes Auftreten und die Suche nach Aufmerksamkeit auszeichnet, manifestiert sich der *vulnerable Narzissmus* eher in negativen Gefühlen, wie Unsicherheit und Unzulänglichkeit (Miller et al., 2013). Furtner (2017) beschreibt dies als „helle und dunkle Seite des Narzissmus“ (S. 7).

Im Rahmen der Untersuchungen und in Bezug auf Hacker ist relevant, dass Narzissmus nicht per se antisozial sein muss, sondern auch eine adaptive ‚helle Seite‘ hat. Narzisstische Merkmale kommen z.B. bei Führungskräften häufig vor (Brunell, Gentry, Campbell, Hoffman, Kuhnert & Demarree, 2008). Da Narzissten oft ehrgeizig und überzeugend sein können (Furtner, 2017, S. 17, Tab. 3.1) und häufig eine bessere emotionale Intelligenz besitzen (Petrides, Vernon, Schermer & Veselka, 2011, S. 39), gilt Narzissmus als die „vergleichsweise sozialste Dimension der Dunklen Triade“ (Furtner, 2017, S. 6).

Narzisstische Persönlichkeitszüge könnten daher in Bezug auf Black Hat Hacker, aber auch White Hat Hacker relevant sein. Ego und Anerkennung gehören zu möglichen Motiven krimineller Hacker (Kirwan & Power, 2013, S. 63), was ein Indikator narzisstischer Persönlichkeitszüge sein könnte. Gaia et al. (2021) weisen hingegen in ihrer Untersuchung darauf hin, „white hatters, the good guys, tend to be narcissists“ (S. 23), wobei die Ergebnisse dazu nicht signifikant waren. Während Machiavellismus (skrupellos) und Psychopathie (gefühlskalt) eindeutig eher bei Black Hats zu vermuten wären, gibt es Gründe, anzunehmen, dass Narzissmus vielleicht sogar auf der ‚guten Seite‘ des Hackings stärker vertreten ist. Black Hats können den Ruhm ihrer Taten meist nicht mit ihrer wahren Identität verknüpfen und auch nicht vor Bekannten mit Cyberangriffen prahlen. Anerkennung und Bewunderung bekommen sie, wenn überhaupt, in Hacker-Foren, maskiert hinter Pseudonymen und Anime-Figuren als Profilbildern. Besteht das Grundmotiv einer Person darin, Anerkennung für die eigene Leistung oder das eigene Talent ernten zu können, könnte tatsächlich eine Karriere als White Hat Hacker oder Sicherheitsforscher interessanter sein. Furtner (2017, S. 9) vergleicht Narzissten mit Darstellern im Theater, die die Öffentlichkeit, die Bühne, die

Aufmerksamkeit, die Anerkennung suchen, während Machiavellisten eher die mächtigen ‚Strippenzieher‘ hinter den Kulissen wären, die kaum Interesse an öffentlicher Bewunderung haben, sondern im Hintergrund bestrebt sind, Macht und Vermögen aufzubauen. Sind Black Hat Hacker also eher die ‚Puppenspieler‘ im Hintergrund (Machiavellismus und Psychopathie), während White Hats eher die Bewunderung und Anerkennung suchen (Narzissmus)? Wie der Name der ‚Dunklen‘ Triade impliziert, sind diese Eigenschaften im Wesentlichen antisozial und somit eher im Zusammenhang mit Cyberkriminalität zu vermuten. Aus den oben genannten Gründen ist es jedoch möglich, dass Narzissmus bei White Hat Hackern im gleichen Maße oder ggf. sogar stärker ausgeprägt sein könnte als bei Black Hat Hackern.

2.6 Machiavellismus

In seinem Werk *Der Fürst (Il principe)* beschrieb der italienische Philosoph Niccolò Machiavelli im Jahr 1532 seine politische Philosophie der damaligen Zeit (deutsche Übersetzung, 10. Auflage, siehe: Machiavelli, 2016). Die Lehre Machiavellis lässt sich im Kern durch die Redewendung „‘der Zweck heiligt die Mittel‘“ (Externbrink & Keil, 2018, S. 10) beschreiben (siehe auch: Henning, 1983, S. 170; Furtner, 2017, S. 8; Schwarzingen, 2020, S. 40).

Ursprünglich war also Machiavellismus keine Persönlichkeitseigenschaft, sondern ausschließlich eine politische Ideologie des frühen 16. Jahrhunderts. Christie & Geis (1970) übertrugen Aussagen und Überzeugungen von Machiavelli in ein psychometrisches Messinstrument und entwickelten die Skala *MACH IV*, welche die Zustimmung zu Aussagen von Machiavelli auf einer 6-stufigen Likert-Skala abfragt und somit Machiavellismus als Persönlichkeitseigenschaft erhebt (Deutsche Version: Henning & Six, 1997). Machiavellisten haben nach Christie & Geis (1970) ein zynisches Menschenbild und manipulieren andere zu ihrem eigenen Nutzen, ohne Rücksicht auf Moral. Während Psychopathie teils impulsiven Charakter hat, sind Machiavellisten „Langzeitstrategen“ (Bergk & Raschke, 2023, S. 86). Furtner (2017) bezeichnet sie daher als „Meister der taktischen Täuschung“ (S. 8).

Henning & Six (1977, 1997) haben basierend auf den Arbeiten von Christie & Geis (1970) eine deutsche, angepasste Version einer Machiavellismus-Skala vorgestellt, die häufig für die Messung von Machiavellismus als Persönlichkeitseigenschaft eingesetzt wird. Beispiel-Items zu Machiavellismus aus der deutschsprachigen Version des *MACH IV* von Henning & Six (1997) verdeutlichen einige typische Einstellungen machiavellistischer Persönlichkeiten:

Tabelle 2: Machiavellismus-Items aus Henning & Six (1997)

„Jeder ist sich selbst der Nächste.“
„Man soll seine Bekanntschaften unter dem Gesichtspunkt auswählen, ob sie einem nützen können.“
„Um eine gute Idee durchzusetzen, ist es unwichtig, welche Mittel man anwendet.“
„Man sollte nur dann den wahren Grund seiner Absichten zeigen, wenn es einem nützt.“
„Es ist nicht so wichtig, wie man gewinnt, sondern, dass man gewinnt.“
„Wer sich für die Zwecke anderer ausnützen lässt, ohne es zu merken, verdient kein Mitleid.“

Wie aus den Itemformulierungen deutlich wird, wird praktisch alles im persönlichen und beruflichen Kontext (Bekanntschaften, Handlungen, Aussagen) nach persönlichem Nutzen im Sinne der eigenen Zielerreichung bewertet.

Aktuelle Diskussionen um Machiavellismus drehen sich weniger um die Validität der Skala, sondern um deren Faktorstruktur (Paulhus & Jones, 2015, S. 565). Verglichen mit dem Konstrukt der Psychopathie, welches bis heute Auseinandersetzungen zur Faktorstruktur und Konzeptionalisierung entfacht, konkurrieren bei Machiavellismus kaum unterschiedliche Skalen und Konzeptionalisierungen miteinander. Es wird jedoch zum Teil hinterfragt, ob es überhaupt sinnvoll ist, Machiavellismus als separates Konstrukt zu betrachten, oder als sekundäre Folge oder sogar Teil von Psychopathie. Psychopathie und Machiavellismus haben in der Tat einige Gemeinsamkeiten und korrelieren daher deutlich miteinander ($r = .5$, $p < .001$) (Paulhus & Williams, 2002, S. 559). Kritiker des Machiavellismus als subklinisches Persönlichkeitsmerkmal betonen, dass Psychopathie bereits so breit operationalisiert ist, dass sie machiavellistische Facetten beinhaltet. Miller und Kollegen (2017) fanden z.B. starke

Ähnlichkeiten und zweifeln daher an der Sinnhaftigkeit der Unterscheidung zwischen Psychopathie und Machiavellismus: „Psychopathy and Machiavellianism: A Distinction Without a Difference?“ (S. 439). Paulhus (2014, S. 422, Table 1) zeigt jedoch bei der direkten Gegenüberstellung auf, dass die fehlende Impulsivität bei Machiavellismus ein zentrales Distinktionsmerkmal darstellt.

Psychopathie hat zwei Seiten: Die kühle, strategische, furchtlose Seite einerseits, welche Hare (1991) als *Faktor 1* beschreibt und andere Autoren als primäre Psychopathie (Lykken, 1995, S. 132), die damit dem Machiavellismus ähnelt. Zum Psychopathiekonstrukt gehört aber auch der *Faktor 2*, der eher für sekundäre Psychopathie steht (Lykken, 1995, S. 132) und impulsive Tendenzen beschreibt. Diese impulsive Facette fehlt bei Machiavellismus gänzlich.

Möglicherweise sind Black Hat Hacker der Ansicht, dass Opfer selbst schuld seien (zynisches Menschenbild), sie manipulieren sie geschickt durch weiche Techniken, wie *Social Engineering* (zur Definition siehe: Wernert, 2021, S. 26) und probieren möglicherweise so, opportunistisch ihren eigenen Nutzen zu maximieren. Wie auch bei Psychopathie, ist anzunehmen, dass Black Hat Hacker bei Machiavellismus höhere Scores aufweisen, verglichen mit White Hat Hackern.

2.7 Kurzskalen zur Erfassung der Dunklen Triade

Zwei wesentliche Gründe sprechen für die Notwendigkeit von Kurzskalen zur gemeinsamen Erfassung der Dunklen Triade. Der erste Grund ist forschungsökonomischer Natur, also dem zu hohen Zeitaufwand geschuldet, die drei Eigenschaften der Dunklen Triade separat zu erheben (Schwarzinger, 2020, S. 113). Allein das PPI-R (dt. Version: Alpers & Eisenbarth, 2008) besteht aus 154 Items und stellt eine sehr breite Abdeckung des Konstruktes dar (Jones & Paulhus, 2014, Schwarzinger, 2020, S. 113). Zusammen mit den Standardmessinstrumenten für Narzissmus (*NPI* mit 40 Items) und Machiavellismus (*Mach IV* mit 18 Items) würde dies zu über 200 Items zur Erfassung der Dunklen Triade führen. Das umfasst lediglich die Triadeeigenschaften und beinhaltet noch keine Einführung (Zweck der

Studie) oder allgemeine Fragen zu Alter, Geschlecht, Hacking, Motiven oder anderen Daten. Die Bearbeitungszeit für die PPI-R allein wird mit 20-45 Minuten angegeben (Alpers & Eisenbarth, 2008, S. 23). Im zu hohen Zeitaufwand der Einzelmessungen liegt der Hauptgrund für die Notwendigkeit von kombinierten Kurzskalen (Jones & Paulhus, 2014). Der zweite Grund, der für eine gemeinsame Erfassung der Triade spricht, ist die Redundanz, da die Triadeeigenschaften nicht überschneidungsfrei sind, sodass teilweise vom „Construct Creep“ (Schwarzinger, 2020, S. 70) gesprochen wird, also einem Verschwimmen der Grenzlinien der Konstrukte.

Die Neigung, andere Menschen zu manipulieren, ist z.B. in verschiedenen Formulierungen mehrfach Teil der *PPI-R*, der *MACH IV* und des *NPI-40*. Gerade Black Hat Hacker außerhalb des Strafvollzugs sind für akademische Forschung ohnehin schwierig zu finden und zu überzeugen. Würde man hier Probanden lange ‚Itembatterien‘ vorlegen, bei denen sie zum Teil 7-10-mal dieselbe Frage in unterschiedlicher Formulierung beantworten sollen, wäre das ineffizient und die Abbruchquote zu hoch. Insbesondere Psychopathie und Machiavellismus korrelieren stark; die Meta-Analyse von O’Boyle, Forsyth, Banks & McDaniel (2012, S. 569) berichtet eine Interkorrelation von $r = .59$ für Psychopathie und Machiavellismus. Einzeln operationalisiert sind die Konstrukte nicht überschneidungsfrei. Gerade das PPI-R mit den 154 Items operationalisiert Psychopathie so breit, dass „auch Bestandteile von Machiavellismus und Narzissmus integriert worden sind“ (Schwarzinger, 2020, S. 113). So ist beispielsweise „Machiavellistischer Egoismus“ (Alpers & Eisenbarth, 2008, S. 28) wörtlich eine der PPI-R-Subskalen. Aus diesen Gründen entstand die Notwendigkeit komprimierter Kurzskalen zur gemeinsamen Messung der Dunklen Triade (Jones & Paulhus, 2014).

Mit dem Instrument des *Dirty Dozen* (Dreckiges Dutzend) schlugen Jonason & Webster (2010) eine extrem kurze Operationalisierung der Dunklen Triade mit nur 12 Items (4 Items pro Konstrukt) vor. Die deutsche Übersetzung (und noch weiter gekürzte Version) trägt den Namen der *Niederträchtigen Neun* (Küfner, Dufner & Back, 2015).

In zahlreichen Untersuchungen wurde das *Dirty Dozen* für geringe Alpha-Reliabilitäten, mangelnde Validität, schlechte Vorhersagegüte, abweichende Faktorstrukturen und fehlende Aspekte kritisiert (z.B. Maples, Lamkin & Miller, 2014). Auf Basis der Ergebnisse kommen Jones & Paulhus (2014) zu dem Fazit “[u]nfortunately, it appears to be too short” (S. 28) und entwickeln in vier Studien ($N = 1.063$) eine umfassendere, aber dennoch kompakte Skala zur Messung der Dunklen Triade, die sogenannte *Short Dark Triad (SD3)*. Die ersten beiden Studien identifizierten durch Faktoranalysen 27 Items, welche die Dunkle Triade valide abbilden sollen. Die Studien 3 und 4 haben die Subskalen validiert, indem diese mit den Standardmessverfahren und Fremdbeurteilungen verglichen wurden. Die häufig in nicht-klinischen Kontexten verwendete *Short Dark Triad* besteht aus 27 Items (9 pro Konstrukt) und ist nach Jones & Paulhus (2014) “efficient, reliable, and valid measures of the Dark Triad of personalities” (S. 28). Furnham (2013) betont, dass die *Short-Dark Triad* eine bessere Vorhersagegüte zeigt als das (zu kurze) *Dirty Dozen*. Auch Maples et al. (2014) und Schwarzingen (2020, S. 115) plädieren im direkten Vergleich der Instrumente für die Nutzung der *Short Dark Triad* von Jones & Paulhus (2014), sofern aus forschungsökonomischen Gründen eine Kurzsкала zur Erfassung der Dunklen Triade benötigt wird. Die *SD3* wurde in zahlreiche Sprachen übersetzt und ist ein häufig genutztes Standard-Verfahren zur gemeinsamen Erfassung der Dunklen Triade.

3 Aktueller Forschungsstand

In diesem Kapitel soll der aktuelle Forschungsstand zur Dunklen Triade, Profilen und Motiven von Hackern zusammengefasst werden und in den Kontext cyberkriminologischer Theorien eingeordnet werden. Da zu der Dunklen Triade und Hacking kaum empirische Erkenntnisse vorliegen, wurden dem Hacking ähnliche Verhaltensweisen einbezogen, wie z.B. Cyber-Aggression oder *Trolling Behavior*.

3.1 Die Dunkle Triade und Kriminalität

3.1.1 Gewaltkriminalität, Wirtschaftskriminalität und antisoziales Verhalten

Ein zentraler Befund zur Triade ist die deutliche Verbundenheit mit sozial aversiven, antisozialen oder kriminellen Verhaltensweisen, weshalb die Triade als ‚dunkel‘ bezeichnet wird. Innerhalb der drei Triadebestandteile hat sich besonders Psychopathie empirisch als ein zuverlässiger Prädiktor für Gewaltkriminalität und Aggression erwiesen (Porter et al., 2019). Die Untersuchung von 317 kanadischen Straftätern ergab, dass psychopathische Straftäter ($PCL-R \geq 30$) im Vergleich zu nicht-psychopathischen Straftätern über Jahrzehnte andauernde Zeiträume hinweg mehr Delikte begingen und schneller rückfällig wurden (Porter, Birt & Boer, 2001). Psychopathische Straftäter zeigen zudem mehr Gewalt in der Ausführung ihrer Taten (Porter, Woodworth, Earle, Drugge & Boer, 2003), darunter einige der schwersten Formen der Gewaltkriminalität, wie Serienmorde (Hickey, Walters, Drislane, Palumbo & Patrick, 2019). Psychopathische Straftäter (operationalisiert durch die PCL-R und einen Cut-Off Score von >29) zeigten, verglichen mit nicht-psychopathischen Straftätern, eine bis zu 5-mal höhere Rückfallwahrscheinlichkeit innerhalb von 5 Jahren nach Freilassung (Serin & Amos, 1995, S. 232). DeLisi (2009) sieht Psychopathie daher als bedeutsamsten Faktor zur Erklärung von Kriminalität:

“Of all the theories emanating from the social, behavioral, and criminological sciences, psychopathy is superior to its competitors. Here I argue that psychopathy is the unified theory of delinquency and crime and the purest explanation of antisocial behavior.” (DeLisi, 2009, S. 256)

Es ist aufgrund der deutlichen Zusammenhänge darauf hinzuweisen, dass Psychopathie und Kriminalität nicht äquivalent sind, da „nicht alle Kriminellen Psychopathen sind und nicht alle Psychopathen Kriminelle“ (Hare, 2005, S. 76). Einerseits ist die Psychopathieprävalenz in Justizvollzugsanstalten ca. 7- und bis zu 25-mal höher als in der Bevölkerung (1 % Referenzwert) (z.B. Coid, Yang, Ullrich, Roberts & Hare, 2009; Coid, Yang, Ullrich, Roberts, Moran, et al., 2009; Hare, 2005, S. 76), das bedeutet jedoch im Umkehrschluss, dass mindestens 75 % und bis zu 93 % der Gefängnisinsassen keine Psychopathen sind (operationalisiert durch einen PCL-R-Score von über 30 Punkten).

Psychopathie wurde lange im primär klinischen oder forensischen Kontext betrachtet, wird inzwischen aber zunehmend auch in nicht-klinischen Populationen - z.B. unter Studenten oder im Wirtschaftskontext - untersucht. Studien zur Dunklen Triade thematisieren z.B. Zusammenhänge mit Stalking (z.B. Branković, Dinić & Jonason, 2023), der Neigung zu sexueller Belästigung (z.B. Lyons, Houghton, Brewer, O'Brien, 2022), Doping im Sport (z.B. Nicholls, Madigan, Backhouse & Levy, 2017) oder auch Drogenmissbrauch (z.B. Brajković, Jelinčić, Kopilaš, 2022). Die Dunkle Triade zeigt ergänzend signifikante Korrelationen mit antisozialem Verhalten, welches nicht unbedingt strafbewährt ist oder im Graubereich des Strafrechts liegt, wie Mobbing (z.B. Baughman, Dearing, Giammarco & Vernon, 2012), Lügen (z.B. Jonason, Lyons, Baughman & Vernon, 2014), Fremdgehen in Beziehungen (z.B. Brewer, Hunt, James & Abell, 2015), akademischem Fehlverhalten (z.B. Ternes, Babin, Woodworth & Stephens, 2019) oder destruktivem Führungsverhalten (z.B. Furtner, 2017).

Bei den Korrelationen der Triademerkmale mit antisozialem Verhalten zeigt sich jedoch häufig eine Rangfolge der Stärke der Zusammenhänge:

Eine Meta-Analyse von Duradoni, Gursesli, Martucci, Gonzalez Ayarza, Colombini & Guazzini (2023) bestätigt z.B. Zusammenhänge zwischen *Counterproductive Work Behavior* und allen Persönlichkeitsmerkmalen der Dunklen Triade, wobei Psychopathie die stärksten Korrelationen mit *CWB* zeigt, gefolgt von Machiavellismus und Narzissmus.

Die Dunkle Triade hat sich empirisch auch als valider Prädiktor für Wirtschaftskriminalität herausgestellt, und auch hier zeigte Psychopathie die stärksten Korrelationen ($r = .48$, $p < .01$) (Amos et al., 2024, S. 58).

Baughman et al. (2012) untersuchten Korrelationen zwischen Mobbingverhalten unter Erwachsenen und der Dunklen Triade (operationalisiert durch die SD3) und fanden ebenfalls die stärksten Zusammenhänge zu Psychopathie, wieder gefolgt von Machiavellismus und Narzissmus.

Dieses Muster bzw. diese ‚Rangfolge der Dunkelheit‘ der Konstrukte in Bezug auf antisoziales Verhalten (1. Psychopathie, 2. Machiavellismus und 3. Narzissmus), ist ein roter Faden, der in zahlreichen empirischen Ergebnissen erkennbar ist. Nach Schwarzingen (2020) „sind alle Triade-Bestandteile mit verschiedensten Formen expliziten Fehlverhaltens verbunden [...] bis zu leichten wie schweren Formen strafrechtlich relevanter Kriminalität; deutlich am stärksten jeweils Psychopathie“ (S. 57).

Bei Gesamtbetrachtung der Literatur zur Dunklen Triade zeigen sich also recht konsistente Korrelationen zwischen den Komponenten der Dunklen Triade und antisozialem Verhalten, wobei Psychopathie die stärksten und Narzissmus die schwächsten Zusammenhänge aufweist. Dieser Befund passt zu der Analyse von Furtner (2017): „Unter den Dark Triad-Persönlichkeitseigenschaften zählt Narzissmus zur hellsten und positivsten Dimension, während Psychopathie am wenigsten adaptiv und sozial akzeptiert ist“ (S. 6).

In Bezug auf Cyberkriminalität wäre demzufolge ebenfalls davon auszugehen, dass sich Black Hat Hacker vor allem in Psychopathie und Machiavellismus von White Hats und der Allgemeinbevölkerung unterscheiden.

3.1.2 Die Dunkle Triade und Cyberkriminalität

Da die Dunkle Triade (vor allem Psychopathie) empirisch mit nahezu allen Formen von kriminellem und antisozialem Verhalten in der analogen Welt in Verbindung gebracht wurde, liegt die Annahme nahe, dass Personen mit Triadeeigenschaften auch online mit größerer

Wahrscheinlichkeit zu kriminellem und antisozialem Verhalten tendieren. Im Bundeslagebild Cybercrime für das Jahr 2024 des Bundeskriminalamtes heißt es: „Im Bereich der Cyberkriminalität ist das Dunkelfeld weit überdurchschnittlich ausgeprägt“ (BKA, 2025a, S. i). Bedingt durch die geringen Aufklärungsquoten und die Tatsache, auf die Plank (2020, S. 28) hinweist, dass Tätergruppen primär aus dem Ausland agieren, sind nur wenige Hacker inhaftiert. Es liegen somit verhältnismäßig wenig empirische Ergebnisse zu Persönlichkeitsmerkmalen von Hackern vor (Gaia et al., 2022, S. 2227; Selzer & Oelrich, 2021, S. 175).

Am relevantesten, im Sinne der Forschungsfrage und des geplanten Forschungsdesigns, ist die Untersuchung von Gaia et al. (2021), die explizit die Dimensionen der Dunklen Triade, *Thrill Seeking*, Entdeckungswahrscheinlichkeit und das Ablehnen von Autoritäten bei Black Hat-, White Hat- und Gray Hat Hackern untersucht hat.

Als signifikante Prädiktoren für Cyberkriminalität (Black Hat Hacking) konnten die Autoren Machiavellismus ($\beta = .35, p < .001$), Psychopathie ($\beta = .23, p < .001$) und auch das *Thrill Seeking* ($\beta = .14, p < .001$) identifizieren, wobei das Gesamtmodell 37,2 % der Varianz bei Black Hat Hackings erklären konnte (Gaia et al. 2021, S. 34). Überraschenderweise waren auch bei White Hat Hacking Psychopathie ($\beta = .29$) und Machiavellismus ($\beta = .30$) signifikant mit $p < 0.000$ (S. 32). Bei Gray Hat Hacking spielten ebenfalls Machiavellismus ($\beta = .214, p < .000$) und Psychopathie ($\beta = .20, p < .001$) eine Rolle und das Ablehnen von Autoritäten ($\beta = .20, p < .000$) (S. 33).

Eine methodische Kritik an dieser Untersuchung und auch zahlreichen anderen empirischen Studien zu Hackern ist die Art der Operationalisierung bzw. Stichprobenziehung. Bei einer so hohen Fallzahl von $N = 439$, schließt sich die Frage an, wie es den Autoren gelungen ist, 439 Hacker zu finden, inklusive krimineller Black Hat Hacker. Das Sample besteht in Wahrheit aus 246 Management-Studenten und 193 Studenten der Computerwissenschaft, die einen Fragebogen zu selbstberichteter Computerdelinquenz ausgefüllt haben. Natürlich mögen hier vereinzelte Personen dabei sein, die tatsächlich bereits *Cyberkriminalität im engeren Sinne*

begangen haben, die über das illegale Streamen von Kinofilmen hinausgeht. Es ist aber fraglich, ob aus einer Befragung eines studentischen Samples die Aussage abgeleitet werden kann, dass Black Hat Hacking mit Psychopathie korreliert. Aus forschungsökonomischen Gründen ist es verständlich, auf ein Sample von Studentinnen und Studenten zurückzugreifen, doch um die Kritik zugespitzt zusammenzufassen, gibt es eine Reihe von Studien zu ‚Hackern‘, die jedoch keine Hacker beinhalten. Grundsätzlich deuten die Ergebnisse von Gaia et al. (2021) aber in die Richtung, dass Psychopathie und Machiavellismus bei Black Hat Hacking eine Rolle spielen, überraschenderweise aber auch bei White Hat Hacking. Auch Amo et al. (2023, S. 105) finden fast identische Effektgrößen zu Psychopathie und Machiavellismus in Bezug auf das Motiv zum Black Hat- und aber überraschenderweise auch White Hat Hacking (siehe auch: Gaia et al., 2022). Auch Selzer und Oelrich (2021) finden Korrelationen, die zeigen, dass höhere Psychopathie- und Machiavellismus-Scores mit krimineller Intention einhergehen, wobei auch hier das Sample Studenten der Computerwissenschaft und/oder Teilnehmer an Informatikkursen waren.

Dass Psychopathie mit Cyberkriminalität in Verbindung steht, gilt bereits als recht gut abgesicherte Erkenntnis (z.B. March, 2022; Perenc, 2022), während über die Rolle von Narzissmus oder Machiavellismus bisher weniger bekannt ist.

Es liegen jedoch eine Reihe von Studienergebnissen zu anderen, ähnlichen antisozialen Verhaltensweisen im Cyberraum sowie *Cyber Aggression* vor, die darauf hindeuten, dass antisoziale Verhaltensweisen im Cyberspace ebenfalls zum Teil auf dunkle Persönlichkeitsdispositionen zurückzuführen sein könnten. Branković et al. (2023) konnten zeigen, dass sowohl Korrelationen zwischen Eigenschaften der Dunklen Tetrad und traditionellem Stalking, aber auch Cyberstalking bestehen. Tennakoon (2021, S.1) resümiert: „Antisocial behaviours have escalated to the cyberspace“. Grigg (2010) definiert *Cyber Aggression* als „intentional harm delivered by the use of electronic means“ (S. 152). Beispiele hierfür sind Online-Verhaltensweisen wie Cybermobbing, Belästigung von Personen in digitaler Form oder Hasskommentare. Pabian, Backer & Vandebosch (2015) untersuchten

Zusammenhänge zwischen Triadeigenschaften, operationalisiert durch die *Short Dark Triad* (Jones & Paulhus, 2014) und *Cyber Aggression*. Kontrolliert nach Alter und Geschlecht zeigte lediglich Psychopathie Korrelationen mit cyber-aggression ($r = .60$), wobei keine Zusammenhänge zwischen cyber-aggression sowie Narzissmus und Machiavellismus festgestellt werden konnten. Die Ergebnisse deuten darauf hin, dass sich der „psychopathy-aggression link“ (Porter et al., 2019, S. 612), also die starke Korrelation zwischen psychopathischen Persönlichkeitsmerkmalen und aggressivem und antisozialem Verhalten, auch auf den Cyberraum übertragen lässt.

Ein weiteres Online-Verhalten, das dem Hacking ähnlich ist, ist das sogenannte *Trolling Behavior*. *Trolling* (seltener *Black Hat Trolling*) wird uneinheitlich definiert, beschreibt jedoch allgemein das bewusste Stören von Online-Communities oder die Freude daran, andere (online) zu provozieren oder zu ärgern (z.B. Matthews & Goerzen, 2019, S. 523-524). Zwischen der Hacking-Subkultur und Trolling gibt es klare Parallelen. Viele Internet-Memes, Trolling-Verhalten und Slangausdrücke haben ihren Ursprung auf den Plattformen Reddit oder 4chan. Auch das wahrscheinlich bekannteste Hacker-Kollektiv Anonymous ist aus 4chan heraus entstanden, da sich hier Gleichgesinnte gefunden haben (Stryker, 2011). Die Übergänge zwischen Hacking, Trolling und Hacktivismus sind demnach fließend. Viele ‚Online-Trolle‘ und Hacker kommen nicht nur aus derselben Subkultur, nutzen dieselben Memes und denselben Slang, sondern es handelt sich möglicherweise auch um dieselben Personen.

Trolling ist also nicht direkt mit dem Hacking gleichzusetzen; die Subkulturen überschneiden sich jedoch und es bestehen Ähnlichkeiten zwischen den motivationalen Faktoren und Profilen der handelnden Akteure. Buckels, Trapnell & Paulhus (2014) untersuchten Zusammenhänge zwischen der Dunklen Tetrad (Charaktersadismus eingeschlossen) und *Trolling Enjoyment*, also der Frage, inwiefern Nutzer Freude dabei empfinden, andere digital zu ärgern und so Reaktionen zu provozieren ($N = 1.215$). Charaktersadismus zeigte die stärksten Korrelationen mit *Trolling* ($r = .52, p < .001$), gefolgt von Psychopathie ($r = .38, p <$

.001) und Machiavellismus ($r = .37, p < .001$), wobei kein signifikanter Zusammenhang mit Narzissmus identifiziert wurde (Buckels et al., 2014, S. 100, Table 1). Auch Gylfason, Sveinsdottir, Vésteinsdóttir & Sigurvinsdottir (2021) konnten die Zusammenhänge replizieren und identifizierten ebenfalls Psychopathie, Sadismus und Machiavellismus als relevante Persönlichkeitsdispositionen im Zusammenhang mit der Neigung zu *Trolling-Verhalten* innerhalb des sozialen Netzwerks *Facebook*. Die Ergebnisse zu Trolling in Verbindung mit Psychopathie und Sadismus konnten auch Volkmer, Gaube, Raue & Lerner (2023) an einem Sample von $N = 1.026$ deutschsprachigen Internetnutzern bestätigen. Sie fanden allerdings keine signifikanten Zusammenhänge zwischen *Trolling Motivation* und Machiavellismus.

Zusammenfassend deuten die bisherigen Ergebnisse darauf hin, dass zwei grundlegende Muster, die sich in der analogen Welt zeigen, sich auch auf den Cyberraum übertragen lassen:

(1) In der analogen Welt zeigen sich Zusammenhänge zwischen der Dunklen Triade und Kriminalität, aber auch nahezu allen anderen antisozialen Verhaltensweisen, von Doping bis Fremdgehen (Übersicht: Schwarzingen, 2020, S. 55-57). Auch im Cyberspace hat die Dunkle Triade Vorhersagekraft in Bezug auf Cyberkriminalität, aber auch anderes antisoziales Verhalten, wie Hasskommentare, Cybermobbing oder feindseliges Trolling.

(2) In der analogen Welt haben die Konstrukte nicht dieselbe prädiktive Kraft, sondern in zahlreichen Untersuchungen zeichnet sich eine ‚Rangfolge der Dunkelheit‘ ab, wobei Psychopathie die dunkelste Eigenschaft darstellt, Machiavellismus in der Mitte liegt und Narzissmus die hellste Eigenschaft der Dunklen Triade ist (Furtner, 2017, S. 6). Einige Befunde deuten in die Richtung, dass Psychopathie und Machiavellismus bei Black Hat Hackern eine Rolle spielen könnten, überraschenderweise aber auch bei White Hat Hackern (z.B. Gaia et al. 2021).

3.2 Cyberprofiling und die Dunkle Triade

Die Profile und Motive von Hackern besser zu verstehen und einzugrenzen, ist vor allem für „selektive Prävention“ (Bürger & Kaess, 2024, S. 405) relevant. Je besser das Verständnis der potentiellen Risikoprofile und Radikalisierungsprozesse ist, desto besser lassen sich Personengruppen gezielt ansprechen, um präventiv zu intervenieren. Aber kann das Wissen über Profile und Persönlichkeiten auch zur Profilerstellung dienen, also als Hilfsmittel der Verbrechensaufklärung?

Das Profiling ist eine ermittlungsunterstützende Methode, bei der mittels Analyse von Verhalten (*Operativer Fallanalyse*) u.a. Wahrscheinlichkeitsaussagen über einen oder eine Täterin abgeleitet werden. Metaphorisch ausgedrückt, geht es beim Verhaltens-Profiling nicht darum, Fingerabdrücke zu finden, sondern 'Abdrücke' der Persönlichkeit. Nach Musolff (2002) besteht der Ansatz der Operativen Fallanalyse bzw. des Profilings darin, aus Verhaltensspuren am Tatort Rückschlüsse auf die Persönlichkeitsmerkmale von Tätern zu ziehen (S. 3-4). Es ist selbstverständlich, dass die Voraussetzung für diesen Rückschluss ist, dass die Persönlichkeit eines Täters tatsächlich das Verhalten am Tatort beeinflusst: „Profiling in effect is based on the assumption that the perpetrator’s decisions and behavior at the crime scene reflect personality traits [...]“ (Chiesa et al. 2009, S. 9). Wenn es keinerlei Korrelationen zwischen Persönlichkeit und Verhalten gäbe, wäre der ganze Ansatz des Täterprofilings obsolet. Doch in zahlreichen Deliktsfeldern gibt es empirisch belegte Zusammenhänge zwischen Tatverhalten und Persönlichkeit. Hazelwood & Warren (2003, S. 587) unterscheiden bei Serien-Sexualstraftaten z.B. die drei Verhaltensarten *Modus Operandi* (das Vorgehen bei der Tat), *Ritual* (Aspekte sexueller Fantasien, die im Sinne des Modus Operandi nicht nötig wären) und *Signature* (eine Kombination aus bestimmten Aspekten von *Modus Operandi* (MO) und Ritual, die individuell für einen Täter sind). Bei Delikten, wie z.B. Sexualstraftaten, Serienmord oder auch Fällen von Erpressung oder Brandstiftung werden Profilingansätze bereits seit Jahrzehnten erfolgreich eingesetzt (siehe z.B. Musolff, 2002, S.1). Mord oder Sexualstraftaten sind jedoch emotionale, hochpersönliche Delikte, bei denen sexuelle Paraphilien oder jahrelange persönliche Kränkungen sich in Form

von Verbrechen physisch manifestieren. Je persönlicher das Delikt, desto mehr Persönlichkeitsspuren werden potentiell am Tatort sichtbar. Doch schon bei weniger affektiv aufgeladenen Delikten, wie z.B. Fahrrad- oder Ladendiebstahl, stößt das Konzept an seine Grenzen, da hier kaum Persönlichkeitsaspekte am Tatort sichtbar werden und es auch keine Leiche gibt, die obduziert werden könnte. Bei *Cybercrime im engeren Sinne* kommt noch die Besonderheit hinzu, dass es keinen Tatort im physischen Sinne gibt, weshalb lange Zeit fraglich war, inwiefern Profilingmethoden bei Hackern anwendbar sind (Chiesa et al., 2009, S. 10).

Letztlich geht die Anwendbarkeitsfrage von Profilingmethoden auf die Grundfrage zurück, ob es beim Hacking signifikante Korrelationen zwischen Persönlichkeitsmerkmalen (z.B. der Dunklen Triade) und dem *Modus Operandi* der Tat gibt, und auch hierzu gibt es erste empirische Erkenntnisse.

Jones, Padilla, Curtis, Kiekintveld (2021) gaben Probanden ein hypothetisches Spielszenario, in dem sie einen Cyberangriff ausführen, um die Dunkle Triade in Zusammenhang mit bevorzugten Angriffsarten zu untersuchen. Während Machiavellisten eher heimliche und langfristige Strategien der Täuschung bevorzugten (Social Engineering), waren Narzissmus und Psychopathie eher typisch für einen schnellen, brachialen *Brute Force Angriff*, - die Ergebnisse wurden in einer zweiten Studie (Laborexperiment) bestätigt.

Wenn Persönlichkeitseigenschaften der Dunklen Triade tatsächlich einen Einfluss auf bevorzugte Angriffsmethoden haben, bedeutet das im Umkehrschluss, dass aus der Angriffsart Wahrscheinlichkeitsaussagen über Hackerpersönlichkeiten möglich sind. Auch Hacker hinterlassen also durch ihren Modus Operandi möglicherweise einen ‚Abdruck ihrer Persönlichkeit‘ am digitalen Tatort, was die Grundvoraussetzung wäre, um Profiling-Techniken im Cyberspace anwenden zu können.

Diese Erkenntnisse und theoretischen Überlegungen haben eine direkte Implikation für die geplante Befragung von Hackern. Die Online-Befragung von Hackern (Studie 2) soll vor allem die Dunkle Triade messen. Es wäre ebenfalls ein nützlicher Erkenntnisgewinn, zumindest mit

einem Item die bevorzugte Angriffsart von Black Hat Hackern im Sinne von Jones et al. (2021) zu erfassen. Somit ließe sich in der statistischen Analyse prüfen, ob signifikante Korrelationen zwischen Triademerkmale und bevorzugter Angriffsart bestehen. Das wiederum wäre die Grundvoraussetzung und ein Indiz dafür, dass Cyberprofiling grundsätzlich möglich ist. Auch Korrelationen zwischen Motiven und Triademerkmale können aufschlussreich sein.

3.3 Forschungsergebnisse zu Persönlichkeitsmerkmalen von Hackern

Nur wenige Täter im Bereich der *Cyberkriminalität im engeren Sinne* sind inhaftiert oder überhaupt je mit dem Strafvollzugssystem in Berührung gekommen. Black Hat Hacker entziehen sich daher auch weitestgehend dem Zugang empirischer Forschung. Die meisten Erkenntnisse zu Mördern und anderen Straftätern wurden an und mit Gefängnisinsassen erhoben. Da dieser Forschungszugang in diesem Deliktsbereich nicht möglich ist, sind die Erkenntnisse bis heute begrenzt. „Despite decades of research, our understanding of cybercriminals remains limited“ (Martineau et al., 2023, S. 452). Die Aufklärungsquote für Cyberkriminalität von 31,9 % für das Berichtsjahr 2024 in der polizeilichen Kriminalstatistik (BKA, 2025a, S. 7) kann hierbei einen falschen Eindruck vermitteln, wie viele Hacker tatsächlich inhaftiert sind. Bei der Aufklärungsquote von rund einem Drittel gilt es im Kontext zu beachten, dass:

- (1) Die PKS nur das Hellfeld abbildet, wobei bis zu 91,5 % der Taten im Dunkelfeld liegen (BKA, 2023, S. 4).
- (2) Die PKS betrachtete bis einschließlich 2024 nur Inlandstaten, das heißt Taten, bei denen Opfer *und* Täter bekanntermaßen im Inland agieren, was bei Cybercrime selten der Fall ist: „In der Inlands-PKS werden Fälle, bei denen zwar Schäden in Deutschland verursacht werden, aber der Aufenthaltsort des Täters im Ausland liegt oder unbekannt ist (sogenannte Auslandstaten), nicht berücksichtigt“ (BKA, 2023, S. 6).
- (3) Der polizeiliche Begriff der ‚Aufklärungsquote‘ bedeutet lediglich, dass Tatverdächtige identifiziert wurden, sie sagt jedoch nichts darüber aus, ob ein Täter festgenommen oder verurteilt werden konnte (Statistisches Bundesamt, 2025b).

Die beiden bisher umfangreichsten und viel rezipierten Publikationen zu Hackern und deren Persönlichkeitsprofilen stammen aus den Jahren 2009 bzw. 2015. Das *Hacker Profiling Project* von Chiesa et al. (2009) war ein mehrjähriges Forschungsprojekt mit dem Ziel, die Persönlichkeit, motivationalen Faktoren und bibliografischen Hintergründe von Hackern ausführlich zu beschreiben. Die Autoren befragten 216 Hacker aus 37 Ländern schriftlich. Im Jahr 2015 publizierte auch das BKA eine ausführliche Literaturanalyse zu Tätern im Bereich Cybercrime, die zu einem großen Teil die Ergebnisse von Chiesa et al. (2009) wiedergibt, aber auch andere Studien kritisch würdigt. Während Hacker medial und auf der Kinoleinwand häufig als sozial isolierte ‚Nerds‘ in schwarzen Kapuzenpullovern dargestellt werden, ist das empirische Fazit zu Hackerprofilen, „dass es *den* Hacker nicht gibt“ (BKA, 2015b, S. 8). Die Akteursgruppen reichen von Hackern, die hauptberuflich im staatlichen Auftrag für Nachrichtendienste oder Militär hacken, über Berufsverbrecher, Anfänger, Hacktivist*innen bis zu ethischen Hackern (Kirwan & Power, 2013, S. 56-57). Die Spannweite der Akteure ist so groß, dass fraglich ist, inwiefern es überhaupt sinnvoll oder möglich ist, allgemeine Merkmale von Hackern herauszuarbeiten. Ziel dieser Übersicht ist die Nennung einiger Merkmale, die viele Hacker gemeinsam haben und die somit eine Art ‚kleinsten gemeinsamen Nenner‘ bilden.

Soziodemografische Merkmale

Die Untersuchung von Chiesa et al. (2009, S. 74) enthielt 6 % Frauen und 94 % Männer ($N = 567$), was darauf hindeutet, dass Hacking ein deutlich männlich dominiertes Feld ist, auch wenn Chiesa et al. (2009) bereits vor über 15 Jahren auf mögliche Trendveränderungen und steigende Frauenquoten hinweisen. Auch Vick & Roters (2003, S. 10) untersuchten Accountmissbrauchstäter und bei ihrem Sample von $N = 599$ waren ebenfalls nur 35 weiblich (6 %). Auch die Literaturanalyse des BKAs (2015b, S. 10) berichtet 76-94 % Männeranteil über verschiedene Studien hinweg.

Auch das junge Alter von Hackern ist auffällig: Chiesa et al. (2009, S. 74) berichten, dass 31 % zwischen 10-20 Jahre alt sind, 30 % in der Altersspanne 21 bis 25 Jahre und weitere 19

% unter 30 Jahre alt. Lediglich 3 % waren über 45 Jahre alt, während 80 % der Hacker unter 30 Jahre alt waren. Das Durchschnittsalter lag für männliche Hacker bei 25. Rheinberg und Tramp (2006) untersuchten intensive Computernutzer ($N = 271$), wovon über 40 % Hacker waren. Rund 87 % waren männlich, ihr Durchschnittsalter $M = 24.75$ ($SD = 5.01$). Trotz des jungen Alters lag der Modalwert der Computererfahrung bei 10 Jahren. Die Ergebnisse decken sich mit den Studienergebnissen von Chiesa et al. (2009, S. 74), dass 61 % der Hacker bereits im Alter zwischen 10-15 Jahren das Hacking erlernen, wobei sie meist Autodidakten sind. Da viele Hacker der ersten Generation immer noch aktiv dabei sind, könnte das Durchschnittsalter steigen, jedoch ist insgesamt „von einer in hohem Maße jungen Hackerpopulation auszugehen“ (BKA, 2015b, S. 8), also „most hackers belong to the *average teenager age group*“ (Chiesa et al., 2009, S. 91, Hervorhebung im Original).

Unter Hackern sind Personen aus allen Teilen der Welt vertreten (Chiesa et al., 2009, S. 91), ebenfalls alle sozialen Schichten und Bildungsniveaus. Die meisten gehören der oberen oder unteren Mittelschicht an (S. 95), sind oft gut gebildet oder befinden sich noch in der Ausbildung, wobei insbesondere die naturwissenschaftlichen und computerbezogenen Fächer von Interesse sind (S. 98). Hacking wird jedoch meist autodidaktisch erlernt und ist nicht abhängig vom akademischen Werdegang (BKA, 2015b, S. 28). Obwohl Cybercrime ein ortsunabhängiges Delikt ist und eine geografische Nähe zu großen Städten nicht nötig wäre, ist Hacking nach Chiesa et al. (2009, S. 91) dennoch eher eine urbane Erscheinung: Die meisten Hacker der Untersuchung ($N = 551$) kamen aus großen Städten (45 %) oder aus kleinen Städten (34 %), lediglich 21 % aus sehr kleinen Städten und Dörfern.

Persönlichkeitsmerkmale, Beziehungen und Motive

Chiesa et al. (2009, S. 93) befragten Hacker auch in Bezug auf persönliche Beziehungen und die Primärfamilie und weisen darauf hin, dass zahlreiche Hacker ein schwieriges Verhältnis zu Eltern haben und teilweise aus eher schwierigen Familienverhältnissen stammen, in denen Vernachlässigung, Streit, Scheidung oder häufiges Umziehen eine Rolle spielen können. Die Autoren sehen hierin eine mögliche Ursache für die Orientierung hin zum

Cyberraum und der Untergrund-Subkultur: „Computers are viewed as an *escape route*“ (Chiesa et al., 2009, S. 94, Hervorhebung im Original). Hierbei geht es darum, Anschluss in der Online-Community zu finden und so ein Zugehörigkeitsgefühl zu entwickeln. Zudem beschrieben Chiesa et al. (2009) Hacker als „rebels and dreamers“ (S. 92), wobei die Beschreibung der Persönlichkeiten und Beziehungen zu Freunden komplex ist, da Hacker in der realen Welt teils andere Persönlichkeitseigenschaften zeigen als in ihrem „‘natural element’, Cyberspace“ (S. 92). Während einige in der analogen Welt schüchtern, introvertiert und in zwischenmenschlichen Beziehungen eher unsicher und wenig kontaktfreudig wirken, sind sie im Cyberspace offen, kontaktfreudig und auch selbstbewusst bis arrogant in Bezug auf ihre Fähigkeiten (S. 102). Chiesa et al. (2009) beschreiben dies am Fallbeispiel des Hackers mit dem Pseudonym *Phiber Optik*:

“He says he feels insecure and awkward in his daily life, especially with girls, but when he’s in his room hacking away on his computer, he feels like a different person, he becomes the most brilliant, ‘coolest’ guy of the whole underground world.” (S. 92).

Nach Chiesa et al. (2009) ist das Bild des introvertierten Einsiedlers jedoch keineswegs pauschalisierbar, im Gegenteil sind viele Hacker kontaktfreudig, charmant und auch sportlich und gutaussehend (S. 91) und können in der realen Welt sehr überzeugend auftreten (S. 102). Die Motive sind von Haktivisten über *Script Kiddies* (also neugierige Anfänger) bis hin zu Cyberterroristen sehr breit gefächert und beinhalten nach Chiesa et al. (2009, S. 145-146) u.a. *Neugierde, Technologiefaszination, Unterhaltung/Spaß, die eigenen Fähigkeiten unter Beweis stellen, Langeweile, Problemlösung* (Hacking als Rätsel/ Herausforderung), *Rebellion, Ablehnen von Autoritäten, Geld, Adrenalin/ Thrill, Frustration* oder *Zugehörigkeitsgefühl*.

Abgeleitet aus der internationalen Literatur, bildet das BKA (2015b) neun übergeordnete motivationale Kategorien für das Hacking: *Spaß am Hacken / Neugier, Nervenkitzel, Zugehörigkeit* (S. 18), *Ruhm/Status, Macht/Kontrolle, finanzielle Motive* (S. 19), *Politische Gründe, Rache und Sucht* (S. 20). Ein Motiv ist innerhalb der Subkultur wie ein kleinster gemeinsamer Nenner, da es sowohl bei Black Hats, Gray Hats und White Hats zutrifft: Das

Ablehnen von Autoritäten und Rebellion (z.B. Chiesa et al., 2009, S. 153-154), also eine Anti-Establishment-Einstellung, in Verbindung mit der libertären Haltung, dass Informationen grundsätzlich frei verfügbar sein sollten (S. 146; 115). Das Hacking wird sinnbildlich als ein Akt der Rebellion verstanden (Chiesa et al., 2009, S. 146; 120), der Reiz des Verbotenen ist Teil des Motivs, sowie das ‚Katz-und-Maus-Spiel‘ mit den Strafverfolgungsbehörden (S. 146), die häufig als inkompetent oder unterlegen gesehen und verspottet werden (S. 114). Es verwundert daher nicht, dass Internetseiten von Behörden, Banken, und generell Großkonzerne zu den favorisierten Angriffszielen von Hackern gehören (Chiesa et al., 2009, S. 166), da es in Einklang mit der grundsätzlichen Motivstruktur steht.

Das BKA (2015b) betont, dass bei Hackern von „Motivbündeln“ (S. 28) auszugehen ist, das heißt, es können mehrere Motive zeitgleich vorliegen. Beispielsweise schließen sich finanzielle Motive, Spaß, Thrill, Langeweile, das Ablehnen von Autoritäten und die Suche nach Anerkennung in der Hacker-Community nicht aus.

Die Erhebungsmethode und auch einzige Möglichkeit, die inneren Motive empirisch zu erheben, sind quantitative oder qualitative Befragungen, also Selbstauskünfte. Das BKA (2015b, S. 22) weist auf eine methodische Grundkritik bei der Motivforschung hin, inwiefern den handelnden Akteuren ihre wahren Motive bewusst sind oder sich teilweise oder vollständig mit Post-Rationalisierungen und Rechtfertigungsstrategien mischen. Wenn jemand beispielsweise hackt, um eine innere Leere durch Vernachlässigung in der Kindheit zu kompensieren, ist unklar, inwiefern jemand dies reflektieren und offen angeben würde und könnte.

Einige Motive von Hackern (zur Übersicht siehe: Kirwan & Power, 2013, S. 63) erinnern direkt an Eigenschaften der Dunklen Triade: *Thrill-Seeking* erinnert an das Stimulationsbedürfnis, das typisch für Psychopathie ist. Egozentrik, Status und die Suche nach Bewunderung sind typische narzisstische Motive und Rache oder skrupelloses Profitstreben erinnern an Machiavellismus.

3.4 Cyberkriminologische Theorien

Herkömmliche Theorien der Kriminologie sind nur bedingt geeignet, cyberkriminelles Verhalten in Gänze zu erklären (Huber, 2019, S. 72). Einige Theorien wurden auf den Cyberraum übertragen, um Teilaspekte zu erklären, wie z.B. Cohen & Felsons (1979) *Routine Activity Theory*, welche besagt, dass Kriminalität dann wahrscheinlich ist, wenn drei Komponenten zeitlich zusammen auftreten: Ein geeignetes Opfer, ein Täter mit entsprechender Motivation und das Fehlen von Abwehrmechanismen. *Warum* Täter cyberkriminell agieren, ist die Theorie jedoch nicht im Stande zu erklären. Rüdiger (2023) sieht daher die Notwendigkeit einer Subdisziplin der Cyberkriminologie, die er als „Lehre von digitalen Normenbrüchen“ (S. 10) definiert. Im Folgenden soll die Fragestellung der Arbeit in den Kontext kriminologischer Theorien eingeordnet werden und bisherige cyberkriminologische Erklärungsansätze vorgestellt werden, die mögliche Unterschiede zwischen Black Hats und White Hats zu erklären vermögen.

3.4.1 Einordnung in den Kontext kriminologischer Theorien

Warum werden Black Hat Hacker kriminell, während White Hats einen legalen Karriereweg in der Cybersicherheit einschlagen? Der aktuelle Forschungsstand zur Dunklen Triade und Cyberkriminalität wurde dargestellt. Bisherige empirische Befunde legen nahe, dass Psychopathie und Machiavellismus auch eine bedeutsame, ursächliche Rolle bei der Erklärung der Motive zur Begehung von Cyberkriminalität spielen könnten. Dem Untersuchungsdesign, die Dunkle Triade bei Hackern zu messen, liegt also die Hypothese zugrunde, dass individuelle Persönlichkeitseigenschaften (*Traits*) der Grund für kriminelles Verhalten sein können.

Mentzel & Schröder (2005) unterteilen Kriminalitätstheorien in „Täterorientierte Theorien“ (S. 36) und „Gesellschaftsorientierte Theorien“ (Abbildung Gesellschaftsorientierte Theorien, S. 36). Die eine Gruppe von Theorien richtet den Blick auf das Individuum, die andere auf die Gesellschaft und Umstände. Auch Kirwan und Power (2013) grenzen die „individual theories“ (S. 17) von den „community theories“ (S. 17) ab. Die individuellen Theorien suchen nach

Ursachen für Kriminalität in der Person (z.B. genetische Faktoren oder Persönlichkeitseigenschaften), während Gesellschafts-, Community- und Sozialisationstheorien die Ursache eher ‚im Außen‘ suchen (z.B. Erziehung, Lerntheorien, Subkulturtheorien).

Die Dunkle Triade bei Hackern zu untersuchen, fällt gemäß dieser Klassifizierung also in die Logik und Tradition der Individualtheorien. Huber (2019) spricht von „Merkmalstheorien von Kriminalität“ (S. 69) bei denen Kriminalität z.B. anhand von Persönlichkeitsmerkmalen der Täter erklärt wird. Kirwan & Power (2013) betonen jedoch ausdrücklich, dass Kriminalität nicht monokausal ist: „criminality results from a variety of different causes, occurring at various levels (from societal levels, through community and social influence theories, to specific individual theories)“ (S. 16). Es kann verschiedene Ursachen *gleichzeitig* geben, die jeweils einen Einfluss haben. Gemäß der Verhaltensformel in der Feldtheorie von Kurt Lewin (1951) ist Verhalten eine Funktion von *Person (P) x Umwelt (U)*. Die Erklärung für Verhalten liegt also nicht allein in Persönlichkeitsdispositionen begründet, sondern häufig auch in Faktoren der Situation oder Umwelt, in der das Verhalten gezeigt wird. Auch wenn sich das Forschungsinteresse auf Triademerkmale und deren Facetten bei Hackern bezieht, soll dies nicht ausschließen, dass es parallel andere Umweltfaktoren geben kann, die einen Einfluss auf kriminelles Verhalten im Cyberspace haben (siehe Abbildung 6).

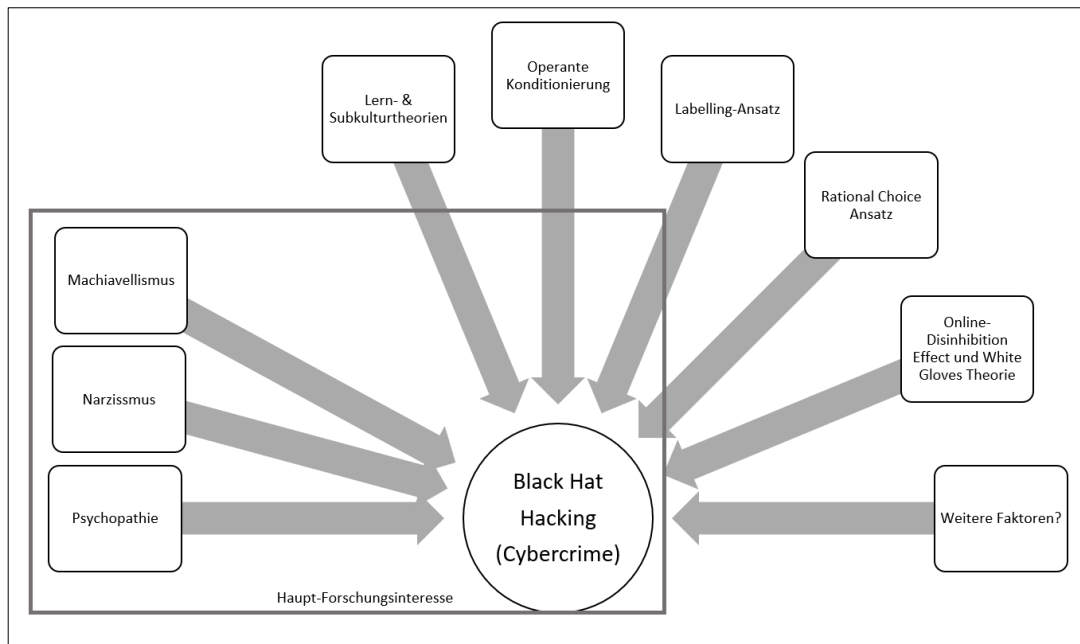


Abbildung 6. Mögliche Einflussfaktoren auf kriminelles Hacking

Quelle: Eigene Darstellung.

Die nachfolgenden Kapitel lenken den Blick weg von der Persönlichkeit hin zu Kontextmerkmalen und strukturellen Merkmalen des Cyberspace (also der Umwelt im Sinne Lewins, in der Hacking ausgeübt wird), um zu zeigen, inwiefern dies Einfluss auf Verhalten hat. Gewissermaßen stellt dies die Gegenhypothese dar: Sind tatsächlich ‚dunkle Persönlichkeitsmerkmale‘ nötig, um Cyberkriminalität zu begehen? Oder sorgt die Anonymität des Cyberspace für eine derartige Enthemmung, dass potentiell jede Person Hacker sein könnte? Stone (2001) analysierte Straftaten und Taten von 99 Serienmördern und bewertete diese anhand der Psychopathy Checklist-Revised (PCL-R, Hare, 1991). Nach Stones (2001) Einschätzung, erreichen 91 % der untersuchten Fälle einen PCL-R-Score von 30 oder höher und können somit als Psychopathen eingestuft werden (siehe auch Hickey et al., 2019, S. 575). In diesem extremsten Deliktsbereich verwundert es nicht, dass Menschen, die in der Lage sind, andere in Serie aus Mordlust zu töten, schlicht empathielos oder psychopathisch sein *müssen*. Es ist jedoch fraglich, ob Empathielosigkeit oder psychopathische Persönlichkeitsmerkmale überhaupt vonnöten sind, um andere Menschen oder Unternehmen zu hacken. Zwischen Tätern und Opfern besteht räumliche und oft auch

zeitliche Distanz bzw. „Asynchronity“ (Perenc, 2022, S. 253). In vielen Fällen kennen Hacker nicht einmal die Identität ihrer Opfer. Das Leid der Opfer sehen die Täter nicht, weswegen das Hacken möglicherweise nicht denselben Grad an Empathie- und Furchtlosigkeit erfordert, wie eine Person, ein Unternehmen oder eine Bank von Angesicht zu Angesicht auszurauben. In diesem Kapitel sollen spezifische Aspekte des Cyberraums und deren möglicher Einfluss auf kriminelles Verhalten beschrieben werden.

3.4.2 Der Online Disinhibition Effect

In diesem Zusammenhang ist insbesondere der *Online Disinhibition Effect* zu nennen, also ein Effekt der Enthemmung (engl. *disinhibition*) im digitalen Raum: Er beschreibt die Neigung, dass Menschen online Dinge tun oder sagen, die sie sich in persönlichen Interaktionen in der Form nicht trauen würden (Kirwan & Power, 2013, S. 151). Dies schließt positive und negative Interaktionen mit ein (Suler, 2004, S. 321). Auf Online-Datingportalen oder Apps, wie *Tinder* ist es sehr leicht, durch ‚swipen‘ nach rechts Menschen romantisches Interesse zu bekunden oder Komplimente zu machen. Jemanden in der Realität anzusprechen, ist dabei weit schwieriger und die Hemmung und Angst vor Zurückweisung größer. Der Cyberspace enthemmt aber auch in negativer Hinsicht, so werden z.B. Hasskommentare in den ‚sozialen‘ Medien im Schutz der Anonymität und räumlichen Distanz vermutlich leichter geäußert.

Suler (2004) unterscheidet daher sprachlich die gutartige Enthemmung und toxische Enthemmung („benign and toxic disinhibition“, S. 321). Er sieht Gründe für den Online Disinhibition Effect u.a. in der Anonymität, der Unsichtbarkeit (gerade in Foren, Chats oder textbasierten Interaktionen sehen Kommunikationspartner sich nicht) und in der zeitlich versetzten Kommunikation. Diese und weitere Faktoren führen dazu, dass Personen ihr Online-Verhalten wie ein fiktives Spiel ohne Regeln betrachten: „They split or dissociate online fiction from offline fact“ (Suler, 2004, S. 323). Perenc (2022) nennt ebenfalls explizit Merkmale des Internets, die kriminelle Aktivitäten von Psychopathen begünstigen. Neben der Anonymität und Asynchronität betont Perenc (2022) zusätzlich das Fehlen von „non-verbal indicators of interaction“ (S. 153). Gerade im Cyberspace könnte auf Täterseite somit leichter

ein Gefühl entstehen, ‚nur‘ Computer, Konten oder Systeme anzugreifen, nicht Menschen. Letztlich ist Cyberkriminalität jedoch keine Tat von Computer gegen Computer, sondern Mensch gegen Mensch. Auch Einstellungen der Schuldumkehr („Wer ein schwaches Passwort hat, ist ‚selbst schuld‘, gehackt zu werden“) sind online leichter aufrecht zu erhalten, wenn Täter mit dem Leid ihrer Opfer nie persönlich konfrontiert sind. Bandura (1999) begründete die *Moral Disengagement Theorie*, die 8 Mechanismen beschreibt, mit denen Taten gerechtfertigt werden. Drei der Aspekte nach Bandura, die in diesem Zusammenhang zu nennen sind, sind die „Diffusion of Responsibility“ (S. 198), die „Dehumanization“ (S. 200) und „Attribution of Blame“ (S. 203), also Schuld zu externalisieren und z.B. Opfern die Schuld zu geben.

Perenc (2022, S. 253) nennt zusätzlich das Fehlen klarer Normen im digitalen Raum. Ob oder inwiefern der Cyberraum enthemmt, hängt also eng mit der Frage der subjektiv wahrgenommenen Entdeckungswahrscheinlichkeit und der subjektiv wahrgenommenen (In)Kompetenz der Strafverfolgungsbehörden im Cyberspace zusammen.

Ganz grundsätzlich zeigen Menschen in der Logik des *Online Disinhibition Effects* also tendenziell online andere Persönlichkeitseigenschaften, agieren enthemmter in positiver und negativer Hinsicht, was zu der Frage führt, was eigentlich der echten Persönlichkeit, dem „true self“ (Suler, 2004, S. 324), entspricht. Sind viele Personen in Wahrheit viel psychopathischer, halten sich aber in der Realität zurück und zeigen online dann enthemmt ihre wahre Persönlichkeit? Oder ist es andersherum, dass Personen in Wahrheit mitfühlend sind, aber die strukturellen Merkmale des Internets sie zu „cyberpsychopaths“ (Perenc, 2022, S. 253) machen? Manche Autoren, Dissertationen und auch populärwissenschaftliche Publikationen nutzen die Begriffe „Cyber-Psychopathy“ (Nevin, 2015, S. 1) oder „Dark E-Personality“ (S. 1), um diese Kernthese zum Ausdruck zu bringen. Wenn der Cyberspace und seine strukturellen Merkmale Menschen online zu ‚Psychopathen‘ macht, unabhängig von deren eigentlicher Persönlichkeit, müsste dies auch gleichermaßen für White Hat Hacker gelten. Warum die einen dem Gesetz treu bleiben und andere es brechen, kann durch den

Online Disinhibition Effect allein nicht erklärt werden. Nach Suler (2004, S. 325) handelt es sich um ein komplexes Zusammenwirken aus Aspekten der Umwelt und Aspekten des Selbst, oder im Sinne Lewins Feldtheorie (1951) ist Verhalten auch im Cyberraum eine Funktion aus Person und Umwelt.

Im Rahmen der Befragung könnte es trotzdem von Interesse sein, den *Online Disinhibition Effect* zu operationalisieren, um Black Hats und White Hats diesbezüglich zu vergleichen.

3.4.3 Die White Gloves Theorie

Auf dem Grundgedanken, dass Menschen sich online anders verhalten, als sie es in der Realität tun würden, basiert die *White Gloves Theorie*. Die White Gloves Theorie ist ein cyberkriminologischer Erklärungsansatz, der den Gedanken einer vom Selbstbild in der realen Welt getrennten Online-Persönlichkeit weiterführt und in Theorieform gießt. Nach Acker (2023) basiert die Theorie auf zwei Grundgedanken: „Geringe Kosten im Sinne möglicher negativer Folgen [...] und die Trennung der digitalen Handlung vom analogen Image“ (S. 64). Dies verdeutlicht die Metapher weißer Handschuhe, da Handschuhe zum einen bewirken, dass jemand keine Fingerabdrücke hinterlässt (geringe Entdeckungswahrscheinlichkeit), aber weiße Handschuhe bedeuten auch, dass jemand sich nicht selbst beschmutzt, sie symbolisieren „Unschuld, aber auch ein reines Gewissen“ (Acker, 2023, S. 63). Im Sinne dieser Metapher von Acker wäre der Prozess des Onlinegehens das Anlegen der weißen Handschuhe: Was im Cyberraum passiert, lässt sich kaum zurückverfolgen und bleibt getrennt vom Selbstbild. Pointiert könnte die Überzeugung einiger Black Hat Hacker lauten: „What happens in Cyberspace, stays in Cyberspace“. Nach Acker (2023, S. 39) könnten Menschen also zeitgleich unterschiedliche Sets moralischer Überzeugungen haben für die digitale und analoge Welt. Basierend auf der bisherigen Literatur entwickelt Acker (2023) einen Vorschlag zur Operationalisierung und methodischen Überprüfung der Theorie: Ein Fehlverhalten oder eine Straftat wird jeweils in ihrer digitalen und analogen Variante ausformuliert und die Zustimmung, inwiefern man dies für moralisch vertretbar halte, abgefragt, z.B. „illegal Filme im Internet zu streamen“ (S.65) vs. „ohne Ticket

in einen Kinosaal zu schleichen, um einen Film zu gucken“ (S. 65). Gemäß der Theorie würden Menschen ggf. das Verhalten in der Realität moralisch ablehnen, es aber online für möglich oder weniger verwerflich halten. Acker (2023) spricht hier von „digitalen Obligationsprofile[n]“ (S. 67). In Bezug auf die Untersuchung von Hackern wäre es durchaus aufschlussreich, zu untersuchen und zu hinterfragen, ob sich ihre Moralvorstellungen in der digitalen und analogen Welt unterscheiden, und falls ja, was die Enthemmung auslöst. Kriminalität ist, wie erwähnt, nicht monokausal. Dass es einen Enthemmungseffekt im Cyberraum gibt, schließt nicht aus, dass Hacker hohe Ausprägungen in Bezug auf Merkmale der Dunklen Triade zeigen. Acker (2023) betont selbst „[d]ie White Gloves Theorie erklärt damit nicht die Motivation zur Begehung von Straftaten“ (S. 64).

3.4.4 Der Labelling-Ansatz

Labelling-Ansätze (dt. Etikettierungsansätze) befassen sich mit der Frage, was das gesellschaftliche Label ‚kriminell‘ oder ‚Black Hat Hacker‘ mit den Betroffenen selbst macht, aber auch mit der Wirkung auf andere und deren Reaktionen darauf. Kirwan & Power (2013, S. 24) erklären dies exemplarisch an dem Label, ein ‚Student‘ zu sein: Wer sich selbst als Student identifiziert, verhalte sich studententypisch und auch wenn jemand sich anderen Menschen als Student oder Studentin vorstellt, gehe das mit bestimmten Reaktionen oder auch Vorurteilen einher.

Bezogen auf Cybercrime geht es um die Frage, inwiefern das Label ‚Black Hat Hacker‘ Cyberkriminalität wahrscheinlicher macht. Diese Theorie wird implizit häufig angeführt, um der Gesellschaft eine Mitverantwortung zu geben. Wenn Personen (zu früh) als Kriminelle abgestempelt würden, mache dieser Prozess Kriminalität noch wahrscheinlicher. Gerade bei Cyberkriminalität scheint dies jedoch eine schwache Erklärung zu sein, da die Aufklärungsquoten in kaum einem Deliktsfeld geringer sind (Acker, 2023, S. 64). Hacker haben eben im realen Leben gerade *keine* Konsequenzen zu befürchten, und in Hacker-Foren im Darknet werden sie für ihre Taten nicht verurteilt und entscheiden selbst, wie viel sie von sich preisgeben.

3.4.5 Subkultur- und Lerntheorien

Es handelt sich bei Hackern mehrheitlich um junge Männer, die häufig bereits im Alter von 11-15 Jahren mit dem Hacking beginnen (Chiesa et al., 2009, S. 74). Bei Betrachtung bisheriger Theorien zu jugendlicher Delinquenz wird diese häufig aufgrund der Zugehörigkeit zu einer Subkultur erklärt. Cohen (1955) untersuchte Delinquenz von jugendlichen Gangmitgliedern. Nach Cohen (1955) sind Gangmitglieder häufig Teil einer sozial benachteiligten Schicht, die Frustration fühlen, da sie keinen höheren Status erreichen können. Sie schließen sich deshalb in Subkulturen zusammen, in denen sie die Normvorstellungen der Gesellschaft dann durch eigene Vorstellungen ersetzen. Kriminalität und Gewalt können dann akzeptierte Mittel in der Gruppe sein, um innerhalb der Subkultur Ansehen und Status zu gewinnen. Nach Lipp (1987) zeichnen sich Subkulturen dadurch aus, dass sie „Normenordnungen aufweisen, die vom Wertgefüge, den institutionellen Prämissen und Rollenerwartungen der Gesamtkultur abweichen“ (S. 196). Zweifelsohne sind auch Hacker Teil einer Subkultur mit eigenen Regeln, Foren und Slang (zur Hacking-Subkultur, siehe: Holt, 2019). Das Gefühl von Unzugehörigkeit kann jedoch nicht nur aus sozialen Unterschieden entstehen. Hacker stammen aus allen sozialen Schichten (BKA, 2015b, S. 11; Chiesa et al., 2009, S. 95). Einige Hacker geben jedoch an, Probleme mit sozialen Beziehungen zu haben, sowie schwächere oder gestörte Beziehungen zu Familienmitgliedern (BKA 2015b, S. 12). In der Befragung von Chiesa et al. (2009, S. 92) gaben einige Hacker selbst an, dass ihnen soziale Interaktionen im digitalen Raum leichter fielen als im persönlichen Kontakt. Rennie & Shore (2007, S. 238) nennen explizit Anerkennung innerhalb der Hacking-Subkultur als mögliches Motiv: „Hacking can install a sense of belonging by achieving the recognition of peers“. Gerade für jugendliche Hacker gelte die Zugehörigkeit zu einer Gruppe als wesentliches Motiv (BKA, 2015b, S. 18).

Cyberkriminalität aus der Zugehörigkeit zu Subkulturen und Darknet-Foren zu erklären, stellt eine Gegenhypothese zur bisherigen Vermutung dar, dass Black Hat Hacker psychopathischer und machiavellistischer sind als White Hat Hacker. Ggf. haben White Hat Hacker ihre Fähigkeiten im regulierten Rahmen gelernt (Universitäten oder Kurse), während

Black Hat Hacker frühzeitig ihre Fähigkeiten in Darknet-Foren und einer entsprechenden Subkultur gelernt haben. Die Entscheidung für oder gegen Kriminalität wäre dann nicht - im Sinne der Individualtheorien - primär auf Unterschiede der Persönlichkeiten (*traits*) zurückzuführen, es würde sich stattdessen um gelerntes Verhalten handeln. Gemäß der sozial-kognitiven Lerntheorie nach Bandura (1977) lernen Menschen am Modell, indem sie Verhalten beobachten sowie die Konsequenzen. Gemäß diesem Modell entscheidet das Umfeld maßgeblich darüber, welches Verhalten erlernt wird und ob jemand Hackingfähigkeiten eher im legalen oder illegalen Rahmen erlernt. Gerade im Darknet ist Kriminalität allgegenwärtig und scheint von außen betrachtet keine erkennbaren Konsequenzen zu haben. Angelehnt an die *Broken Window Theorie* spricht Rüdiger (2018) vom „Broken Web“ (S. 259). Wenn Gesetzesverstöße demnach keine sichtbaren Konsequenzen nach sich ziehen, führt dies zu immer weiteren Verstößen. Kirwan & Power (2013, S. 20) weisen im Zusammenhang mit Lerntheorien und Cybercrime auch auf die *operante Konditionierung* hin, nach der Menschen ihr Verhalten, je nach Konsequenzen (Belohnungen oder Bestrafungen), anpassen. Das ist bei Cyberkriminalität bedeutsam, da kaum ein anderes Deliktsfeld eine derart hohe Profitabilität bei gleichzeitig so geringer Entdeckungswahrscheinlichkeit hat. Das subjektive Kosten-Nutzen-Verhältnis ist aus Tätersicht besonders günstig. Somit könnten Täter vielleicht aus Spaß, zufälligem ‚Herumprobieren‘ oder Neugierde kleinere Delikte begangen haben (Kirwan & Power, 2013, S. 20). Durch die hohen Gewinne und einen Mangel an Konsequenzen könnte sich dieses Verhalten bis zu einer Hacker-Karriere eskalieren. Huber (2019, S. 68) nennt ebenfalls die *Rational Choice Theorie* in Bezug auf Cybercrime, bei der eine Entscheidung für ein Verhalten (z.B. Kriminalität) eine rationale Abwägung von Kosten und Nutzen darstellt. Die *Rational Choice Theorie* ist gerade bei Cyberkriminalität bedeutsam (Rüdiger, 2023, S.10), da hier eine hohe Profitabilität (Nutzen) einer geringen Entdeckungswahrscheinlichkeit (Kosten) entgegensteht.

3.5 Fragestellungen der Arbeit

Eine Vielzahl von Studien belegt Zusammenhänge zwischen der Dunklen Triade (besonders Psychopathie und Machiavellismus) und nahezu allen Arten antisozialen Verhaltens (siehe Kapitel 3.1.1). Erste Ergebnisse deuten darauf hin, dass die Dunkle Triade auch in Bezug auf Black Hat Hacking eine bedeutsame Rolle spielen könnte (siehe Kapitel 3.1.2). Ob sich Black Hat Hacker und White Hat Hacker hinsichtlich der Triademerkmale unterscheiden, soll empirisch überprüft werden.

Die Kernhypothese der empirischen Studien ist die Annahme, dass sich Black Hats und White Hats hinsichtlich ihrer Persönlichkeit unterscheiden, also Black Hats ‚dunklere‘ Persönlichkeitsmerkmale aufweisen. Psychopathie ist die komplexeste der drei Triadeeigenschaften. Es handelt sich um ein mehrdimensionales, breites Konstrukt, weshalb nach Möglichkeit zwischen den beiden Faktoren primärer und sekundärer Psychopathie differenziert werden sollte.

Bei der Betrachtung der Literatur und aktuellen empirischen Studien sind neben der Dunklen Triade weitere Aspekte zu Tage getreten, die cyberkriminelles Verhalten (mit)erklären könnten, da davon auszugehen ist, dass Cyberkriminalität nicht monokausal erklärbar ist. Möglicherweise lernen Black Hat Hacker ihre Fähigkeiten öfter aus informellen, ‚dunklen Quellen‘, wie Darknet-Foren (Kontext: Lerntheorien). Möglicherweise gibt es enthemmende Faktoren des Cyberspace, die Kriminalität begünstigen (Kontext: Online Disinhibition Effect). Ebenfalls ist die Frage von Interesse, ob es Korrelationen zwischen bevorzugten Angriffsarten und Persönlichkeitsmerkmalen gibt (Kontext: Cyber-Profiling) und wie Black Hat Hacker bereits heute KI für ihre Taten einsetzen (Kontext: Zukunftsrelevanz). Neben der Dunklen Triade sollten auch diese Aspekte bei der Befragung von Black Hats und White Hats empirisch überprüft werden.

Ein klares Bild der Profile, Motive und Triademerkmale soll durch drei Studien im Sinne eines *Mixed Method Designs* nach Creswell & Plano Clark (2018) gewonnen werden. Die Studien

haben jeweils einen unterschiedlichen forschungsmethodischen Zugang, sodass im Sinne der Triangulationsmetapher (Flick, 2004) ein ganzheitlicher Blick auf den Forschungsgegenstand ermöglicht wird. Die Hypothesen, Methoden, Durchführung sowie die kritische Diskussion der Ergebnisse werden zuerst *je Studie* dargestellt (Kapitel 4, 5 und 6) und im Anschluss in einem gemeinsamen Diskussionsteil zusammengefasst und zueinander in Beziehung gesetzt werden (Kapitel 7).

4 Studie 1: Quantitative Inhaltsanalyse der FBI Most Wanted Hacker

4.1 Zielsetzung, Forschungsfragen, Hypothesen

Seit 2010 führt das FBI eine separate ‚Most Wanted Liste‘ ausschließlich für Hacker, die *FBI Cyber Most Wanted Fahndungsliste*. Ziel der ersten Teilstudie ist es, ein klares Bild der demografischen Merkmale von Black Hat Hackern zu erhalten (Durchschnittsalter, Geschlechterverteilung und Nationalitäten). Hierzu sollen alle FBI-Fahndungsplakate der Cyber Most Wanted Liste von 2010 bis 2024 inhaltsanalytisch ausgewertet werden. Die Aussagekraft und Übertragbarkeit der Nationalitäten der angreifenden Länder ist hierbei jedoch eingeschränkt, da es sich um die Fahndungsliste des FBIs (also der USA) handelt. Wo die Gefahr geopolitisch zu verorten ist, stellt damit ausschließlich eine US-amerikanische Perspektive dar.

Die quantitative Inhaltsanalyse ist nach Brosius, Haas & Unkel (2022) eine häufig genutzte Methode der Kommunikationswissenschaft und auch Gewaltforschung, wobei sie in der Psychologie weniger etabliert ist (S. 143-144). „Der Untersuchungsgegenstand der Inhaltsanalyse sind nicht Personen wie bei der Befragung, sondern es sind in der Regel Medieninhalte“ (Brosius et al., 2022, S. 144). Diese Medieninhalte können nach Brosius et al. (2022, S. 144) sehr unterschiedlicher Natur sein und von Zeitungsartikeln bis Social-Media-Beiträgen reichen oder - wie im vorliegenden Fall - digital publizierte Fahndungsplakate des FBIs sein.

In dieser ersten Teilstudie sind der Untersuchungsgegenstand also nicht direkt cyberkriminelle Akteure, sondern Fahndungsplakate, mit denen nach Hackern gefahndet wird. Vorteil der Methodik der Inhaltsanalyse ist, dass der Untersuchungsgegenstand (Fahndungsplakate) non-reaktiv ist und es sich um behördlich validierte Informationen handelt. Die demografischen Daten basieren auf Ermittlungsergebnissen der US-Strafverfolgungsbehörden und nicht freiwilligen Selbstauskünften der Täter. Es ist zudem möglich, weiter zurückliegende Daten (z.B. ab 2010) mit einzubeziehen. Wie die Fahndungsplakate beschafft werden, wie frühere, bereits gelöschte Daten rekonstruiert

werden können und nach welchen Regeln was codiert wird, soll intersubjektiv nachvollziehbar beschrieben werden, sodass die Untersuchung auch jederzeit unter identischen Bedingungen replizierbar ist.

Über Befragungen lassen sich zwar innere Einstellungen, Persönlichkeitseigenschaften und Motive erheben, aber Black Hat Hacker in anonymen Darknet-Foren sind besorgt um ihre Operational Security und geben kaum valide, präzise Informationen zu ihrem Alter oder ihren Nationalitäten preis. Bei Fahndungsplakaten verhält es sich andersherum: Es lassen sich formelle soziodemografische Daten codieren, wobei sich mit dieser Methodik keine Einstellungen, Motive oder Persönlichkeitsdispositionen erfassen lassen.

Im Sinne der „Methodentriangulation“ (Flick, 2004, S. 42) zielt die Studie 1 auf valide soziodemografische Daten ab, die eine Online-Befragung in Hacker-Foren (Studie 2) nicht im Stande ist zu liefern.

Es wurden fünf Variablen ausgewählt, die inhaltsanalytisch codiert werden sollen: das Geschlecht, das Alter, die Nationalität (Land), die Zugehörigkeit zu Nachrichtendiensten oder Militäreinheiten sowie die Höhe der ausgelobten Belohnung des FBIs.

Geschlecht und Durchschnittsalter sind relevante demografische Daten und können vor allem für gezielte Präventionsansätze relevant sein, da gerade bei jungen Personen die Chance zur Intervention besteht und die Talente noch in legale Bahnen gelenkt werden könnten. Je präziser sich das Profil von Hackern demografisch eingrenzen lässt, desto besser sind die Chancen für eine *selektive Prävention*, die sich an bestimmte Risikogruppen richtet (z.B. Bürger & Kaess, 2024).

Die Variablen Nationalität, Nachrichtendienstzugehörigkeit und FBI-Belohnung werden erhoben, um der geopolitischen Komponente von Cybercrime Rechnung zu tragen. So weisen beispielsweise Fyshchuk, Noesgaard & Nielsen (2024) darauf hin, dass die Cyberangriffe aus Russland seit Beginn des Ukrainekrieges zugenommen haben. Cybercrime ist politisch. Teils wird Cyberkriminalität gegen die Vereinigten Staaten auch direkt von anderen Staaten bzw. deren Nachrichtendiensten ausgeführt oder orchestriert (z.B. Holt et al., 2023). Manche Personen auf der Cyber Most Wanted Liste tragen militärische

Uniformen und sind Mitarbeiter oder Offiziere der Nachrichtendienste geopolitischer Kontrahenten der USA. Codiert wird, ob ein Hacker Teil eines fremden Geheimdienstes ist (staatliche Akteure) und wie hoch die Belohnung des FBIs für Hinweise ist, die zur Festnahme führen. Die Belohnung des FBIs ist dabei als Indikator für den Fahndungsdruck und die Relevanz für die nationale Sicherheit der USA zu werten.

Die Forschungsfragen der ersten Teilstudie lauten:

F1: Wie ist die Geschlechterverteilung innerhalb der FBI Most Wanted Hacker?

F2: Wie alt sind die FBI Most Wanted Hacker durchschnittlich zum Tatzeitpunkt?

F3: Welche Nationalitäten sind am häufigsten vertreten innerhalb der FBI Most Wanted Hacker?

F4: Wie viele Akteure sind *Nation State Threat Actor* und stehen direkt oder indirekt mit Nachrichtendiensten oder Militäreinheiten in Verbindung?

F5: Wie hoch ist die durchschnittlich genannte Belohnung des FBIs und wie unterscheidet sich die durchschnittliche Belohnung bei staatlichen vs. nicht-staatlichen Akteuren?

Auf Basis der geopolitischen Relevanz von Cyberkriminalität und den bisherigen empirischen Erkenntnissen zu Hackerprofilen (siehe aktueller Forschungsstand Kapitel 3.3) lauten die Hypothesen:

H1: Hacker sind zu über 80 % männlich.

H2: Hacker sind zum Tatzeitpunkt eher jung (Durchschnitt, Modus und Median unter 30).

H3: Die Nationalitäten der FBI Cyber Most Wanted spiegeln die geopolitischen Konflikte und Kontrahenten der USA wider (vor allem Russland und China).

H4: Mehr als ein Drittel der gesuchten Hacker haben eine direkte oder indirekte Verbindung zu Nachrichtendiensten.

H5: Vor allem bei Tätern, die eine Verbindung zu anderen Nachrichtendiensten haben, ist der Fahndungsdruck groß und es werden Belohnungen über eine Million USD angesetzt.

4.2 Forschungsdesign

4.2.1 Untersuchungsgegenstand und Zeitraum

Untersuchungsgegenstand sind Fahndungsplakate im PDF-Dateiformat des FBIs der meistgesuchten Hacker (Straftäter im Bereich *Cybercrime im engeren Sinne*) von 2010 bis 2024.

Die Fahndungsliste der USA wurde gewählt aus Gründen der Relevanz, der Verfügbarkeit und der (teilweise möglichen) Übertragbarkeit auf Deutschland.

Im Erhebungszeitraum September bis November 2022 zielten rund 65 % der entdeckten Cyberangriffe auf Unternehmen in den USA, gefolgt von Japan mit 8 % (Statista, 2025b). Die USA sind somit am stärksten Cyberangriffen ausgesetzt. Da Cyberkriminalität eine ausgeprägte geopolitische Komponente hat und sowohl die USA als auch Deutschland Teil des Westens sowie der NATO sind, haben die Daten der USA auch für Deutschland eine gewisse Relevanz. Deutschland ist auch Teil des Westens, Mitglied der NATO und unterstützt ebenfalls die Ukraine, sodass es zumindest Schnittmengen zwischen den geopolitischen Spannungsfeldern der USA und Deutschlands gibt.

Neben der inhaltlichen Relevanz der USA ist die Verfügbarkeit der Daten der dritte Grund, warum die Cyber Most Wanted Liste des FBIs ausgewählt wurde.

Seit 2010 misst das FBI dem Thema Cyberkriminalität eine besondere Bedeutung bei und publiziert eine eigene Most Wanted Liste ausschließlich zum Thema Cybercrime, was die meisten anderen Staaten bis dato nicht tun. Europol publiziert eine allgemeine Europe's Most Wanted Liste³, die primär auf Morde und schwere Gewaltkriminalität fokussiert ist. Zum Zeitpunkt Januar 2025 waren beispielsweise lediglich 54 Personen auf der Europe's Most Wanted Liste von Europol und davon 0 im Bereich *Cybercrime im engeren Sinne*.

Unter der URL <https://www.fbi.gov/wanted/cyber> veröffentlicht das FBI seit 2010 die Cyber Most Wanted Liste, also Täter im Bereich *Cybercrime im engeren Sinne*, und grenzt dies von *Cybercrime im weiteren Sinne* ab (siehe Definition Kapitel 2.1). Abbildung 7 zeigt die Übersichtsansicht der meistgesuchten Hacker. Beim Anklicken einer der gesuchten

³ <https://eumostwanted.eu/>

Personen steht das Fahndungsplakat als PDF-Datei zum Download bereit, das neben einem oder mehreren Fotos auch Angaben zu Geschlecht, Nationalität, Geburtsdatum, Tatvorwürfen, Tatzeiträumen, sowie dem Datum des Haftbefehls enthält. Die Analyseeinheit bildet somit jeweils ein einzelnes Fahndungsplakat eines FBI Most Wanted Hackers im Zeitraum von 2010 bis 2024.

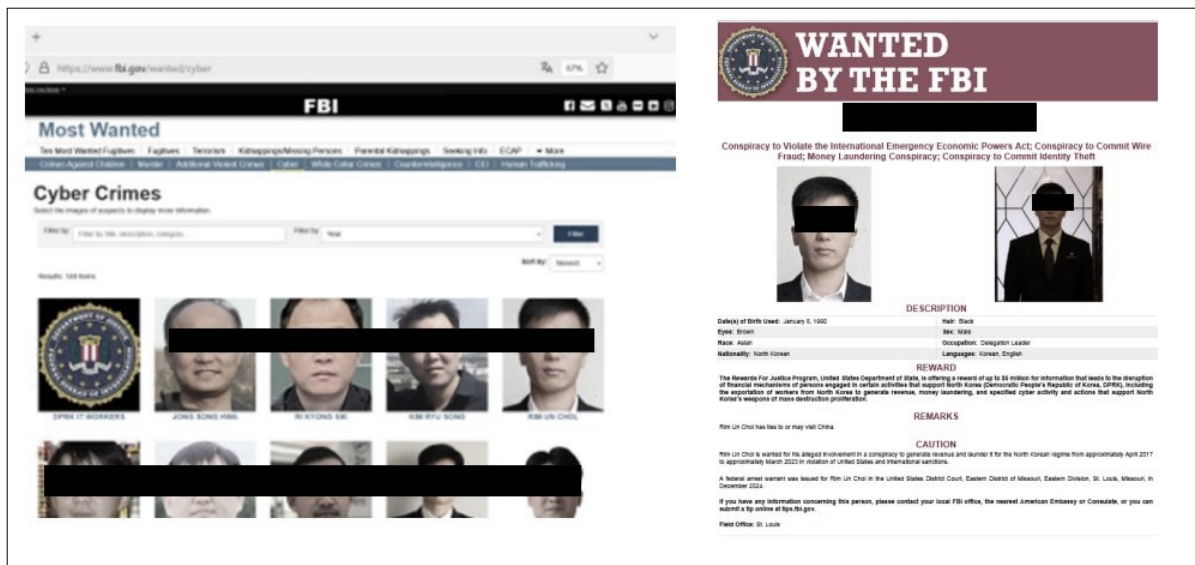


Abbildung 7. Anonymisierte Screenshots FBI Cyber Most Wanted

Quelle: FBI (2025a) fbi.gov/wanted/cyber

4.2.2 Materialbeschaffung durch die Wayback Machine (Internet Archive)

Um nicht nur die aktuell publizierte Liste gesuchter Hacker zu codieren, sondern auch rückwirkend ab 2010, wurde auf archivierte Daten zurückgegriffen.

Die *Wayback Machine* ließe sich als ein ‚digitales Archiv des gesamten Internets‘ charakterisieren und ist somit eine Manifestierung dessen, was durch die Redewendung „Das Internet vergisst nie“ zum Ausdruck kommt. Die *Wayback Machine* wird unter der Seite <https://web.archive.org> von der gemeinnützigen Organisation *Internet Archive* betrieben. Die *Wayback Machine* eröffnet damit eine Möglichkeit, quasi in der Zeit ‚zurückzuspulen‘ und die dort archivierten Webseiten in ihrem Zustand zu beliebigen Zeitpunkten der Vergangenheit zu betrachten. Sie ist deshalb ein beliebtes Ermittlungs- und Recherchetool für Polizei und Nachrichtendienste für OSINT, was für *Open Source Intelligence* steht, also die Analyse

öffentlich verfügbarer Informationen. Das Internetarchiv ermöglicht es z.B. Investigativjournalisten oder Forschern, frühere Versionen von öffentlichen Webseiten aufzurufen, auch wenn die Seiten mittlerweile längst verändert oder gelöscht wurden. Die *Wayback Machine* nutzt dafür sogenannte Webcrawler (automatisierte Bots), um Momentaufnahmen öffentlich zugänglicher Webseiten in regelmäßigen Abständen zu archivieren. Eine solche Momentaufnahme zu einem beliebigen Zeitpunkt nennt sich *Snapshot*.

Von der Webseite der Universität Tübingen wurden z.B. zwischen 1996 und 2025 insgesamt 28.097 Snapshots archiviert. Beim Anklicken einer der Snapshots gleicht dies einer digitalen Reise in die Vergangenheit; so lässt sich z.B. die Website der Universität Tübingen ansehen, wie sie 1997 aussah. Abbildung 8 zeigt die Darstellung der Website der Universität Tübingen zum 16. März 1997 sowie die kalendarische Übersicht der verfügbaren Snapshots im Zeitverlauf.

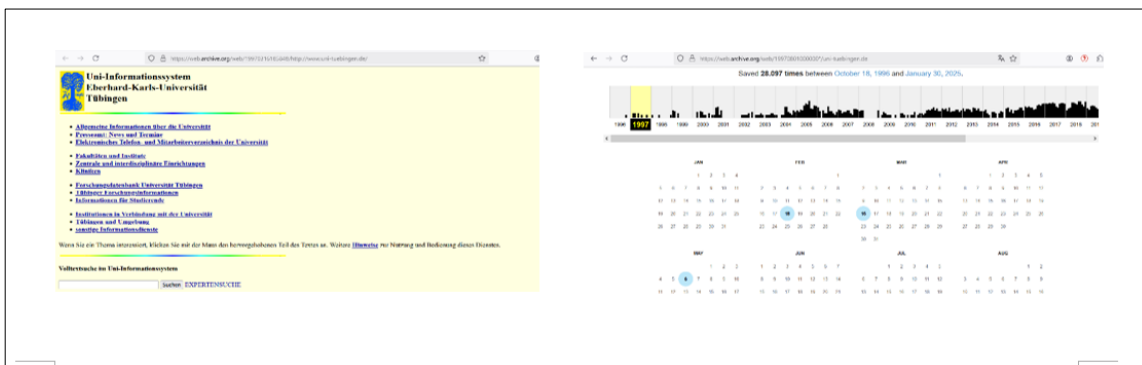


Abbildung 8. Screenshot *Wayback Machine* (2025a), Archivierte Seite der Uni Tübingen

Weder die Nutzung noch die Aktivitäten der *Wayback Machine* sind verboten. Es ist vergleichbar mit der Sammlung alter Zeitungsartikel, es ist eine Sammlung öffentlicher Informationen zu vergangenen Zeitpunkten. Nutzer haben zudem das Recht und die Möglichkeit, die eigene Website aus der *Wayback Machine* auszuschließen und die archivierten Daten somit zu löschen. Da jedoch die wenigsten Personen, Organisationen oder Prominenten überhaupt von der Existenz dieser Technologie wissen, sind fast alle Webseiten des Internets in der Rückschau verfügbar. Laut Angaben des Internet Archives wurden 916 Milliarden (engl. *billion*) Webseiten archiviert. Auch die Webseite des FBIs ist verfügbar und

lässt sich zu beliebigen Zeitpunkten der Vergangenheit rekonstruieren. Bei Prüfung der URL www.fbi.gov/wanted/cyber stellte sich heraus, dass auch diese URL seit ihrer Existenz 2010 archiviert wurde und insgesamt 1.978 gespeicherte Momentaufnahmen bis 2024 existieren, mit teilweise fast täglicher Abdeckung (Abbildung 9).

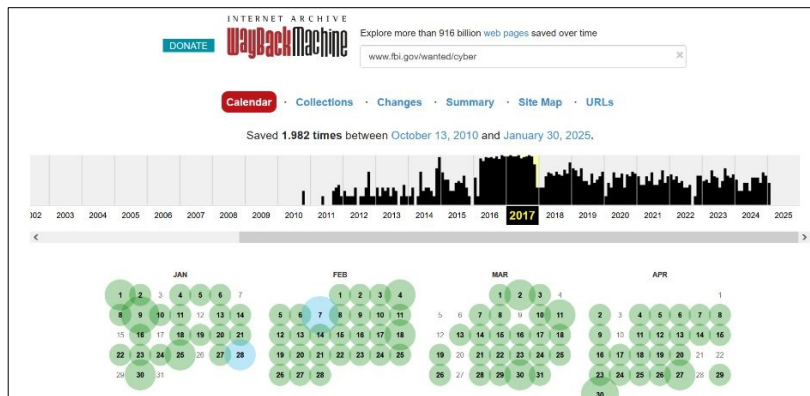


Abbildung 9. Screenshot *Wayback Machine* (2025b): Archivierung der Cyber Most Wanted

Beginnend mit dem ersten Snapshot am 13.10.2010 wurden alle 1.978 archivierten Momentaufnahmen der Website einzeln analysiert und jeder neu aufgenommene Most Wanted Hacker als Fahndungsplakat im PDF-Format gespeichert. Dies hat die Datenmenge und Fallzahl jedoch nicht in dem Ausmaß erhöht, wie erwartet. Im Jahr 2010 hat das FBI beispielsweise nur nach 5 Hackern gefahndet. Ende 2011 waren es 6 Personen.

Eine weitere Erkenntnis ist, dass seit 2010 zwar immer mehr Hacker auf der Liste hinzukamen, aber kaum Hacker von der Fahndungsliste gelöscht wurden. Ende 2014 (31. Dezember) waren beispielsweise 18 Hacker auf der Cyber Most Wanted Liste. Zum 31.1.2025 (also mehr als ein Jahrzehnt später) sind 12 der 18 Hacker, also zwei Drittel, noch immer auf der Liste zu finden.

Jedoch ist auch das eine wesentliche Erkenntnis: Wer auf der FBI Cyber Most Wanted Fahndungsliste aufgeführt wird, bleibt dort mit großer Wahrscheinlichkeit für sehr lange Zeit (teils über ein Jahrzehnt), was für die geringe Verurteilungsquote spricht.

Dies liegt primär an der Schwierigkeit, Personen festzunehmen, die ihren Wohnsitz und gewöhnlichen Aufenthalt im Ausland haben, welches nicht an die USA ausliefert. Zahlreiche Personen auf der Fahndungsliste tragen militärische Uniformen und sind Teil

nachrichtendienstlicher Aktivitäten z.B. Russlands, Chinas oder Nordkoreas. Wer Cyberangriffe im Staatsdienst ausführt, hat im Heimatland keine Strafverfolgung oder Auslieferung zu befürchten.

Die FBI Cyber Most Wanted Liste ist also eher im Sinne einer kumulativen Liste zu verstehen, die 2010 mit 5 publizierten Hackern begann und im Zeitverlauf auf ca. 150 Personen angewachsen ist, wobei immer neue Täter hinzugekommen sind und nur wenige im Zeitverlauf von der Liste gelöscht wurden. Abbildung 10 zeigt die Anzahl der gesuchten Hacker jeweils zur letzten verfügbaren Momentaufnahme eines Jahres im Erhebungszeitraum.

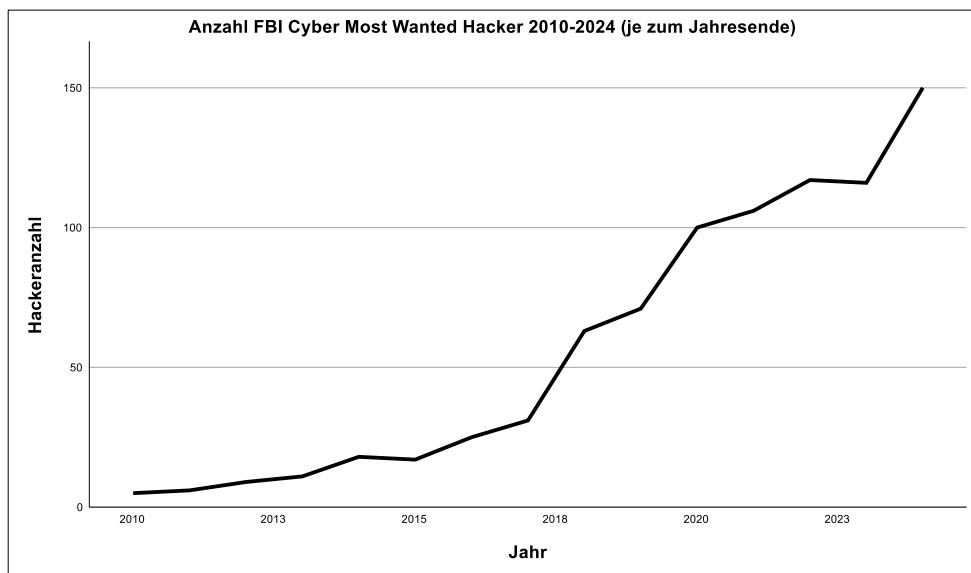


Abbildung 10. Anzahl gesuchter Hacker im Zeitverlauf

Quelle: Eigene Darstellung.

Das Diagramm verdeutlicht, dass es sich um eine kumulative Liste handelt, weshalb beispielsweise ein Zeitvergleich der Hackerprofile der Jahre 2010 und 2020 nicht sinnvoll wäre.

Mithilfe des *Internet Archives* konnten 170 Cyber Most Wanted Fahndungsplakate im PDF-Format gesichert werden, was einer Vollerhebung aller publizierten Hacker des FBIs im Untersuchungszeitraum 2010-2024 entspricht.

Es sei darauf hingewiesen, dass die meistgesuchten Hacker der USA nicht dem Durchschnitt aller Black Hat Hacker entsprechen, sondern möglicherweise eher dem oberen Prozent,

gemessen an den technischen Fertigkeiten und der Schwere der Taten. Die meisten Täter auf der Liste haben besonders schwere Taten begangen oder die nationale Sicherheit oder demokratische Wahlen beeinflusst. Beschrieben wird durch die Daten letztlich nicht unbedingt der ‚typische Black Hat Hacker‘, sondern ‚der typische ‚FBI Most Wanted Hacker‘. Dass es sich dabei um eine extremere Stichprobe und ausschließlich eine US-Perspektive handelt, wird im Diskussionsteil und bei der Einordnung der Ergebnisse entsprechend kritisch berücksichtigt.

4.2.3 Definition der Analyseeinheit und Auswahleinheit

Die Analyseeinheit ist ein einzelnes FBI Cyber Most Wanted-Fahndungsplakat im PDF-Format im Untersuchungszeitraum 2010 bis 2024. Es konnten mithilfe des Internetarchives 170 PDF-Dateien gesichert werden. Im Zeitverlauf ist der strukturelle Aufbau der Fahndungsplakate nicht ganz konsistent, aber ähnlich. Grundsätzlich sind Name, begangene Delikte, Fahndungsfotos, Geburtsdatum, Nationalität und Geschlecht aufgeführt, sowie eine mögliche Belohnung für Hinweise (engl. *reward*) und weitere Merkmale zur Identifikation (engl. *remarks*). Der Bereich *Caution* oder *Details* enthält eine Beschreibung der Taten, in denen meistens der Ort der Opfer und Täter genannt wird, eine Tatzeit oder ein Tatzeitraum sowie das Datum und der Ort des US-Gerichts, an dem der Haftbefehl erlassen wurde. Abbildung 11 zeigt beispielhaft die Struktur eines Fahndungsplakates.

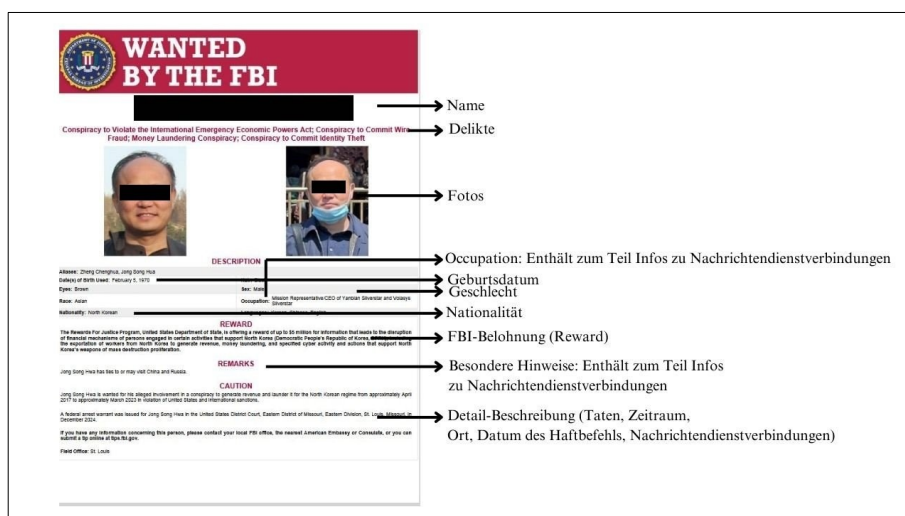


Abbildung 11. Aufbau eines FBI-Fahndungsplakats (Analyseeinheit, anonymisiert)

Quelle: FBI (2025a), URL: www.fbi.gov/wanted/cyber

Auswahleinheit/ Aufgreifkriterium

In der Inhaltsanalyse entspricht die Bestimmung der Auswahleinheit der Stichprobenziehung (Rössler & Geise, 2013, S. 273). Es werden sogenannte *Aufgreifkriterien* bestimmt, die darüber entscheiden, welche Inhalte in die Analyse einbezogen werden (Rössler & Geise, 2013, S. 275). Da es sich um eine Vollerhebung handelt, entspricht die Auswahleinheit weitestgehend der Analyseeinheit. Die beiden Aufgreifkriterien, die entscheiden, ob oder welche der 170 Plakate codiert werden, sind (1), dass es sich um eine identifizierbare Einzelperson handelt (keine Gruppen) und (2) die Person ein Black Hat Hacker ist, also *Cybercrime im engeren Sinne* begangen hat (siehe Definition Kapitel 2.2).

Erstes Aufgreifkriterium: Einzelpersonen

Codiert werden nur die Fahndungsplakate auf denen identifizierbare Einzelpersonen zu sehen sind (keine Gruppen). Beim Namen ist bereits erkennbar, ob es sich um einen Gruppennamen (z.B. DPRK IT Workers) oder einen Namen einer natürlichen Person handelt. Alle Personen auf Gruppenfahndungen sind ebenfalls als Einzelpersonen Teil der Liste. Die Gruppenfahndungen auszuschließen, reduziert also nicht die Materialmenge, sondern vermeidet lediglich Dopplungen. Zudem werden auf den Gruppen-Plakaten keine demografischen Angaben zu Alter oder Nationalität publiziert.

Zweites Aufgreifkriterium: Black Hat Hacker (Cybercrime im engeren Sinne)

Direkt unter dem Namen wird eine Liste von Delikten aufgeführt, die begangen wurden. Codiert wurden lediglich Black Hat Hacker, also Personen, die *Cybercrime im engeren Sinne* begangen haben. Dies sind Taten, die direkt auf Daten oder Informationssysteme abzielen und ohne Computer nicht möglich wären. Häufig sind die Worte ‚Wire‘ oder ‚Computer‘ wörtlicher Teil der Strafnorm (siehe auch: Wernert, 2021). Ausgeschlossen werden Taten, die lediglich mithilfe von Informationstechnologie begangen wurden, wie z.B. die Verbreitung kinderpornografischer Inhalte oder der Online-Drogenhandel. Die Cyber Most Wanted Liste bezieht sich ausschließlich auf Hacker (*Cybercrime im engeren Sinne*). Dennoch sollte vor

Codierung geprüft werden, ob die Person mindestens eines oder mehrere der folgenden Delikte im Sinne des US-Strafrechts⁴ begangen hat:

- *Computer Intrusion*
- *Intentional Damage to a Protected Computer*
- *Threats Relating to a Protected Computer*
- *Conspiracy to Commit Wire Fraud*
- *Wire Fraud*
- *Aggravated Identity Theft*
- *Conspiracy to Obtain Information from a Protected Computer*
- *Commit Fraud Involving Authentication Features*
- *Commit Aggravated Identity Theft*
- *Commit Access Device Fraud*
- *Commit Wire Fraud While Falsely Registering Domains*
- *Wire Fraud*
- *Conspiracy to Commit Computer Hacking*
- *Identity Theft*
- *Conspiracy to Commit Fraud and Related Activity in Connection with Computers*
- *Transmitting a Demand in Relation to Damaging a Protected Computer*
- *Conspiracy to Access Protected Computers and Obtain Information and to Intentionally Damage Protected Computers by Knowing Transmission*

Ausgeschlossen werden Personen, die nicht als Hacker klassifiziert werden können, da sie lediglich das Internet zum Begehen anderer Taten nutzen, wie z.B. Online-Waffenhandel oder Online-Drogenhandel (engl. *Drug Trafficking*).

Basierend auf den genannten Aufgreifkriterien wurde die Anzahl der zu codierenden Fahndungsplakate von 170 auf $N = 145$ reduziert.

Endergebnis der Materialbeschaffungsphase waren somit 145 gespeicherte PDF-Dateien, sowie eine SPSS-Datei, in der die 145 Fälle mit Namen der Täter und Kategorien zur Codierung vorbereitet wurden.

⁴ Beispielhafte Liste der Cybercrime im engeren Sinne betreffenden US-Strafnormen, entnommen aus Fahndungen der Cyber Most Wanted Liste (FBI, 2025a)

4.2.4 Kategorien, Codebuch, Datenerhebung

Ziel der Codierung ist es, aus den 145 Fahndungsplakaten die relevanten Informationen zur Beantwortung der Forschungsfrage systematisch zu extrahieren; das Codebuch ist dabei „[d]as Regelwerk, nach denen diese Erfassung erfolgt“ (Rössler & Geise, 2013, S. 278). Das Codebuch ist somit das Herzstück der Inhaltsanalyse, da es alle Kategorien und trennscharfe Regeln enthält, was in welcher Form codiert werden soll (Brosius et al., 2022, S. 163). Als relevante Variablen zur Beantwortung der Forschungsfragen und Prüfung der Hypothesen wurden zehn zu codierende Variablen ausgewählt (Tabelle 3).

Tabelle 3: Kategorien des Codebuchs

Direkt codierte Variablen	Später berechnet
1. Name	9. Abstand Tat zu Haftbefehl
2. Geschlecht	10. Alter zur Tatzeit
3. Nationalität (Land)	
4. Nachrichtendienstzugehörigkeit (dichotom, ja/nein)	
5. FBI-Belohnung (in USD)	
6. Geburtsdatum	
7. Mittlerer Tatzeitpunkt	
8. Datum Haftbefehl	

Der Name der gesuchten Person dient gleichzeitig als ID/ Identifikationsvariable pro Fall.

Da es sich primär um formelle Kategorien handelt, wurde im Sinne der intersubjektiven Nachvollziehbarkeit und Reliabilität ein möglichst einfaches Codebuch erstellt (Anhang 1), das beschreibt, wo auf den Plakaten die Informationen zu finden sind und wie diese zu codieren sind.

Es folgte eine Testcodierung von 20 Plakaten, bei denen doch einige Sonderfälle, Ausnahmen und Schwierigkeiten aufgetreten sind. Beispielsweise gibt es Hacker, bei denen das FBI nicht sicher über das korrekte Geburtsdatum ist und zwei mögliche Daten angibt, die aber teilweise mehrere Jahre auseinanderliegen. In einigen Fällen nutzt das FBI anstelle konkreter Monatsangaben unschärfere Zeitangaben, wie z.B. ‚Summer of 2009‘.

Auf Basis der Ausnahmen und Sonderfälle bei der Testcodierung wurde das Codebuch angepasst und für jeden möglichen Grenzfall eine eindeutige Regel festgelegt. Die finale Version des Codebuchs enthält eine eindeutige Regel für alle gefundenen Grenz- und Sonderfälle.

Während Geschlecht, Nationalität (Land) oder die ausgelobte Belohnung leicht direkt zu codieren sind, war die Bestimmung des Alters von Hackern weniger trivial, als es auf den ersten Blick erscheint. Das Geburtsdatum allein ist wenig aussagekräftig, denn von Interesse ist ja nicht das heutige Alter der Täter, sondern wie alt sie zur Tatzeit waren. Insbesondere bei einem so langen Untersuchungszeitraum, von 2010 bis 2024, ist völlig unerheblich, wie alt ein Täter heute wäre. Von Interesse ist also das Alter zum Tatzeitpunkt, wofür also mindestens zwei Kategorien codiert werden müssen: Das Geburtsdatum und der Tatzeitpunkt. Das nächste Problem besteht darin, dass es bei Cybercrime oft keinen *Tatzeitpunkt*, sondern einen *Tatzeitraum* gibt.

Bei Cybercrime sind Tatort und Tatzeit komplexer zu bestimmen als bei Gewaltkriminalität. Gewaltdelikte oder Raubüberfälle setzen voraus, dass Täter und Opfer zur selben Zeit am selben Ort sein müssen. Es gibt einen (und nur einen) eindeutigen Tatort und eine Tatzeit. Bei Cybercrime können sich Täter und Opfer in unterschiedlichen Ländern befinden und auch die Tatzeit kann sich beim Hacking, Ausspähen von Daten oder Angriffen auf Informationssysteme über Monate oder Jahre ziehen. Wird ein Tatzeitraum genannt, wird der mittlere Tatzeitpunkt bestimmt.

Es gibt eine Reihe von Fällen, bei denen zwar das Geburtsdatum angegeben ist, ebenfalls das Datum des Haftbefehls, aber kein Tatzeitpunkt. Der Haftbefehl liegt meist wenige Jahre hinter dem mittleren Tatzeitpunkt. Bestimmt man also den Durchschnittswert, wie viele Jahre zwischen mittlerem Tatzeitpunkt und Haftbefehl liegen, lässt sich im Umkehrschluss aus dem Datum des Haftbefehls ein ungefährender mittlerer Tatzeitpunkt abschätzen. Aus diesem Grund wurde das Datum des Haftbefehls mitcodiert.

Alle zeitbezogenen Kategorien (Geburtsdatum, mittlerer Tatzeitpunkt, Datum Haftbefehl, Abstand Tat zum Haftbefehl) sind lediglich Mittel zum Zweck, um daraus die eigentliche

Zielvariable zu berechnen, nämlich das Alter zum Tatzeitpunkt. Codiert wurde direkt in die SPSS-Datenansicht. Der vollständige SPSS-Datensatz mit den vom FBI publizierten Klarnamen, sowie alle codierten Fahndungsplakate im PDF-Format wurden den Betreuern auf einem USB-Datenträger bei Abgabe ausgehändigt.

4.2.5 Berechnung des Alters zur Tatzeit

Das Alter hat eine hohe Relevanz, da daraus wichtige Implikationen z.B. zur Prävention abgeleitet werden können. Wenn Tatzeit und Geburtsdatum codiert werden konnten, lautet die Formel für das Alter:

Alter zur Tatzeit = Mittlerer Tatzeitpunkt - Geburtsdatum

Bei insgesamt 40 Fällen war kein Tatzeitpunkt genannt, dafür aber das Geburtsdatum und das Datum des Haftbefehls. Zuerst musste bestimmt werden, wie viele Monate der Haftbefehl im Durchschnitt hinter dem mittleren Tatzeitpunkt liegt. Hierfür wurden die 86 Fälle einbezogen, bei denen sowohl der mittlere Tatzeitpunkt als auch das Datum des Haftbefehls direkt codiert werden konnten (siehe Tabelle 4).

Tabelle 4: Deskriptive Statistiken: Abstand Tat zu Haftbefehl, $n = 86$

	Minimum	Maximum	<i>M</i>	<i>SD</i>
Zeitr. Abstand zwischen Tat und Haftbefehl in Monaten	4	109	36.29	20.71

Der Haftbefehl liegt im Durchschnitt 36.29 Monate (= 3.02 Jahre) hinter dem mittleren Tatzeitpunkt ($SD = 20.71$ Monate). Mit der Formel *Datum des Haftbefehls* minus 3 Jahre lässt sich also eine Annäherung an den Tatzeitpunkt erreichen, statt diese Daten völlig auszuschließen.

Geschätzter Tatzeitpunkt = Datum Haftbefehl - 3 Jahre

Bei den 40 Fällen, bei denen keine Daten zum Tatzeitpunkt codiert werden konnten, aber Geburtsdatum und Datum des Haftbefehls, lautet die Formel:

Alter zur Tatzeit = (Datum Haftbefehl - 3 Jahre) - Geburtsdatum

Im Sinne der intersubjektiven Nachvollziehbarkeit enthält das Codebuch (Anhang 1) Anweisungen zur Codierung der Variablen und zur Berechnung der Variable ‚Alter zur Tatzeit‘.

4.3 Ergebnisse und Hypothesenprüfung

4.3.1 Deskriptive Statistiken: Geschlecht

100 % ($N = 145$) der codierten FBI Most Wanted Hacker sind männlich. Es gab ein Gruppenfahndungsplakat, auf dem zwei Frauen als Teil einer Gruppe abgebildet waren. Gruppenfahndungen wurden jedoch ausgeschlossen, da hier keine Informationen zu Einzelpersonen enthalten sind (weder die Geburtsdaten noch, welche der Personen welche Delikte begangen haben). Das FBI hat einzeln nicht nach den Frauen gefahndet; ob diese selbst *Cybercrime im engeren Sinne* (Hacking) begangen haben oder nur mitwissend oder unterstützend waren, ist unklar.

H1: Hacker sind zu über 80 % männlich.

Die Hypothese kann bestätigt werden. Die Ergebnisse der quantitativen Inhaltsanalyse der Hackerprofile zeigen, dass 100 % der auf der Cyber Most Wanted Liste des FBIs aufgeführten Hacker ($N = 145$) männlich sind. Dieser Befund deckt sich mit bisherigen Studien zur Geschlechterverteilung in der *Cyberkriminalität im engeren Sinne*, die ebenfalls darauf hinweisen, dass Männer in diesem Bereich deutlich überproportional vertreten sind (BKA, 2015b).

4.3.2 Deskriptive Statistiken: Alter

Zu $n = 123$ Hackern konnte ein Alter zur Tatzeit bestimmt werden. Das Durchschnittsalter der Hacker beträgt $M = 30.65$ Jahre ($SD = 7.36$, $n = 123$). Bei $n = 83$ Hackern konnte das Tatalter direkt aus dem mittleren Tatzeitpunkt und Geburtsdatum berechnet werden, bei $n = 40$ Personen wurde das Tatalter indirekt aus dem Datum des Haftbefehls berechnet. Bei $n = 22$ Personen konnte kein Alter berechnet werden, da entweder das Geburtsdatum fehlte oder

Angaben zum Tatzeitpunkt oder Haftbefehl. Abbildung 12 zeigt die Häufigkeitsverteilung des berechneten Alters zur Tatzeit in absoluten Zahlen. Insgesamt zeigt sich eine annähernde Normalverteilung.

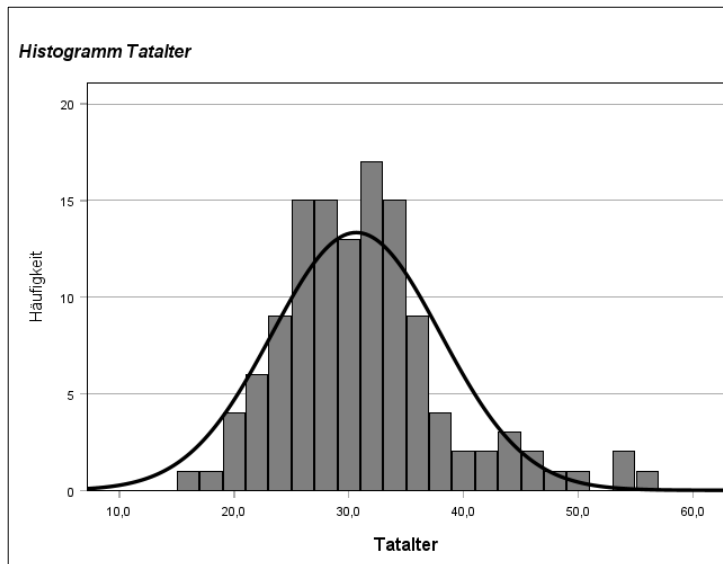


Abbildung 12. Histogramm: Alter der Hacker zur Tatzeit ($n = 123$)

Anmerkung. $M = 30.65$ Jahre ($SD = 7.36$ Jahre).

H2: Hacker sind zum Tatzeitpunkt eher jung (Durchschnitt, Modus, Median unter 30).

Die Hypothese kann teilweise bestätigt werden. FBI Most Wanted Hacker sind im Durchschnitt 31 Jahre alt ($M = 30.65$ Jahre, $SD = 7.36$, $n = 123$). Der Median liegt bei 29 Jahren. Es ist eine bimodale Verteilung mit den Modalwerten 29 und 31. In Übereinstimmung mit anderen Untersuchungen (z.B. BKA, 2015b, S. 8) ist festzuhalten, dass Hacker eher jung sind.

4.3.3 Deskriptive Statistiken: Nationalitäten, Nachrichtendienstzugehörigkeit, Belohnung

H3: Die Nationalitäten der FBI Cyber Most Wanted spiegeln die geopolitischen Konflikte und Kontrahenten der USA wider (vor allem Russland und China).

Die Hypothese kann bestätigt werden. Für $n = 138$ Hacker konnte die Nationalität codiert werden. Mit Abstand die meisten Hacker kamen aus Russland ($n = 39$), dem Iran ($n = 37$),

Nordkorea ($n = 18$) und China ($n = 15$). Diese vier Länder zusammen machten 75,17 % aus, also rund drei Viertel der erfassten Hackerprofile, und spiegeln deutlich geopolitische Spannungen der Vereinigten Staaten von Amerika wider. Abbildung 13 zeigt die codierten Nationalitäten in absoluten Zahlen, sortiert nach absteigender Häufigkeit.

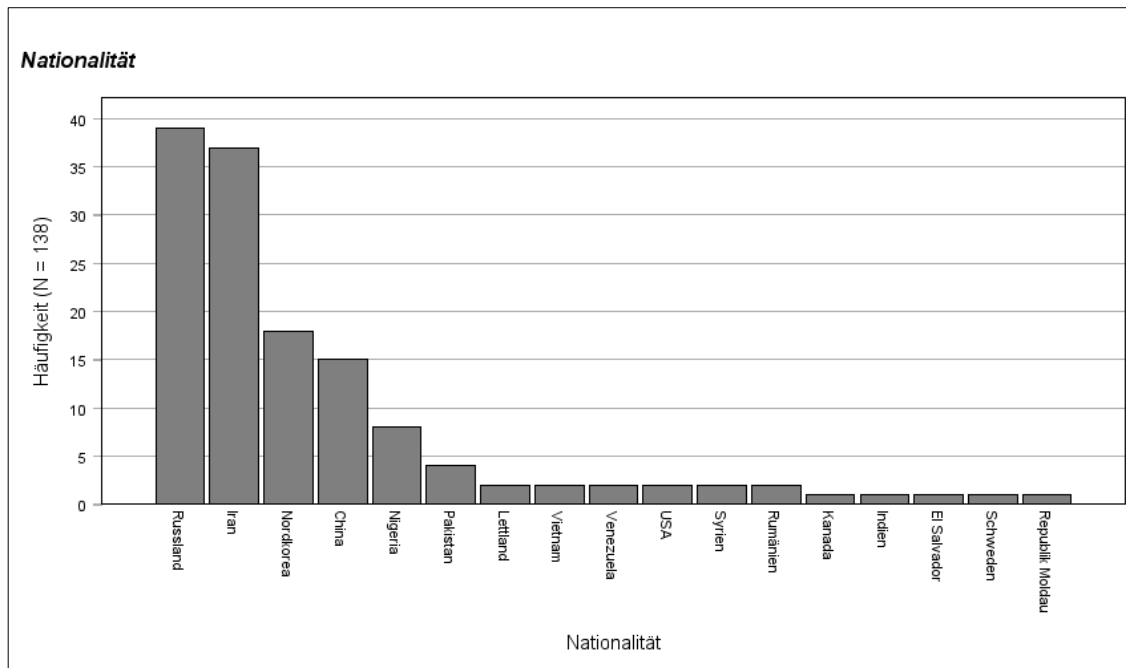


Abbildung 13. Deskriptive Statistik: Häufigkeiten der Nationalitäten ($n = 138$)

Während Russland, Iran, Nordkorea und China die häufigsten Nationalitäten waren, umfasst die Liste insgesamt 17 Nationalitäten. Acht Hacker kommen aus Nigeria, vier aus Pakistan, jeweils zwei Täter aus Lettland, Vietnam, Venezuela, USA, Syrien und Rumänien. Jeweils ein Täter kam aus Kanada, Indien, El Salvador, Schweden und der Republik Moldau.

H4: Mehr als ein Drittel der gesuchten Hacker haben eine direkte oder indirekte Verbindung zu Nachrichtendiensten.

Die Hypothese kann bestätigt werden. 58,6 % der Hacker haben eine Nachrichtendienstzugehörigkeit. Betrachtet man lediglich diese Gruppe der staatlichen Akteure ($n = 85$), kommen diese fast ausschließlich aus Russland, dem Iran, Nordkorea und China (und zwei Hacker aus Syrien). Abbildung 14 zeigt prozentuale Häufigkeiten der Nationalitäten in der Gruppe der staatlichen Akteure.

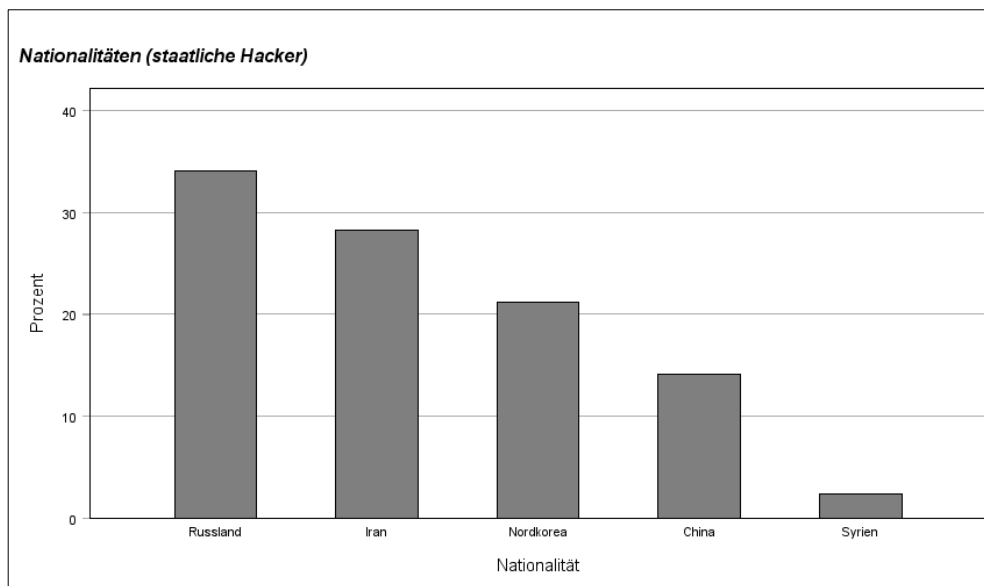


Abbildung 14. Deskriptive Statistik: Nationalitäten staatlicher Hacker ($n = 85$)

Dass viele Hacker mit Geheimdienstverbindung aus den vier genannten Staaten stammen, bedeutet nicht, dass auch die Mehrheit der Hacker aus diesen Staaten eine solche Verbindung hat. Daher wurde der Zusammenhang auch in entgegengesetzter Richtung untersucht: Wie hoch ist der Prozentsatz der Personen mit staatlichen Verbindungen innerhalb der Nationalitätsgruppen?

Tabelle 5 zeigt als Kreuztabelle den prozentualen Anteil der Personen mit Nachrichtendienstzugehörigkeit nach Nationalitäten. 80 % der Hacker aus China hatten staatliche Verbindungen, rund 65 % der iranischen Hacker, 74,4 % der russischen Hacker und 100 % der nordkoreanischen Hacker hatten staatliche Verbindungen zu Nachrichtendienst oder Militäreinheiten. Bei der Nationalität ‚Syrien‘ war die Fallzahl lediglich zwei, aber auch hier hatten beide Hacker eine Verbindung zu staatlichen Institutionen, Militär oder Geheimdienst.

Tabelle 5: Kreuztabelle Nachrichtendienstzugehörigkeit x Nationalität

Nationalität	n	n (Personen mit Nachrichtendienst- Verbindung)	% (von Nationalität)
China	15	12	80,0 %
Iran	37	24	64,9 %
Nordkorea	18	18	100 %
Russland	39	29	74,4 %
Syrien	2	2	100 %

Die Hypothesen H3 und H4 können bestätigt werden. Insgesamt und insbesondere bei den staatlichen Akteuren sind die ‚Top 4‘ der Angriffsländer (aus westlicher/ US-amerikanischer Sicht) eindeutig: Russland, Iran, Nordkorea und China.

H5: Vor allem bei Tätern, die eine Verbindung zu anderen Nachrichtendiensten haben, ist der Fahndungsdruck groß und es werden Belohnungen über eine Million USD angesetzt.

Die Hypothese kann bestätigt werden. Dass Cybercrime als Bedrohung für kritische Infrastruktur, Unternehmen und Wahlen ernst genommen wird, zeigen die hohen Belohnungen von bis zu 10 Mio. US-Dollar für Hinweise zu den gesuchten Akteuren. Die Tatsache, dass die Täter zum Teil mit Namen, Bild und Geburtsdatum öffentlich bekannt sind, aber über Jahrzehnte trotzdem nicht von den USA gefasst werden können, zeigt, wie schwierig die Strafverfolgung in diesem globalen Konfliktfeld ist. In $n = 99$ Fällen (68,3 %) nannte das FBI keine Belohnung, während in $n = 46$ Fällen (31,7 %) eine Belohnung angegeben wurde.

Abbildung 15 zeigt alle Fälle, in denen eine Belohnung genannt wurde ($n = 46$), und stellt die Beträge in USD (X-Achse) und prozentualen Häufigkeiten (Y-Achse) dar.

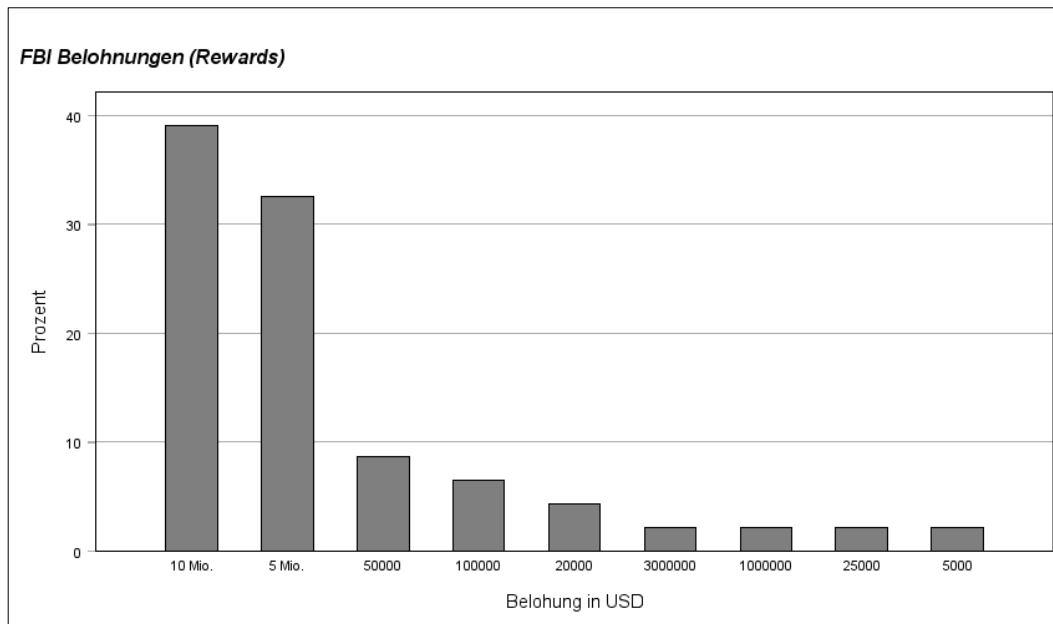


Abbildung 15. Deskriptive Statistik: Häufigkeiten der FBI-Belohnungen ($n = 46$)

Nur in der Minderheit der Fälle wird eine Belohnung genannt, *wenn* aber eine Belohnung genannt wird, liegt diese häufig im Bereich von Millionenbeträgen.

Bei Hackern mit Nachrichtendienstzugehörigkeit wurde in 31,8 % der Fälle eine Belohnung genannt, und die durchschnittliche Höhe der Belohnung bei staatlichen Akteuren liegt bei 6.67 Mio. USD. Bei Hackern ohne Nachrichtendienstzugehörigkeit wurde ebenfalls in rund 31,7 % der Fälle eine Belohnung genannt, aber in durchschnittlicher Höhe von nur 4.18 Mio. USD. Der Fahndungsdruck ist insgesamt hoch, besonders bei staatlichen Akteuren, wobei die Höhe der Belohnung als Indikator für die Relevanz und den Fahndungsdruck interpretiert werden kann.

4.4 Diskussion

4.4.1 Zusammenfassung und Bewertung der zentralen Befunde

Basierend auf der quantitativen Inhaltsanalyse der Fahndungsplakate lässt sich zusammenfassen, dass ein typischer FBI Most Wanted Hacker im Durchschnitt 31 Jahre alt und männlich ist. Rund drei Viertel kommen aus Russland, dem Iran, Nordkorea und China und haben zu 59 % direkte oder indirekte Verbindung zu staatlichen Organen, wie Nachrichtendienst oder Militäreinheiten. Gerade die Nationalitäten der Angreifer spiegeln die

geopolitischen Kontrahenten der USA wider und sind daher nicht allgemeingültig. Ebenfalls ist einschränkend anzumerken, dass die USA nicht nur passives Ziel von Cyberangriffen sind, sondern selbst aktiver Akteur. Der Fahndungsdruck ist hoch und die ausgelobten Belohnungen des FBIs für Hinweise betragen bis zu 10 Millionen USD. Auf Osama bin Laden wurden damals 25 Mio. USD Belohnung ausgesetzt (FBI, 2025b); dass für zahlreiche Hacker 10 Mio. USD ausgelobt werden, zeigt die Relevanz von Cybercrime und dass Cybercrime eine ernstzunehmende Bedrohung für die nationale Sicherheit sein kann.

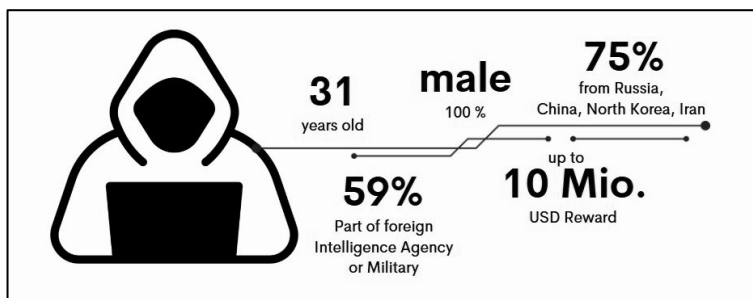


Abbildung 16. Durchschnittliches Profil eines typischen FBI Most Wanted Hackers

Quelle: Eigene Darstellung.⁵

Damit konnten die meisten Hypothesen und der bisherige Forschungsstand bestätigt werden: Dass Hacker überwiegend männlich sind, deckt sich mit vorherigen empirischen Befunden. Chiesa et al. (2009, S. 74) führten das bisher umfassendste Hacker Profiling Project durch und kamen bei $N = 567$ befragten Hackern auf 94 % Männer. Vick & Roters (2003, S. 10) berichten ebenfalls 94 % männliche Hacker bei ihrer Untersuchung zu Accountmissbrauchstätern und einem Sample von $N = 599$. Wie in Kapitel 3.3 aufgeführt, berichtet auch eine Meta-Analyse des BKAs (2015b) 76-94 % Männeranteil.

Der sehr hohe Männeranteil könnte damit begründet werden, dass sich hier zwei Phänomene überlagern. Zum einen spiegelt diese Verteilung strukturelle Gegebenheiten der IT-Branche wider, in der Männer traditionell dominieren. Der Geschlechterunterschied zeigt sich schon in der Auswahl technologischer Studienfächer (z.B. Zhang, Gros & Mao, 2021). Zum anderen

⁵ Zur Grafikerstellung wurden die KI-Software Canva und Microsoft Powerpoint als Hilfsmittel eingesetzt.

sind Männer in fast allen Kriminalitätsbereichen überrepräsentiert; so waren z.B. 82 % aller verurteilten Personen im Jahr 2023 Männer (Statista, 2025a).

Bisherige empirische Forschung fand zwar einen sehr hohen Männeranteil, doch die vollständige Abwesenheit von Hackerinnen auf der FBI Cyber Most Wanted Liste scheint erklärungsbedürftig. Steffensmeier & Allan (1996) haben in einer der Standardpublikationen zu Geschlecht und Kriminalität festgehalten: „Criminologists agree that the gender gap in crime is universal“ (S. 459). Die Autoren heben jedoch hervor, dass der Männeranteil in extremen Deliktsbereichen noch größer ist: „This gender gap in crime is greatest for serious crime and least for mild forms of lawbreaking“ (S. 460). Bei den FBI Most Wanted Hackern handelt es sich nicht um den durchschnittlichen, gewöhnlichen Black Hat Hacker, sondern um eine extreme Stichprobe, worin der Grund für den noch größeren Männeranteil liegen könnte. Ob der Frauenanteil auf anderen Ebenen höher liegt, kann auf Basis der erfassten Daten nicht beantwortet werden.

Die Überrepräsentanz von Männern in der Cyberkriminalität kann teilweise durch geschlechtsspezifische Sozialisation erklärt werden, die Männer häufiger zu technisch riskanten und wettbewerbsorientierten Aktivitäten ermutigt (z.B. Holt, Burruss & Bossler, 2010).

Doch insbesondere, wenn man geschlechtsspezifische Sozialisation als Hauptargument für die Geschlechterunterschiede anführt, müsste dies sich im Zeitverlauf wandeln. 30 % Frauenanteil in technischen Berufen ist zwar immer noch verhältnismäßig wenig, aber hat sich im Zeitverlauf bereits geändert. 30 % Frauenanteil sind weit mehr als 0 %, wie bei den Most Wanted Hackern. Chiesa et al. postulierten daher bereits 2009 (S. 90), dass es in Zukunft mehr Frauen im Hacking geben wird. Zumindest innerhalb der FBI Most Wanted Hacker bis 2024 ist dieser Trend nicht erkennbar.

Gleichzeitig bleibt die Frage offen, ob Frauen in der Cyberkriminalität oder grundsätzlich in der Kriminalität tatsächlich seltener aktiv sind oder ob sie nur seltener identifiziert und verfolgt werden. Weniger riskante Taten und Vorsichtsmaßnahmen könnten die

Strafverfolgungswahrscheinlichkeit senken. Vielleicht planen Hackerinnen ihre Taten besser oder wählen weniger risikoreiche Angriffsziele.

Zukünftige Forschung sollte auch untersuchen, inwieweit Frauen in Cyberkriminalität involviert sind und die Praxis und Selektion der Strafverfolgungsorgane ihre Sichtbarkeit beeinflusst.

Auch das recht junge Alter von Hackern deckt sich mit bisherigen Erkenntnissen zu den Profilen von Hackern. Chiesa et al. (2009, S. 74) berichten ein Durchschnittsalter von 25 Jahren bei männlichen Hackern und weisen darauf hin, dass 61 % mit dem Hacking zwischen 10-15 Jahren begonnen haben. Auch die Meta-Analyse des BKAs (2015b, S. 8) resümiert, dass „von einer in hohem Maße jungen Hackerpopulation auszugehen“ ist. In den meisten Untersuchungen ist das Durchschnittsalter im Bereich von 25 Jahren (BKA, 2015b). In der durchgeführten Inhaltsanalyse konnte ein Durchschnittsalter von 31 Jahren ermittelt werden, d.h., FBI Most Wanted Hacker sind etwas älter als der durchschnittliche Black Hat Hacker. Da es sich jedoch innerhalb der FBI Cyber Most Wanted um extreme und fortgeschrittene Cyberangriffe handelt, ist durchaus davon auszugehen, dass Täter bereits weit vorher aktiv waren und schon in jungen Jahren ihre Fähigkeiten erworben haben.

Einer der codierten Fälle war z.B. Guang T., geboren 1994, dem es im Alter von 26 Jahren gelang, 81.000 Firewalls zu hacken. Wenn er im Alter von 26 Jahren bereits die Fähigkeiten hatte, Hacking in dieser Dimension auszuführen und damit zu den meistgesuchten Hackern des FBIs zu werden, ist davon auszugehen, dass auch er in jungen Jahren das Hacking gelernt hat und dies nicht seine erste Tat war. Dass die (sehr fortgeschrittenen) Hacker auf der Cyber Most Wanted Liste im Schnitt etwas älter sind als der durchschnittliche Black Hat Hacker, ist demnach plausibel.

In der Literatur gibt es verschiedene Erklärungen für das junge Alter von Hackern. Aiken, Davidson, Walrave, Ponnet, Phillips & Farr nennen das „typical adolescent risk-taking“ (2024, S. 24) als Faktor, der Cyberkriminalität begünstigen kann, also die Entwicklungsphase des „Storm and Stress“ (Aiken et al., 2016, S. 9) als Erklärung für das junge Alter von Hackern.

Zusammenfassend lässt sich festhalten, dass der Forschungsstand, dass Hacker jung und männlich sind, bestätigt werden konnte. Da es sich bei den FBI Most Wanted Hackern um eine extreme Stichprobe handelt, war der Männeranteil noch größer (100 %) und das Durchschnittsalter etwas höher ($M = 31$).

Die FBI Most Wanted Hacker unterscheiden sich jedoch deutlich von ‚gewöhnlichen Hackern‘ hinsichtlich der Nationalitäten und Zugehörigkeit zu Nachrichtendiensten. Gewöhnliche Accountmissbrauchstaten oder Identitätsdiebstahl in sozialen Netzwerken, wie sie sich täglich tausendfach ereignen, liegen unterhalb der Relevanzschwelle, um es auf die Liste der meistgesuchten Hacker des FBIs zu schaffen. Hier liegt der Fokus primär auf staatlichen Akteuren, Aktivitäten anderer Nachrichtendienste, Spionage, Wahlbeeinflussung und Bedrohungen für die nationale Sicherheit der USA. Chiesa et al. (2009) fanden in ihrer Untersuchung: „there are hackers of all nationalities and ethnic groups“ (S. 91). Innerhalb der FBI Cyber Most Wanted sind die Nationalitäten deutlich weniger divers. Dreiviertel der meistgesuchten Hacker kamen aus nur vier Ländern: Russland, Iran, Nordkorea und China. Dies deckt sich mit dem Forschungsstand und aktuellen Bedrohungsanalysen. Katagiri (2024) untersuchte 112 APT-Gruppierungen (*Advanced Persistent Threats*)⁶, die für ihre Verbindung zu Staaten bekannt sind, und identifizierte ebenfalls Russland, China, Nordkorea und den Iran als die Hauptgefahren und nennt diese Länder daher die „Big 4“ (S. 280).

Die *Big 4* geopolitischen Gefahren konnten anhand der Inhaltsanalyse eindeutig bestätigt werden, insbesondere bei den staatlichen Akteuren. Die Nachrichtendienste der USA haben 2019 einen Bericht zum *Worldwide Threat Assessment* veröffentlicht, in dem ebenfalls die *Big 4 Threats* explizit genannt werden, sowie deren geopolitische Interessen: „China, Russia, Iran, and North Korea „increasingly use cyber operations to threaten both minds and machines in an expanding number of ways - to steal information, to influence our citizens, or to disrupt critical infrastructure“ (Coats, 2019, S. 5).

⁶ Beschreibt fortgeschrittene Akteure, die häufig durch Geheimdienste direkt oder indirekt unterstützt werden und Cyberkriminalität als Werkzeug zur Durchsetzung nationaler Interessen nutzen.

Während Russland, China und der Iran Cyberspionage und Cybersabotage einsetzen, um ihre militärischen, politischen und wirtschaftlichen Ziele zu verfolgen (Coats, 2019), finanziere sich Nordkorea nach Coats (2019) u.a. auch durch Cyberkriminalität.

4.4.2 Methodische Reflexion

Durch die standardisierte, quantitative Inhaltsanalyse non-reaktiver Fahndungsplakate war eine Auswertung der demografischen Merkmale dieser spezifischen Gruppe von Black Hat Hackern möglich. Die Repräsentativität und Übertragbarkeit auf die Grundgesamtheit aller Black Hat Hacker ist allerdings eingeschränkt, da es sich *erstens* um eine extreme Stichprobe handelt und *zweitens* ausschließlich eine US-Perspektive darstellt, die ebenfalls kritisch gesehen werden kann. Die hier codierten Black Hat Hacker haben tendenziell schwerwiegendere und technisch komplexere Cyberstraftaten gegen die nationale Sicherheit der USA begangen und weisen wahrscheinlich auch deshalb ein höheres Durchschnittsalter auf und stehen überdurchschnittlich oft mit Nachrichtendiensten geopolitischer Kontrahenten der USA in Verbindung. Im Gegensatz dazu sind durchschnittliche Black Hats wahrscheinlich oft jünger, agieren öfter allein oder in kleinen Gruppen und verüben weniger schwerwiegende und komplexe Cyberdelikte.

Eine besondere Stärke der Untersuchung liegt in der Non-Reaktivität des Untersuchungsgegenstandes. Die analysierten Daten basieren auf behördlich verifizierten Informationen, welche im Rahmen offizieller Fahndungen erhoben wurden. Dies unterscheidet sie von anonymen Darknet-Recherchen, bei denen die Validität und Verifizierbarkeit von demografischen Angaben problematisch ist. In der Stärke, dass Fahndungsplakate non-reaktiv und formell sind, liegt auch die Limitation der Studie. Aspekte wie die psychologischen Dispositionen, individuellen motivationalen Faktoren oder Einstellungen der gesuchten Hacker können anhand der inhaltsanalytischen Erfassung von Fahndungsplakaten nicht erfasst werden. Besonders tiefgehende psychologische Analysen, etwa zu Motiven oder subklinischen Merkmalen der Dunklen Triade (Narzissmus,

Machiavellismus, Psychopathie), bleiben somit unberücksichtigt. Die zweite Studie (Online-Befragung von Hackern) soll daher genau diese Aspekte beleuchten.

5 Studie 2: Online-Befragung zur Dunklen Triade und Motiven von Hackern

5.1 Zielsetzung und Forschungsfragen

Während die erste Studie darauf abzielte, ein demografisches Profil von Black Hat Hackern zu erstellen in Bezug auf Geschlecht, Alter und Nationalität, ist es das Ziel der zweiten Studie, innere Zustände wie Motive, Persönlichkeitsmerkmale und Einstellungen zu erfassen. Für diesen Anwendungsfall stellen empirische, standardisierte Online-Befragungen eine geeignete Methode dar, da sie auf die Erforschung innerer Zustände abzielen, die äußerlich weder messbar noch beobachtbar wären. Nach Möhring & Schlütz (2013) seien Befragungen daher eine geeignete Methode, „um miteinander vergleichbare subjektive Bewertungen, Beurteilungen, Einstellungen und Interpretationen eines Untersuchungsgegenstandes zu ermitteln. Die Befragung ist das einzig sinnvolle Verfahren zur Ermittlung von Meinungen, Wissen und Wertvorstellungen“ (S. 185). Da das Ziel der Studie darin besteht, White- und Black Hats hinsichtlich Persönlichkeitsdispositionen der Dunklen Triade, Motiven, Moralvorstellungen und Einstellungen zu vergleichen, wurde die Befragung als geeignete Methode ausgewählt. Über eine gezielte Videokampagne sollen Black Hat- und White Hat Hacker über Darknet-Foren, Reddit-Hacker-Foren, Telegram-Gruppen und präzises Targeting rekrutiert und anschließend in sechs übergeordneten Themenbereichen verglichen und beschrieben werden:

- (1) Profile und Motive
- (2) Merkmale der Dunklen Triade (Psychopathie, Narzissmus, Machiavellismus)
- (3) Quelle der Hackingfähigkeiten (Kontext: Lerntheorien)
- (4) Enthemmungsfaktoren des Cyberspace (Kontext: White Gloves Theorie)
- (5) Korrelationen zwischen Angriffsarten, Motiven und Triademerkmale (Kontext: Profiling)
- (6) Nutzung von Künstlicher Intelligenz für das Hacking (Kontext: Zukunftsrelevanz)

Die Gütekriterien der Befragung sind Validität, Reliabilität und Objektivität (Möhring & Schlütz, 2013, S. 189). Gerade bei der Erfassung der Dunklen Triade soll auf etablierte Skalen mit bekannter Validität und Reliabilität zurückgegriffen werden und die Objektivität durch transparente Darstellung aller methodischen Schritte und Entscheidungen sichergestellt werden.

Da über Black Hat Hacker außerhalb des Strafvollzugs bislang kaum empirisches Wissen existiert, stellt diese Studie einen der ersten systematischen Versuche dar, mit aktiven Black Hats (u.a. im Darknet) in direkten Kontakt zu treten und damit ein besonders schwer zugängliches Forschungsfeld überhaupt empirisch zu erschließen. Aufgrund der Tatsache, dass insbesondere Black Hats ihre Anonymität schützen und potentiell aus allen Teilen der Welt kommen, sind persönliche Treffen und Telefonate in großer, repräsentativer Fallzahl nicht praktikabel. Gerade bei Black Hats außerhalb des Strafvollzugssystems, die international verteilt leben und ihren Wohnort aus Gründen der OpSec geheim halten, ist das Format einer Online-Befragung angemessen und wahrscheinlich auch der einzig praktikable Zugang, da Online-Befragungen (verglichen mit Telefonaten oder Face-to-Face-Interaktionen) die höchste Anonymität bieten und ortsunabhängig sind. Doch wie jede andere Methode, hat auch die Online-Befragung Vor- und Nachteile, welche Taddicken (2013, S. 208, Tabelle 1) tabellarisch gegenüberstellt, wobei die Vorteile der Methodik primär in der Zeit- und Kosteneffizienz liegen und der wesentliche Nachteil darin besteht, dass bei Online-Befragungen kein Interviewer anwesend ist und somit keine Kontrolle der Umgebung oder Situation möglich ist. Die Haupthypothese der Arbeit ist, dass sich Black- und White Hats signifikant in Bezug auf die Dunkle Triade (*traits*) voneinander unterscheiden könnten. Für die eingesetzten Skalen liegen etablierte Cut-off-Werte und Normdaten der Allgemeinbevölkerung als Referenzwerte vor, ab wann beispielsweise von auffälliger Psychopathie oder einer potenziell psychopathischen Gruppe gesprochen werden kann. Von Interesse ist also nicht nur der direkte Vergleich zwischen Black- und White Hats, sondern auch der Bezug zu den Normwerten der Allgemeinbevölkerung.

F1: Inwiefern unterscheiden sich Black Hat- und White Hat Hacker hinsichtlich Persönlichkeitseigenschaften der Dunklen Triade (Psychopathie, Narzissmus, Machiavellismus) voneinander und von der Allgemeinbevölkerung?

Psychopathie ist das komplexeste der drei Konstrukte und wird im Sinne eines „mehrdimensionale[n] Persönlichkeitskonzeptes“ (Schütte & Blickle, 2017, S. 93) gesehen, weshalb eine Differenzierung von primärer- und sekundärer Psychopathie sinnvoll ist.

F2: Inwiefern unterscheiden sich Black Hat Hacker und White Hat Hacker hinsichtlich primärer und sekundärer Psychopathie voneinander und von der Allgemeinbevölkerung?

Die genannten Forschungsfragen F1 und F2 beziehen sich auf Merkmale der Dunklen Triade, insbesondere Psychopathie. Sind Black Hat Hacker schlicht psychopathischer und machiavellistischer als White Hat Hacker? Im Sinne der kriminologischen Theorien (siehe Kapitel 3.4.1) wäre dies den *individuellen Theorien* zuzuordnen, d.h. die Erklärung für Cyberkriminalität läge in diesem Fall primär in Unterschieden der Persönlichkeit (*traits*). Im Theorieteil wurden jedoch auch alternative Ursachen oder verstärkende Faktoren für Cyberkriminalität genannt, z.B. Lerntheorien und Subkulturtheorien. Möglicherweise lernen White Hats ihre Hackingfähigkeiten öfter im formellen, legalen Rahmen (z.B. universitäres Informatikstudium), während Black Hat Hacker es öfter im informellen Selbststudium (z.B. in Darknet-Foren) lernen. Deshalb soll empirisch auch die Quelle der Hackingfähigkeiten erfasst werden, um mögliche Unterschiede zwischen Black Hats und White Hats zu identifizieren im Kontext von Lerntheorien.

F3: Bestehen Unterschiede in der Frage, wo und wie Black Hat Hacker und White Hat Hacker ihre Fähigkeiten erlernt haben?

Außerdem wurden in Kapitel 3.4.2 und 3.4.3 der Online Disinhibition Effect und die White Gloves Theorie vorgestellt. Möglicherweise gibt es enthemmende Eigenschaften des Cyberraums, die Cyberkriminalität begünstigen. Auch diese Aspekte sollen durch einige Items im Fragebogen erfasst werden.

F4: Begünstigt die Anonymität des Internets enthemmtes Verhalten von Black Hat und White Hat Hackern? (Online Disinhibition Effect)

F5: Wie schätzen Black Hat Hacker und White Hat Hacker das Entdeckungsrisiko ein?

F6: Welche Rolle spielt Schuldexternalisierung („Opfer sind selbst schuld“) als moralische Rechtfertigung bei Black Hat Hackern und White Hat Hackern?

Außerdem sind die Motive von Black Hat Hackern und mögliche Zusammenhänge mit der Dunklen Triade von Interesse. Da sich dieser Themenblock ausschließlich auf Motive für *kriminelles* Hacking bezieht, soll dies nur in der Gruppe der Black Hats erfasst und deskriptiv analysiert werden. Die Verbindung von Motiven und Persönlichkeitsmerkmalen zu untersuchen, ist ebenfalls im Kontext des Cyberprofilings von Interesse, z.B., ob Narzissmus mit dem Motiv nach Anerkennung korreliert.

F7: Welche Motive treiben Black Hat Hacker an und wie hängen sie mit Persönlichkeitsmerkmalen der Dunklen Triade zusammen?

Besonders relevant für die Strafverfolgungsbehörden und Kriminalistik ist auch die Frage nach Zusammenhängen zwischen der Art des Angriffs (dem Modus Operandi einer Tat) und Persönlichkeitsdispositionen der Täter. Denn nur, wenn die Persönlichkeit einen Einfluss auf die Tatausführung hat, lässt sich im Umkehrschluss aus der Tatausführung etwas über die Persönlichkeit ableiten (Musolf, 2002). Dies ist die Grundvoraussetzung für jegliches Profiling (siehe Kapitel 3.2).

F8: Gibt es Korrelationen zwischen Eigenschaften der Dunklen Triade und bevorzugten Angriffsmethoden (Technische Hacks vs. Social Engineering) und ist damit Cyberprofiling grundsätzlich realisierbar?

Das Bundeskriminalamt erwähnt bereits im Bundeslagebild Cybercrime 2023, dass künstliche Intelligenz in Zukunft dafür sorgen könnte, dass auch Personen ohne

Hackingfähigkeiten KI-gestützte Cyberangriffe ausführen könnten (BKA, 2024, S. 24). Dies würde die intellektuelle Einstiegshürde senken und den Kreis möglicher Täter maßgeblich vergrößern und wäre somit ein bedeutsamer Treiber künftiger Veränderungen. Daher soll ebenfalls mit einer Frage erfasst werden, ob Black Hat Hacker und White Hat Hacker bereits KI für Hacking-Aktivitäten einsetzen.

F9: Nutzen Black Hat Hacker bereits künstliche Intelligenz für Cyberangriffe?

Abbildung 17 zeigt in der Übersicht die Variablen, welche Zusammenhänge untersucht werden sollen und welche Forschungsfragen sich auf welche Zusammenhänge beziehen.

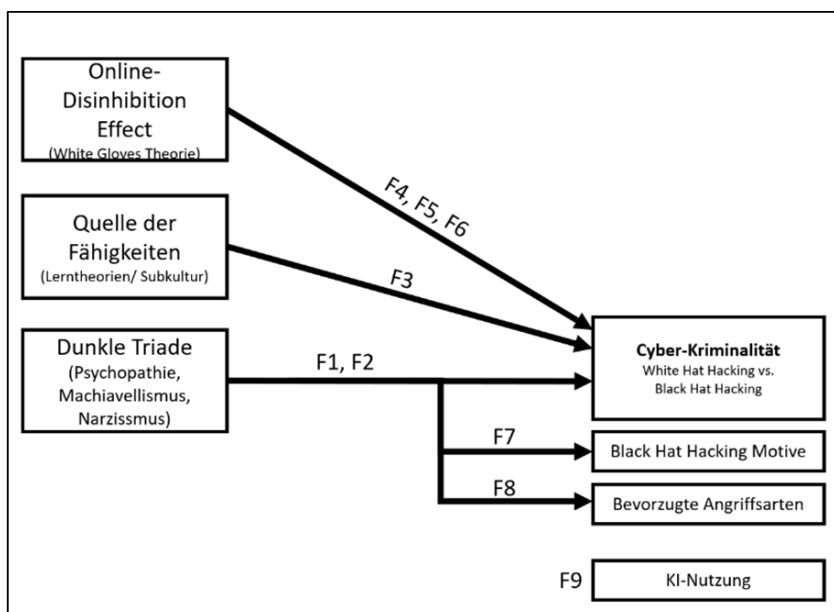


Abbildung 17. Übersicht der Variablen und Forschungsfragen

Anmerkung. Es wird kausallogisch angenommen, dass Persönlichkeitsmerkmale (insbesondere die Dunkle Triade) das Hacking-Verhalten (White-Hat vs. Black-Hat) beeinflussen. Im Rahmen der vorliegenden empirischen Untersuchung erfolgt die Analyse jedoch statistisch primär über einen Gruppenvergleich (t -Tests), bei dem die Gruppenzugehörigkeit (Black Hat / White Hat) als uV modelliert wird, während die Ausprägungen der Dunklen Triade sowie weiterer Variablen als abhängige Variablen gemessen werden.

5.2 Herleitung der Hypothesen

Die Eigenschaften der Dunklen Triade zeigen positive Zusammenhänge mit nahezu allen Formen destruktiven Verhaltens, von Gewaltkriminalität über Fremdgehen bis zu

Cyberaggression (Schwarzinger, 2020, S. 57, siehe zur Übersicht Kapitel 3.1.1 und 3.1.2). Das gilt besonders für Psychopathie und Machiavellismus (Furtner, 2017, S. 7). Erste Ergebnisse von Gaia et al. (2021) deuten darauf hin, dass Psychopathie und Machiavellismus positive Zusammenhänge mit Black Hat Hacking zeigen könnten. In Bezug auf Psychopathie und Machiavellismus ist daher anzunehmen, dass Black Hats hier signifikant höhere Ausprägungen zeigen als White Hats. Die Psychopathie- und Machiavellismus-Scores sollen nicht nur zwischen Black- und White Hats verglichen werden, sondern auch mit Referenzwerten der Allgemeinbevölkerung aus der Literatur in Beziehung gesetzt werden. Hier ist anzunehmen, dass kriminelle Hacker signifikant von den Normwerten abweichen, während White Hats unauffällig sind.

H1: Black Hat Hacker sind signifikant psychopathischer als White Hat Hacker.

H2: Black Hat Hacker sind signifikant psychopathischer als die Allgemeinbevölkerung, während White Hat Hacker unauffällig sind.

H3: Black Hat Hacker sind signifikant machiavellistischer als White Hat Hacker.

H4: Black Hat Hacker sind signifikant machiavellistischer als die Allgemeinbevölkerung, während White Hat Hacker unauffällig sind.

Während Psychopathie und Machiavellismus eindeutig ‚dunkle‘ Persönlichkeitsfacetten widerspiegeln, sind die empirischen Befunde bei Narzissmus diverser (Furtner, 2017, S. 6). In Bezug auf Narzissmus ist anzunehmen, dass die Unterschiede zwischen den Hackergruppen geringer sind. Gaia et al. (2021) weisen darauf hin, dass Narzissmus auch bei White Hat Hacking eine Rolle spielen könnte (S. 23). Da es Narzissten um Anerkennung und Bewunderung geht, ergibt es Sinn, dass dies auch bei White Hat Hackern ausgeprägt sein könnte. Black Hat Hacker können Ruhm oder Status lediglich in Hacker-Foren hinter einem pseudonymen Nutzernamen genießen, es aber meist nicht mit ihrer echten Identität verknüpfen oder vor Familie und Freunden mit ihren Fähigkeiten prahlen. Wenn Anerkennung das Hauptmotiv ist, könnte eine Karriere als Sicherheitsforscher, Penetrationstester oder

ethischer Hacker (also White Hat Hacker) interessanter sein. Daher lauten die Hypothesen 5-6:

H5: Zwischen Black Hat Hackern und White Hat Hackern bestehen keine signifikanten Unterschiede im Narzissmus.

H6: Black Hat Hacker und White Hat Hacker sind signifikant narzisstischer als die Allgemeinbevölkerung.

Die drei Konstrukte der Dunklen Triade unterscheiden sich in ihrer prädiktiven Stärke und Stärke der Korrelationen mit destruktivem Verhalten. In den meisten empirischen Untersuchungen zeigte sich eine Rangfolge in Bezug auf Destruktivität, wobei Psychopathie die stärksten Korrelationen mit destruktivem Verhalten zeigt, gefolgt von Machiavellismus, und Narzissmus zeigt die schwächsten Zusammenhänge (z.B. Duradoni et al., 2023). Deshalb „zählt Narzissmus zur hellsten und positivsten Dimension, während Psychopathie am wenigsten adaptiv und sozial akzeptiert ist“ (Furtner, 2017, S. 6). Es ist daher zu erwarten, dass die Gruppenunterschiede zwischen Black Hats und White Hats bei den drei Merkmalen der Dunklen Triade unterschiedlich groß sind:

H7: Das kriminelle Hacking (Black Hat Hacking) ist am stärksten mit Psychopathie und Machiavellismus verbunden und am schwächsten mit Narzissmus, sowohl in Gruppenvergleichen, Korrelationen als auch in Vorhersagemodellen.

Heutige Konzeptionalisierungen betrachten Psychopathie als ein Konstrukt mit (mindestens) zwei Faktoren und unterscheiden daher meist die Subskalen der primären und sekundären Psychopathie. Diese Unterscheidung wurde erstmals durch Karpman (1941) eingeführt und durch Lykken (1995) etabliert. Primäre Psychopathie beschreibe nach Lykken (1995, S. 133-155) dabei eher die furchtlose Seite von Psychopathie, während sekundäre Psychopathie eher den impulsiven Charakter und auch Defizite in der Selbstbeherrschung ausdrücke (S. 130).

Da Hacking eine hohe intellektuelle Einstiegshürde hat, planvolles Handeln und geschickte Manipulation voraussetzt (Social Engineering) und emotionale Überreaktionen zu Fehlern in der eigenen Operational Security der Täter führen können, ist davon auszugehen, dass Black Hat Hacker eher ‚planvolle Strategen‘ sind und höhere Scores bei primärer Psychopathie aufweisen.

H8: Black Hat Hacker sind signifikant psychopathischer als White Hat Hacker in Bezug auf primäre & sekundäre Psychopathie.

H9: Primäre Psychopathie (planvolles, empathieloses Handeln) ist bei Black Hats stärker ausgeprägt als sekundäre Psychopathie (Impulsivität, Aggression).

H10: Black Hat Hacker sind signifikant psychopathischer als die Allgemeinbevölkerung in Bezug auf primäre und sekundäre Psychopathie, während White Hat Hacker unauffällig sind.

In Kapitel 3.4.5 wurden Subkulturtheorien, Lerntheorien und operante Konditionierung in Bezug auf Cyberkriminalität erläutert. Diese Theorien basieren auf dem Gedanken, dass Kriminalität auch gelerntes Verhalten sein kann. Im Sinne der Theorie wäre anzunehmen, dass White Hat Hacker ihre Fähigkeiten öfter aus legitimen, formellen Quellen erworben haben, z.B. im Informatikstudium, während Black Hat Hacker es öfter im Darknet gelernt haben und sich somit früh in einem Lernumfeld bzw. einer Subkultur befanden, in dem Cyberkriminalität die akzeptierte Norm ist.

H11: White Hat Hacker haben ihre Fähigkeiten häufiger durch formelle Bildungsquellen (z. B. Universität) erworben, während Black Hat Hacker diese häufiger über informelle Quellen (z.B. Darknet) erlernt haben.

In den Kapiteln 3.4.2 und 3.4.3 wurde der Online Disinhibition Effect beschrieben und die White Gloves Theorie. Diese Theorien und Hypothesen fokussieren sich auf Merkmale des Cyberspace und inwiefern dies zur Enthemmung oder zu destruktivem Verhalten beitragen kann (z.B. Suler, 2004). Diese Ansätze suchen nach Ursachen für Kriminalität nicht in der Persönlichkeit, sondern in Kontextfaktoren. Opfer sehen ihre Täter in der digitalen Sphäre

nicht und Täter sehen ihre Opfer nicht. Moralische Aspekte oder Gewissen lassen sich so ggf. leichter ausblenden oder die Schuld externalisieren (z.B., wer ein schwaches Passwort hat, sei selbst schuld, gehackt zu werden). Auch die geringe Aufklärungsquote und Entdeckungswahrscheinlichkeit könnte zur Wahrnehmung eines straffreien, rechtsfreien Raumes führen (Hoheisel-Gruler, 2020). Auf dem Grundgedanken, dass Menschen sich online anders verhalten, als sie es in der Realität tun würden, basiert der cyberkriminologische Erklärungsansatz der White Gloves Theorie (Acker, 2023). Nach Acker (2023) enthemmt der Cyberspace derart, dass Menschen unterschiedliche moralische Leitlinien haben könnten, abhängig davon, ob sie online oder offline agieren. Basierend auf dem Online Disinhibition Effect und der White Gloves Theorie sind die Hypothesen 12-14:

H12: Die Anonymität des Internets führt zu einer Enthemmung im Online-Verhalten bei Black Hat- und White Hat Hackern.

H13: Black Hats schätzen das Entdeckungsrisiko geringer ein als White Hats.

H14: Der Einstellung, dass Opfer ‚selbst schuld‘ seien, wenn sie gehackt werden, stimmen Black Hats signifikant stärker zu als White Hats.

Der Fragebogen soll ebenfalls die Motive von Black Hat Hackern erheben, um zu erfahren, was die Hauptmotive für kriminelles Hacking sind und wie die Motive mit Psychopathie, Machiavellismus und Narzissmus zusammenhängen. Kirwan & Power (2013, S. 63) haben aus der Literatur und empirischen Forschung eine Liste der Motive von Black Hat Hackern erstellt. Einige Motive könnten positive Korrelationen mit Triademerkmale aufweisen, z.B. *Thrill Seeking* mit Psychopathie oder die Suche nach Anerkennung mit Narzissmus. Die Autoren betonen ebenfalls, dass Kriminalität nicht monokausal erklärbar ist, sondern auf einem Zusammenspiel verschiedener Faktoren und multipler Motive beruht (Kirwan & Power, 2013, S. 16). Die Hypothesen 15 und 16 lauten daher:

H15: Hacking ist nicht nur durch finanziellen Gewinn motiviert, es liegen zeitgleich mehrere Motive vor.

H16: Es bestehen signifikante Korrelationen zwischen Merkmalen der Dunklen Triade und Motiven von Black Hat Hackern.

Bei den Angriffsarten von Hackern werden häufig weiche Techniken wie *Social Engineering* (siehe z.B. Wernert, 2021) und harte Techniken wie *Brute Force-Angriffe* (siehe z.B. Dave, 2013, S. 26) differenziert. Jones et al. (2021) fanden Zusammenhänge zwischen Triadeeigenschaften und den bevorzugten Angriffsmethoden: Schnelle, brachiale Angriffe waren eher typisch für Psychopathie und Narzissmus und langfristig geplante Angriffe, die Manipulation beinhalten, eher typisch für Machiavellismus.

H17: Es gibt Korrelationen zwischen Persönlichkeitsmerkmalen der Täter und dem bevorzugten Modus Operandi bei Cyberangriffen, die damit eine Grundlage für psychologisches Cyberprofiling bilden.

Die National Crime Agency (UK) betont in einer Publikation in Bezug auf KI: „The skill barrier to entry into cyber criminality is lower than it has ever been” (National Crime Agency (NCA), 2017, S. 4). Da es sich um eine technisch interessierte Zielgruppe handelt, ist anzunehmen, dass die Mehrzahl der Black Hats und White Hats bereits KI unterstützend für Hacking-Aktivitäten genutzt haben:

H18: Mehr als 50 % der Hacker haben bereits Künstliche Intelligenz für Hacking-Aktivitäten eingesetzt.

5.3 Zugang zum Forschungsfeld

Es gibt kaum Publikationen, die versuchen, ‚echte‘ Black Hat Hacker in Darknet-Foren zu finden, da die technische Hürde (Darknet, Tor-Browser), der Aufwand und auch das Risiko, selbst angegriffen zu werden, hoch ist. Hacker in Freiheit, außerhalb des Strafvollzugs, im Darknet zu einer Teilnahme an akademischen Studien zu überzeugen, ist schwierig.

Vier Aspekte sind daher strategisch bei der Planung des Forschungsdesigns bedeutsam, um überhaupt die Chance zu haben, Black Hat Hacker als Probanden zu erreichen und zu überzeugen.

Erstens sollte die Bearbeitungszeit des Fragebogens ca. 5 Minuten nicht überschreiten, da niedriges zeitliches Investment die Teilnahmehürde senkt. Insbesondere Black Hat Hacker haben beim Teilen von Informationen Bedenken. Das Grundprinzip bei der Erhebung ist es, so viele Daten wie nötig zu erheben, aber so zeiteffizient wie möglich. Die Bearbeitungszeit unter 5 Minuten zu halten, ist ein starkes Teilnahmeargument und erhöht die potentiell erreichbare Fallzahl.

Zweitens muss kompromisslose Anonymität bei der Befragung sichergestellt werden. Es geht hierbei nicht darum, Identitäten aufzuspüren oder Täter an Ermittlungsbehörden auszuliefern. Insbesondere werden keinerlei personenbezogenen Daten erhoben, die Personen identifizierbar machen könnten, also keine Namen, Geburtsdaten, E-Mail-Adresse, IP-Adressen, genaues Alter oder Daten, die die Gefahr einer potentiellen Deanonymisierung bergen. Hacker sprechen von ‚OpSec‘, was für *Operational Security* steht. In diesem Fall geht es lediglich um die Informationsgewinnung für akademische Zwecke, wobei die OpSec der Hacker respektiert wird und dies auch deutlich kommuniziert werden muss, da es sonst kaum möglich ist, Vertrauen aufzubauen.

Drittens soll der Fragebogen bei SoSci-Survey technisch so programmiert werden, dass dieser nicht nur Informationen erhebt, sondern am Ende auch den Teilnehmern die eigenen Ergebnis-Scores der Short Dark Triad (SD3) anzeigt, um die Befragung strategisch als ‚Persönlichkeitstest‘ oder ‚Selbsttest‘ positionieren zu können (Teilnahmemotiv: Neugier, Selbsterkenntnis).

Viertens soll eine ansprechende, aufmerksamkeitsregende Videokampagne erstellt werden, um Motive wie Neugier oder Stolz auf die eigenen Fähigkeiten zu adressieren („*Test your Dark Traits now!*“).

Ziel ist es so, über Videos und Posts in Hacker-Foren und Gruppen im Clear- und Darknet gezielt Motive wie Stolz, Ego und Neugierde auf Seiten der Hacker anzusprechen und so auch aktive kriminelle Black Hat Hacker außerhalb von Gefängnissen zu einer Teilnahme zu bewegen.

5.4 Fragebogenkonstruktion

Zur empirischen Untersuchung von Hackern und Beantwortung der Forschungsfragen wurde ein englischsprachiger Online-Fragebogen mit der Software SoSci-Survey entwickelt, der neben der Dunklen Triade auch weitere Merkmale erfasst, die Unterschiede zwischen Black Hats und White Hats erklären können. Neben der Gruppenzugehörigkeit (Black Hat oder White Hat) und vier allgemeinen demografischen Angaben (Geschlecht, grobe Altersgruppe in Blöcken, Nationalität und dem höchsten akademischen Bildungsabschluss) enthält der Fragebogen zwölf inhaltliche Konstrukte, welche zur Beantwortung der Forschungsfragen nötig sind: Psychopathie (SD3 Subskala), Narzissmus (SD3 Subskala), Machiavellismus (SD3 Subskala), Primäre Psychopathie (LSRP Subskala), Sekundäre Psychopathie (LSRP Subskala), Online Disinhibition Effect, Schuldumkehr, wahrgenommene Entdeckungswahrscheinlichkeit, Quelle der Hackingfähigkeiten, Motive von Black Hat Hackern, Bevorzugte Angriffsmethoden und bisherige KI-Nutzung.

Im Folgenden werden die einzelnen Blöcke, Konstrukte und deren Operationalisierungen beschrieben. Der Online-Fragebogen wurde mit der Software SoSci-Survey erstellt. Der vollständige Fragenkatalog der finalen Version des SoSci-Survey Fragebogens (16 Fragen) ist in Anhang 2 aufgeführt. Der Fragebogen besteht aus sechs inhaltlichen Blöcken (siehe Tabelle 6), sowie einer Einwilligungseite (Zweck der Studie, Anonymität der Daten, Freiwilligkeit der Teilnahme, Möglichkeit des Abbruchs, Kontaktdaten des Forschenden, Verwendung der Daten) und einer Abschlussseite, welche die Ergebnisse der Teilnehmer anzeigt. Der Block D (Black Hat Hacking Motive) bezieht sich konkret auf motivationale Faktoren für kriminelles Hacking und wurde daher nur Teilnehmern angezeigt, die zuvor ‚Black Hat Hacker‘ als Option gewählt haben.

Tabelle 6: Aufbau des Fragebogens

Themenblock	Enthaltene Konstrukte
Block A: Informierte Einwilligung, Hacker Label & Demografische Angaben	• Hacker-Kategorie (Black Hat/ White Hat/ Kein Hacker) • Geschlecht • Grobe Altersgruppe • Nationalität (freiwillig) • Bildungsabschluss
Block B: Dunkle Triade (SD3)	• Narzissmus (SD3, 9 Items) • Psychopathie (SD3, 9 Items) • Machiavellismus (SD3, 9 Items) • <i>Short Dark Triad</i> Gesamtscore
Block C: Quelle der Hackingfähigkeiten, Angriffsmethoden & KI Nutzung	• Quelle der Fähigkeiten (1 Item) • KI-Nutzung (1 Item) • Bevorzugte Angriffsmethoden (1 Item)
Block D: Black Hat Motive (Nur Gruppe Black Hats)	• Hacking Motive (Mehrfachauswahl 11 Items)
Block E: Online Disinhibition Effect, Schuldumkehr, Entdeckungswahrscheinlichkeit	• Online-Enthemmungseffekt (6 Items) • Schuldumkehr (1 Item) • Entdeckungswahrscheinlichkeit (2 Items)
Block F: Primäre & sekundäre Psychopathie Levenson Self-Report Psychopathy Scale (LSRP)	• LSRP Primäre Psychopathie (16 Items) • LSRP Sekundäre Psychopathie (10 Item) • LSRP-Gesamtscore

5.4.1 Operationalisierung der Konstrukte

Operationalisierung: Hacker-Kategorie

Die Zuordnung der Probanden zu den Gruppen ‚Black Hat‘ oder ‚White Hat‘ erfolgte zweischichtig: Zum einen über eine Selbstauskunft im Rahmen des Fragebogens, zum anderen über die gezielte Distribution des Befragungslinks in entsprechenden Hacker-Foren und Communities.

Der Link zur Umfrage wurde *nicht* breit öffentlich gestreut, etwa über Facebook-Posts oder universitäre Verteiler, sondern ausschließlich über gezieltes Targeting innerhalb hochspezialisierter, teilweise schwer zugänglicher Hacker-Foren. Das bedeutet, wer den Befragungslink gefunden hat, muss aktiver Nutzer in entsprechenden Hacker-Foren sein.

Das Hauptsicherstellungsmerkmal, dass es sich bei den Probanden tatsächlich um Hacker handelt, wurde also nicht per Selbstauskunft abgefragt, sondern durch die Distribution des Befragungslinks an sich. Wer diesen Link gefunden oder gesehen hat, muss auf die eine oder andere Art Teil der White Hat- oder Black Hat-Subkultur sein.

White Hat Hacker wurden primär über targetierte LinkedIn-Anzeigen erreicht (z.B. ausschließlich Personen mit dem wörtlichen Berufstitel ‚Ethical Hacker‘ in ihrem LinkedIn-Profil).

Per Selbstauskunft wurde als erste Frage gestellt, ob die Person sich als Black Hat Hacker oder White Hat Hacker bezeichnen würde (mit entsprechender Kurzdefinition) oder kein Hacker ist (diese Fälle wurden alle ausgeschlossen und nicht in die Analyse einbezogen).

1. Are you breaking the rules? Which category describes you (most accurately)?

☐ White Hat Hacker
(e.g. Pentester, **IT Security** Staff, Analyst, Ethical Hacker, Security Researcher)

☒ Black Hat Hacker
(any form of **unauthorized, criminal** hacking within last 12 months)

☐ I have **nothing** to do with any form of Coding, Hacking or Cybersecurity.

Abbildung 18. Screenshot Fragebogen: Operationalisierung der Hacker-Kategorie

Black Hat Hacking wurde hier definiert als jede Form des unautorisierten, kriminellen Hackings innerhalb der letzten 12 Monate. Da davon auszugehen ist, dass auch viele White Hat Hacker in ihrer Jugend ggf. Ungesetzliches getan haben, war das zeitliche Kriterium „innerhalb der letzten 12 Monate“ wichtig, um den Kreis auf *aktive* Black Hat Hacker einzugrenzen. Um dem Problem der sozialen Erwünschtheit entgegenzuwirken, wurde die Frage eingeleitet mit den Worten:

- Are you breaking the rules? Which category describes you (most accurately)?

Aus der Literatur ist bekannt, dass die meisten Hacker Autoritäten ablehnen. Ein ‚Rule Breaker‘ zu sein, ist damit ein bewusst positiveres Framing und senkt eher die Hemmschwelle, die Kategorie des Black Hat Hackings (unauthorized, *criminal* Hacking) auszuwählen, sofern dies zutrifft.

Zusammenfassend wurden Black Hats also operationalisiert als Personen, die aktiv in Darknet- oder Clearnet Hacker-Foren sind (durch Link-Distribution) und sich zusätzlich per Selbstauskunft als Black Hat identifizieren („any form of unauthorized, criminal hacking within last 12 months“).

White Hats wurden operationalisiert als Personen, die entsprechende Berufsbezeichnungen wie ‚Ethical Hacker‘ bei LinkedIn aufweisen oder aktiv in entsprechenden Ethical-Hacking-Foren sind und sich per Selbstauskunft als White Hat Hacker identifizieren („e.g. Pentester, IT Security Staff, Analyst, Ethical Hacker, Security Researcher“).

Allgemeine soziodemografische Angaben

Insbesondere für kriminelle Black Hat Hacker ist absolute Anonymität (OpSec) das wichtigste Gut. Gerade für Black Hats ist der Themenblock der soziodemografischen Angaben der kritischste Teil des Fragebogens und wurde bewusst kurzgehalten und an den Anfang des Fragebogens positioniert.

Es könnte angenommen werden, dass der Block zur Dunklen Triade ein sensibles Thema darstellt, während die Frage nach dem Geschlecht unproblematisch ist. Bei Black Hat Hackern außerhalb des Strafvollzugs verhält es sich jedoch genau umgekehrt. Sie sind in Hacker-Foren sehr offen über inhaltliche Kategorien, wie Motive, Einstellungen und Angriffsmethoden. Extrem verschlossen sind sie aber in Bezug auf ihre Identität. Es wurde sich bewusst dagegen entschieden, personenbezogene Daten gemäß der DSGVO zu erheben, die Personen identifizierbar machen könnten, sondern demografische Merkmale nur in allgemeinen Dimensionen und Altersblöcken zu erfassen.

Das Geschlecht wurde durch eine dichotome Antwortoption (male/female) erfasst. Nach gründlicher Abwägung wurde auf eine dritte Option *divers* verzichtet, da die Gefahr besteht,

dass gerade Black Hats dies als Ausweichoption missbrauchen würden, obwohl es nicht der Wahrheit entspricht. Wenn am Ende der Erhebung 20 % der Black Hats divers angäben, wäre unklar, ob dies tatsächlich der Realität entspricht oder die dritte Option als Ausweichoption missbraucht wurde, um die Frage nicht zu beantworten.

Das Alter wurde zum Schutz der Identität nicht exakt, sondern ab 18 in Gruppen von jeweils 5 Jahren (18-22, 23-27, etc.) erhoben. Lediglich der Block der Teenager unter 18 Jahren umfasst nur die Jahre 14-17, in Übereinstimmung mit der Richtlinie der Deutschen Gesellschaft für Online Forschung (DGOF, 2021), dass Minderjährige ab 14 ohne Einwilligung der Eltern online befragt werden können, sofern dies strikt anonym erfolgt. Die Nationalität wurde als optionale Angabe mit einem Freitextfeld abgefragt. Der höchste akademische Bildungsabschluss wurde in vier Kategorien erfasst von Abitur über Bachelor und Master bis Doktor (mit den jeweiligen US-Pendants dahinter: High School Diploma, Undergraduate, Graduate, PhD) und einem offenen Freitextfeld (Sonstiges).

Pflichtangaben beschränkten sich ausschließlich auf drei allgemeine demografische Merkmale, wie etwa *männlich*, *18-22 Jahre*, *Bachelorabschluss*, wodurch eine Identifikation einzelner Personen innerhalb der Grundgesamtheit ausgeschlossen ist. Da die Grundgesamtheit aktiver Hacker nicht auf eine bestimmte Universität oder Region begrenzt war, sondern potentiell alle Hacker weltweit umfasst, ist es völlig ausgeschlossen, anhand dieser Angaben Rückschlüsse auf einzelne Teilnehmer zu ziehen oder sie zu deanonymisieren.

Operationalisierung: Dunkle Triade

Den Hauptteil der Online-Befragung und das Hauptforschungsinteresse stellt die Erfassung der Dunklen Triade dar. Die Kürze der Befragung (< 5 Minuten) ist essentiell, um überhaupt die Chance eines empirischen Zugangs zu einer repräsentativen Zahl von Black Hat Hackern zu bekommen. Aus diesem Grund bestand die Notwendigkeit zur Verwendung einer Kurzskala zur gemeinsamen Erfassung der Dunklen Triade. In Kapitel 2.7 wurde dargestellt,

dass die SD3-Skala von Jones & Paulhus (2014) eine bessere Validität und Reliabilität zeigt als das (zu kurze) Instrument des *Dirty Dozen* (Jonason & Webster, 2010).

Zur Erfassung der Triademerkmale wurde daher die Short Dark Triad (SD3) von Jones und Paulhus (2014) eingesetzt. Es handelt sich dabei um ein ökonomisches, aber zugleich reliables und valides Instrument zur Messung von subklinischer Psychopathie, Narzissmus und Machiavellismus. In der Originalstudie berichten die Autoren Cronbachs Alpha-Werte von $\alpha = .71$ (Narzissmus), $\alpha = .77$ (Machiavellismus), $\alpha = .80$ (Psychopathie) (Jones & Paulhus, 2014, S. 36). Neben forschungsökonomischen Gründen sprach auch die breite Verwendung der SD3 in anderen Studien für ihren Einsatz, wodurch Vergleichbarkeit und Anschlussfähigkeit an bestehende Forschung gewährleistet sind. Eigene ermittelte Cronbachs Alpha-Werte der Subskalen werden im Ergebnisteil aufgeführt. Das Instrument umfasst insgesamt 27 Items, je 9 pro Subskala. Bei den Items handelt es sich um als Statements formulierte Aussagen, die jeweils Kernmerkmale der Konstrukte widerspiegeln. Eines der Items für Machiavellismus lautet z.B.: „I like to use clever manipulation to get my way“ (Jones & Paulhus, 2014, S. 38). Die Aussagen werden auf einer fünfstufigen Likert-Skala von 1 (= *Strongly Disagree*) bis 5 (= *Strongly Agree*) beantwortet. Pro Subskala wird ein Mittelwert gebildet, wobei einige Items reverse-codiert sind. Alle Punkte der Likert-Skala wurden beschriftet und es wurde auf die Option der grafischen Skalenvisualisierung bei SoSci-Survey zurückgegriffen (Abbildung 19).

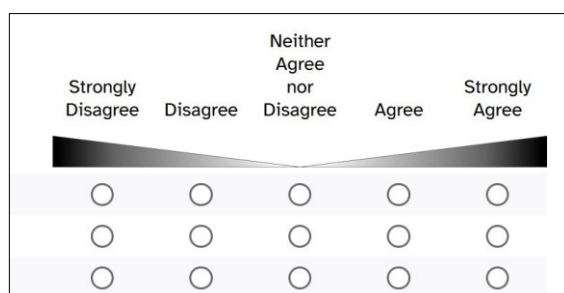


Abbildung 19. Visualisierte 5-stufige Likert-Skala

Um die ‚Itembatterie‘ von 27 Aussagen nicht zu umfangreich aussehen zu lassen und die Abbruchquote niedrig zu halten, wurden die Items auf drei Seiten des Online-Fragebogens verteilt.

In der Originalpublikation zur Entwicklung der Skala berichten die Autoren Jones & Paulhus (2014, S. 33) Normwerte für Psychopathie, Narzissmus und Machiavellismus, die in drei Studien mit insgesamt $N = 998$ Probanden erhoben wurden. Diese Werte der drei Studien der Originalpublikation werden als Normwerte für die Allgemeinbevölkerung verwendet, um Black Hat Hacker und White Hat Hacker mit diesem Referenzwert vergleichen zu können.

Das bedeutet, die Gruppen-Mittelwerte für Black Hats und White Hats wurden selbst erhoben, aber bei den Referenzwerten für die Allgemeinbevölkerung wurde auf bestehende, allgemein akzeptierte Referenzwerte aus der Literatur zurückgegriffen.

Operationalisierung: Primäre und sekundäre Psychopathie

Psychopathie wird im Fragebogen zwar in Form der SD3-Subskala erfasst, die Kürze der Skala von nur 9 Items erlaubt jedoch keine Differenzierung nach primärer und sekundärer Psychopathie. Doch gerade Psychopathie ist potentiell am relevantesten bei der Erklärung von Kriminalität (z.B. DeLisi, 2009) und ein mehrdimensionales Konstrukt (Schütte & Blickle, 2017, S. 93), das mit 9 Items nicht in der ganzen Breite erfasst werden kann. Es gilt als Konsens in der Psychopathieforschung, dass es sinnvoll ist, bei Psychopathie (mindestens) zwei Faktoren zu differenzieren: „Nearly all theoretical models and empirical studies of subtypes have posited a distinction between primary and secondary psychopathy“ (Hicks & Drislane, 2019, S. 299). Aus diesem Grund wurde eine zweite Skala gesucht, die eine zeiteffiziente Messung subklinischer Psychopathie erlaubt, aber lang genug ist, um eine valide Differenzierung von primärer und sekundärer Psychopathie zu erlauben. Da Skalen wie die PPI-R mit 154 Items und ca. 30 Minuten Bearbeitungszeit (Alpers & Eisenbarth, 2008, S. 23) zu umfangreich sind, wurde die Levenson Self-Report Psychopathy Scale (Levenson et al., 1995) als geeignetes Instrument ausgewählt. Die LSRP enthält 26 als Aussagen formulierte Items (16 Items für die Subskala primärer Psychopathie und 10 Items für Subskala sekundärer Psychopathie). Die Zustimmung zu den einzelnen Aussagen wird auf einer 4-stufigen Likert-Skala erfasst. Außerdem ist die LSRP dem Forschungsgegenstand (Hacker außerhalb des Strafvollzugssystems) angemessen. Klinische Diagnoseverfahren, wie die

PCL-R (Hare, 1991) finden vor allem in forensischen- und institutionellen Kontexten Anwendung und beinhalten u.a. Schritte wie die Analyse von Patientenakten oder Strafakten, - sie sind somit deutlich als Fremdbeurteilungsinstrumente konzipiert. Die LSRP-Skala wurde jedoch speziell für den Einsatz in nicht-institutionalisierten Stichproben entwickelt und ist als Selbstbeurteilungsinstrument konzipiert (Levenson et al., 1995). Die LSRP zeigt moderate Korrelationen mit der PCL-R und weist eine gute interne Reliabilität von Cronbachs $\alpha = .82$ für die Gesamtskala auf (Brinkley, Schmitt, Smith & Newman, 2001). Nach Falkenbach, Poythress, Falki und Manchak (2007) liegt die interne Konsistenz der Primärskala der Levenson LSRP in anderen Untersuchungen zwischen $\alpha = .82$ (Levenson et al., 1995) und $\alpha = .88$ (McHoskey, Worzel & Szyarto, 1998). Für die Sekundärskala berichten sie teilweise akzeptable, teilweise aber auch geringe Reliabilitätswerte von $\alpha = .53$ (McHoskey et al., 1998). Die geringere Alpha-Reliabilität der Subskala für sekundäre Psychopathie ist einer der Kritikpunkte der Levenson-Skala, trotzdem zeigen die PCL-R und LSRP „similar patterns of correlations to measures of substance abuse and criminal versatility“ (Brinkley et al., 2001, S. 1021). Die Levenson-Skala gilt insgesamt als etabliertes Instrument zur ökonomischen Messung von Psychopathie, insbesondere in nicht-institutionalisierten Populationen (Brooks & Fritzon, 2020, S. 119).

Ein ähnlich kurzes und ebenfalls etabliertes Selbstbeurteilungsinstrument ist die Self-Report Psychopathy Scale (SRP) (Paulhus, Neumann & Hare, 2009). Bei direktem Vergleich der Items erschienen jedoch einige Formulierungen der LSRP besonders anschlussfähig an die Lebensrealität von Hackern, z.B.: „People who are stupid enough to get ripped off usually deserve it“ oder „I often admire a really clever scam“ (Levenson et al., 1995, S. 153). Die LSRP wurde also aus inhaltlichen Gründen, aufgrund ihrer guten Eignung für die Population (Kriterium der Gegenstandsangemessenheit) und forschungsökonomischen Gründen zur vertiefenden Operationalisierung von Psychopathie ausgewählt.

Operationalisierung: Quelle der Hackingfähigkeiten

Lerntheorien und Subkulturtheorien probieren, kriminelles Verhalten durch das Umfeld zu erklären, in dem das Verhalten gelernt wurde, wie z.B. Sutherlands (1939) Theorie der differentiellen Assoziation. Um herauszufinden, wo und wie Hacker ihre technischen Fertigkeiten primär erlernt haben, wurden fünf Kategorien mit Beispielen zur Wahl gegeben, sowie ein Freitextfeld für eigene, offene Antworten. Eine Mehrfachauswahl war möglich.

How did you primarily learn your Hacking Skills?

- Self-study (Books, Blogs, Tutorials, YouTube)
- Hacker Communities (Forums, Events, Darknet, 4chan, Discord, Telegram)
- Mentor
- Hands-On Challenges (CTFs, Bug Bounties, Hackathons)
- Formal Education (University, Courses, Workshops)
- Others (Please specify)

Die vorgeschlagenen Antwortkategorien wurden zum Teil aus der Literatur abgeleitet (Chiesa et al., 2009, S. 122-127) sowie aus eigener Berufserfahrung durch die Analyse von Hacker-Foren.

Die fünf vorgegebenen Antwortoptionen sowie die frei formulierten Angaben im offenen Antwortfeld lassen sich insgesamt drei Kategorien zuordnen: regelkonform und legal, nicht-regelkonform und eher illegal und ein dazwischenliegender Graubereich.

„Formal Education“ ist eindeutig der legalen Kategorie zuzuordnen, während Plattformen, wie Hacker-Foren oder der Zugang zum Darknet, klar dem illegalen Bereich zugewiesen werden müssen. Bereits der Austausch über oder die Unterstützung von Straftaten kann laut § 27 StGB (Beihilfe) bzw. § 111 StGB (öffentliche Aufforderung zu Straftaten) strafbar sein.

Andere Lernquellen, wie Mentoren, Selbststudium oder Hands-on-Challenges, bewegen sich hingegen in einem Graubereich und können sowohl gesetzeskonform als auch problematisch sein, je nach Kontext, Inhalt und Intention.

Das Ziel bestand darin, herauszufinden, ob es hier systematische Unterschiede zwischen Black Hats und White Hats gibt, aus welchen Quellen und in welchem Umfeld sie ihre Hacking Skills gelernt haben.

Operationalisierung: KI-Nutzung für Hacking-Aktivitäten

Mit der Frage "Did you already use AI-Tools for Hacking or Social Engineering purposes? (e.g. WormGPT, Deepseek, ChatGPT)" wurde erfasst, ob und welche Anwendungen Generativer Künstlicher Intelligenz bereits zum Hacking genutzt wurden. Die Antwortkategorien waren *No / Yes (Please specify)*. Das Ziel bestand darin, herauszufinden, ob sich Black Hats und White Hats hier systematisch unterscheiden, und auch, welche KI-Modelle für kriminelle Aktivitäten gegenwärtig genutzt werden.

Aufgrund der Zukunftsimplicationen und des transformativen Potentials der KI schien es zeitgemäß, die KI-Nutzung mit einer Frage zu erheben, auch wenn dies keinen direkten Bezug zur Hauptforschungsfrage (Dunkle Triade bei Hackern) hat.

Operationalisierung: Bevorzugte Angriffsart (MO)

Im Fragebogen wurde dichotom erhoben, welche Form von Cyberangriffen die befragte Person grundsätzlich bevorzugt:

- Social Engineering (z.B. Phishing, Manipulation, Ausnutzung menschlicher Fehler)
oder
- Technische Hacks ohne menschliche Schwachstelle (z.B. Exploits, DDoS, Zero Days, Brute Force).

Hintergrund dieser Frage ist die empirische Überprüfung der Ergebnisse von Jones et al. (2021). Diese zeigten durch die Vorgabe eines hypothetischen Szenarios, dass Persönlichkeitsmerkmale der Dunklen Triade mit unterschiedlichen Angriffsstrategien zusammenhängen. Während Machiavellisten eher auf langfristige, verdeckte Täuschungsstrategien setzen (Social Engineering), bevorzugen Narzissten und Psychopathen direkte, aggressive Angriffsformen (Brute-Force-Attacks).

Diese Zusammenhänge sind hochrelevant, weil sie den zentralen Grundgedanken des Profilings im digitalen Raum stützen würden, dass sich aus dem Modus Operandi (also der Art des Angriffs) mögliche Rückschlüsse oder Wahrscheinlichkeitsaussagen auf psychologische Tätermerkmale ziehen lassen. Die Operationalisierung der bevorzugten Angriffsart als dichotome Kategorie (Technische Hacks vs. Social Engineering) ermöglicht in der statistischen Analyse das Berechnen punktbiserialer Korrelationen zwischen der bevorzugten Angriffsart der Hacker und Merkmalen der Dunklen Triade. Signifikante Zusammenhänge zwischen Tat und Täter bilden die Grundvoraussetzung für das erfolgreiche Täterprofilierung im Cyberraum.

Operationalisierung: Motive von Black Hat Hackern

Diese Frage bezog sich konkret auf die Motive für kriminelles Hacking und wurde nur Personen angezeigt, die zuvor ‚Black Hat Hacker‘ als Kategorie ausgewählt haben. Die Motive wurden mittels einer Liste von zehn vorgegebenen Motivkategorien und einer zusätzlichen Freitextoption erfasst. Die Aufforderung lautete, sich alle 10 Motive anzusehen und alle auszuwählen, die zutreffen:

- Please check all motives, that describe your motivation for hacking. You can choose multiple answers.

Dieses Fragenformat bietet den Vorteil, dass Teilnehmer an zentrale Motive erinnert werden, die ihnen möglicherweise nicht spontan einfallen würden, lässt gleichzeitig aber genügend Offenheit, individuelle Motive frei anzugeben. Die Liste der 10 Motivkategorien für das Black Hat Hacking wurde aus der Literatur abgeleitet. Kirwan und Power (2013, S. 63, Tabelle 3.2) listen insgesamt 31 teils redundante oder überlappende Motivkategorien für das Black Hat Hacking auf, die sie aus der Fachliteratur zusammengetragen haben. Die Tabelle bietet somit eine komprimierte Übersicht der „theorised motives of hackers“ (Kirwan & Power, 2013, S. 63). Zusätzlich wurden die neun vorgeschlagenen Motivkategorien des Bundeskriminalamtes (BKA, 2015b, S.18-20) einbezogen und alle genannten Motive des Hacker Profiling Projects (Chiesa et al., 2009, S. 144-160) mit einbezogen. Redundante Motive wurden entfernt und

sehr ähnliche Motive (z.B. Ablehnen von Autoritäten und Rebellion) zu einer übergeordneten Motivkategorie zusammengefasst. Auf diesem Wege wurde aus der Literatur und dem aktuellen Forschungsstand eine Liste mit 10 übergeordneten Motivkategorien für das kriminelle Hacking abgeleitet, wobei eine Mehrfachauswahl möglich war (siehe Abbildung 20).

12. Please check all motives, that describe your motivation for hacking.
You can choose multiple answers.

☐	Financial interests (money)
☒	I enjoy the challenge/ technical problem solving/test my own skills.
☐	Peer-recognition in hacking culture/ Status
☒	Feeling of power
☐	Feeling of addiction
☒	I enjoy the „Thrill“/ adrenaline.
☒	I reject authorities/ it's a form of rebellion.
☐	I hack to bring about political or social change.
☐	I hack purely for fun, entertainment, trolling.
☐	Frustration/ Revenge
☐	Others (Please Specify)

Abbildung 20. Screenshot Sosci-Survey Fragebogen: Motivauswahl

Operationalisierung: Online Disinhibition Effect

Der Online Disinhibition Effect beschreibt die Tendenz, sich im Cyberspace in positiver, aber auch negativer Hinsicht enthemmter zu verhalten (siehe Kapitel 3.4.2).

Zur Operationalisierung des Online Disinhibition Effects existiert zwar eine Skala von Udris (2014), diese wurde im Kontext von Mobbing unter High-School Studenten in Japan entwickelt und bezieht sich daher auf Cybermobbing und Hasskommentare. Die Skala ist daher weniger geeignet, um empirisch zu erheben, inwiefern der Online Desinhibition Effect kriminelles Hacking begünstigt. Daher wurde auf keine bestehende Skala zurückgegriffen, sondern sechs eigene Items zur Operationalisierung aus der Literatur abgeleitet. In Kapitel 3.4.3 wurde die White Gloves Theorie vorgestellt (Acker, 2023), wonach Menschen sich

online anders verhalten als in der realen Welt, im Sinne einer „Trennung der digitalen Handlung vom analogen Image“ (Acker, 2023, S. 64).

Zur methodischen Überprüfung schlägt Acker (2023) vor, die Zustimmung zu zwei identischen Verhaltensweisen abzufragen, jeweils in der digitalen und analogen Welt, z.B. „illegal Filme im Internet zu streamen“ (S.65) und „ohne Ticket in einen Kinosaal zu schleichen, um einen Film zu gucken“ (S. 65). Es ist die Beschreibung einer identischen Tat, jedoch in ihrer digitalen und analogen Variante. Das Konstrukt der Disinhibition (Enthemmung) wäre somit die Differenz zwischen der ‚Online-Skrupellosigkeit‘ und der ‚Offline-Skrupellosigkeit‘.

Auf Basis des Vorschlags von Acker (2023) wurden drei (kriminelle) Verhaltensweisen ausgewählt. Für jede dieser Verhaltensweisen wurde jeweils eine analoge und eine digitale Variante als hypothetisches Szenario formuliert (*I would...*). Die Zustimmung zu diesen hypothetischen Szenarien wurde mithilfe einer fünfstufigen Likert-Skala erfasst, die von 1 (= *Strongly Disagree*) bis 5 (= *Strongly Agree*) reicht. Die Likert-Skala, Beschriftung und Visualisierung entspricht der verwendeten Skala bei der Dunklen Triade und sorgt somit für eine Konsistenz und intuitive Verständlichkeit innerhalb des Befragungsinstrumentes.

Die sechs verwendeten Itemformulierungen sind:

- I would stream movies illegally.
- I would sneak into a movie theater without paying.
- I would hack someone's bank account.
- I would steal someone's wallet in real life.
- I would hack companies for profit.
- I would steal from companies in real life.

Wie von Acker (2023) vorgeschlagen, bilden die Items inhaltlich identische Verhaltensweisen in der analogen und der digitalen Welt ab. Besonders deutlich wird dies etwa bei den Items „Ich würde einer Privatperson das Portemonnaie stehlen“ vs. „Ich würde einer Person das

Bankkonto hacken“. Moralisch beschreibt es dasselbe Vergehen, der Unterschied liegt lediglich im Modus Operandi der Tat.

Der Mittelwert der drei Items der analogen Welt ergibt zusammen einen ‚Offline-Skrupellosigkeitsscore‘, während der Mittelwert der drei digitalen Items den ‚Online-Skrupellosigkeitsscore‘ bildet. Mittels *t*-Tests bei einer Stichprobe kann so pro Hackergruppe ermittelt werden, ob der Mittelwert der Online-Skrupellosigkeit und der Offline-Skrupellosigkeit sich signifikant unterscheiden.

Enthemmung wurde also, abgeleitet aus der White Gloves Theorie von Acker (2023), operationalisiert, indem die Mittelwertunterschiede zwischen der Online-Skrupellosigkeit und Offline-Skrupellosigkeit bei drei identischen Verhaltensweisen erfasst wurden.

Operationalisierung: Schuldumkehr

Die sechs Items zum Online Disinhibition Effect erfassen zwar, ob für Black Hat Hacker ein Unterschied in der Hemmung zwischen Taten in der realen Welt und im Cyberspace besteht, sie geben jedoch keinen Aufschluss über die Ursachen einer möglichen Enthemmung.

Um den Aspekt einer möglichen Schuldumkehr (Opfer seien ‚selbst schuld‘) zu erfassen, wurde ein entsprechendes Item als Aussage formuliert:

- If people have weak passwords, it's their own fault if they get hacked.

Die Zustimmung zu dieser Aussage wurde ebenfalls auf einer fünfstufigen Likert-Skala erfasst und bildet die Kategorie *Schuldumkehr* als Form moralischer Rechtfertigung bzw. Externalisierung der Verantwortung.

Operationalisierung: Entdeckungswahrscheinlichkeit

Ein wesentlicher Unterschied bei den beschriebenen Verhaltensweisen in der digitalen Welt (z.B. ein Konto hacken) und der analogen Welt (z.B. ein Portemonnaie stehlen) liegt auch in der Entdeckungswahrscheinlichkeit. Diese ist im digitalen Raum gering, und Verstöße gegen Normen bleiben oft ohne spürbare Konsequenzen für die Täter. Auch wenn das Internet

theoretisch kein rechtsfreier Raum ist, könne nach Hoheisel-Gruler (2020, S. 72) für Täter dieser Eindruck entstehen, wenn das Recht fast nie durchgesetzt wird. Auch Rüdigers (2018) Theorie des *Broken Web* (S. 259) besagt - angelehnt an die *Broken Windows Theorie* -, dass ein Normenverstoß weitere Verstöße nach sich ziehen kann, wenn andere bemerken, dass Fehlverhalten keine sichtbaren, negativen Konsequenzen hat (siehe auch: Hoheisel-Gruler, 2020, S. 81). Die Entdeckungswahrscheinlichkeit ist untrennbar mit der wahrgenommenen Kompetenz der Justiz und Polizeiarbeit in Cyberraum verbunden. Nach Otto (2020) ist der Digitalisierungsfortschritt (bezogen auf Deutschland) „nirgends so weit entfernt wie von der Justiz“ (S. 612). Wenn die Entdeckungswahrscheinlichkeit online als sehr gering eingeschätzt wird, könnte darin eine Ursache liegen, sich online enthemmter zu verhalten. Es ist wichtig zu betonen, dass hier die subjektiv *wahrgenommene* Entdeckungswahrscheinlichkeit der Hacker und die subjektiv *wahrgenommene* Kompetenz der Behörden bedeutsamer ist als die reale Kompetenz und Entdeckungswahrscheinlichkeit. Wenn ein Hacker annimmt, nie gefasst werden zu können, kann dieses Gefühl zu dem beschriebenen Effekt führen, unabhängig davon, ob dies faktisch so ist. Das Konstrukt der ‚wahrgenommenen Entdeckungswahrscheinlichkeit‘ wurde mit den folgenden beiden Items erhoben:

- I believe there is a very low chance of being caught when engaging in illegal hacking activities.
- The police are incompetent when it comes to handling Cybercrime.

Mithilfe einer fünfstufigen Likert-Skala wurde so die wahrgenommene Entdeckungswahrscheinlichkeit erfasst sowie die subjektiv wahrgenommene (In-)Kompetenz der Strafverfolgungsbehörden. Der Mittelwert der beiden Items bildet zusammen das Konstrukt der ‚wahrgenommenen Entdeckungswahrscheinlichkeit‘.

5.4.2 Programmierung der Endseite mit Darstellung der Ergebnisse

Dem Fragebogen wurde mittels HTML-Code die Funktion hinzugefügt, dass bereits während der Befragung die Ergebnis-Scores für die Short Dark Triad berechnet werden und auf der letzten Seite die eigenen Ergebnisse für die (subklinischen) Ausprägungen von Narzissmus,

Psychopathie und Machiavellismus mit entsprechendem Disclaimer angezeigt werden (siehe Abbildung 21). Dies ist ein wichtiges Element, da der Fragebogen so als Kurz-Persönlichkeitstest positioniert werden kann, um bei Hackern das Motiv der Neugier zu wecken („Test your dark traits now“). Somit erhebt der Fragebogen nicht nur Daten, sondern teilt auch die Ergebnisse mit, sodass die Teilnahme auch einen Eigennutzen hat (Selbsterkenntnis, Neugier).

Dark Trait	Your Score (on a Scale 1-5)	Average Score (Non-Hackers)
Psychopathy	2.44	2.4
Machiavellianism	2.44	3.1
Narcissism	2.78	2.8

Important Note:

The scale used in this study to measure Psychopathy, Narcissism, and Machiavellianism aims to capture subclinical expressions of these personality traits and does not constitute a diagnosis. The results represent merely a snapshot of certain tendencies in your personality and should not be interpreted as a medical or psychological diagnosis. If you have concerns about your mental health or wish to obtain a professional diagnosis, we recommend consulting a qualified psychologist or psychiatrist.

Abbildung 21. Screenshot Fragebogen: Ergebnisdarstellung

Die letzte Seite des Fragebogens dankt für die Teilnahme und enthält die Tabelle der eigenen Scores und den entsprechenden Hinweis, dass es sich hierbei lediglich um einen Kurztest subklinischer Tendenzen handelt und dies natürlich keine Diagnose darstellt. Es folgt eine Kurzdefinition der drei Konstrukte der Dunklen Triade, damit Nutzer die Bedeutung einordnen können, gefolgt von einem zweiten Hinweis (Disclaimer), dass dies keine Diagnose ist und selbst hohe Werte auf diesen subklinischen Instrumenten *nicht* als Persönlichkeitsstörung zu interpretieren sind. Außerdem wird auf die Kontaktmöglichkeit per E-Mail hingewiesen, an die eigens eingerichtete Mailadresse cyberpsych.study@protonmail.com, sofern Fragen bestehen. Der E-Mail-Provider *Protonmail* ist eine anonyme und verschlüsselte Art der E-Mail-Kommunikation, mit der Hacker vertraut sind, da sie ein etabliertes Kommunikationsmedium in dieser Subkultur darstellt.

5.4.3 Pretest & Anpassungen

Vor Beginn der Befragung wurde eine Testphase (Pretest) durchgeführt, in der das Befragungsinstrument inhaltlich und technisch überprüft und mehrfach angepasst wurde.

Die erste Phase bestand aus einem selbst durchgeführten technischen Pretest. Hierbei wurde getestet, ob der Online-Fragebogen auf verschiedenen Geräten, Browsern und Bildschirmgrößen technisch korrekt dargestellt wird und die Nutzerfreundlichkeit und intuitive Bedienbarkeit gegeben sind. Es wurde festgelegt, welche Angaben Pflichtangaben sind, inwiefern Skalen zur besseren Verständlichkeit visualisiert werden sollen und wie viele und welche (Sonder-)Zeichen in den Freitextfeldern erlaubt sind. Gerade bei Hackern besteht die Gefahr, dass sie Freitextfelder zum Hacken nutzen, indem sie hier Schadcode eingeben. Bei der Berechnung der Ergebnis-Scores der Short Dark Triad (SD3) wurde anfangs der einfache Mittelwert der Subskalen gebildet. Dies führte zu falschen Ergebnissen, da bei den Subskalen für Narzissmus und Psychopathie einige Items reverse-codiert sind. Dies wurde entsprechend korrigiert, bis der Fragebogen und die Berechnung der Ergebnisse technisch korrekt funktionierten.

In der zweiten Phase wurde ein inhaltlicher Pretest durchgeführt, bei dem der Fragebogen mit vier Bekannten und Familienmitgliedern (keine Hacker) durchgegangen wurde, mit der Bitte, dabei laut zu denken. Hierbei ging es insbesondere darum, ob der englischsprachige Fragebogen auch für Nicht-Muttersprachler verständlich ist. Hacker in englischsprachigen Hacker-Foren verstehen und kommunizieren zwar auf Englisch, es ist aber davon auszugehen, dass die Mehrzahl der Nutzer nicht Muttersprachler sind, sondern aus allen Teilen der Welt kommen. Aktive Hacker im Darknet agieren anonym oder pseudonym und verschleiern ihre Identität und echten IP-Adressen, sodass ein geografisches Targeting ohnehin nicht möglich wäre. Die forschungsökonomische Lösung besteht in einem englischsprachigen Fragebogen, der jedoch auch für Nicht-Muttersprachler verständlich formuliert ist. Beim Pretest wurden einige Fehler korrigiert, die Reihenfolge der Blöcke angepasst und Textbausteine eingefügt, die Nutzer motivieren, die Befragung fortzusetzen.

Bei drei Items der Short Dark Triad traten Verständnisschwierigkeiten bei mehreren Personen auf, da die englischsprachigen Begriffe unbekannt waren („*to get back at people*“, „*dull*“ und „*payback*“). Da es sich um etablierte Standardskalen handelt, wurden die Worte der Originalitems nicht verändert, aber in Klammern ein Synonym hinzugefügt, das im allgemeinen Sprachgebrauch geläufiger ist. Fettgedruckt sind die eigenen Ergänzungen zur Verbesserung der Verständlichkeit der SD3 (Jones & Paulhus, 2014, S. 38):

- You should wait for the right time to get back at people (**take revenge**).
- Many group activities tend to be dull (**boring**) without me.
- Payback (**revenge**) needs to be quick and nasty.

Auf diesem Wege wurde die Verständlichkeit erhöht, ohne die Vergleichbarkeit einzuschränken oder die Originalitems in ihrer Bedeutung oder Tonalität zu verändern.

In der letzten Phase des Pretests wurde der Link drei White Hat Hackern, also Cybersicherheits-Spezialisten aus dem eigenen Netzwerk, gesendet, um die Bearbeitungszeit zu messen. Diese lag im Rahmen der Zielzeit von 5 Minuten. Die kurze Bearbeitungszeit war eines der wichtigsten Argumente, um überhaupt Hacker zu einer freiwilligen Teilnahme zu bewegen.

5.5 Rekrutierungsstrategie und Video

Es existieren eine Reihe von Hacker-Foren, die sich optisch und strukturell kaum von anderen sozialen Netzwerken unterscheiden. Black Hats kommunizieren hier erstaunlich offen, ohne Angst vor Strafverfolgung. In gewisser Weise agieren viele Hacker im Darknet nicht anonym, sondern pseudonym. Somit ist es möglich, zumindest mit diesen Pseudonymen Versuche der Kontaktaufnahme zu unternehmen. Hier schließt die zweite Frage an, warum Probanden bereit sein sollten, an Studien teilzunehmen und Fragen zu ihrer Persönlichkeit wahrheitsgemäß zu beantworten. Zum einen ist Neugierde eines der Motive von Hackern und häufig genanntes Persönlichkeitsmerkmal (BKA, 2015b; S. 18; Chiesa et al., 2009, S.

147; Kirwan & Power, 2013, S. 63). Neugierde könnte Motivation zur Teilnahme sein, wenn die Studie interessant klingt, kompromisslose Anonymität gewährleistet („OpSec-Garantie“) und nicht zu viel Zeit beansprucht. Ebenfalls wurden narzisstische Eigenschaften wie Statusstreben oder Bewunderung, häufig anekdotisch und teils empirisch, mit Hackern in Verbindung gebracht (BKA, 2015b, S. 17; Kirwan & Power, 2013, S. 63). Das Mitteilungsbedürfnis innerhalb der Foren könnte als Stolz auf die Taten interpretiert werden, da Hacker im analogen Leben kaum mit ihren technischen- oder kognitiven Kapazitäten im Bereich Cybercrime prahlen können. Dies im geschützten Rahmen akademischer Forschung (anonym) zu tun, könnte eines der Teilnahmemotive sein. Einen gewissen Narzissmus, Neugierde und Stolz auf Seiten der Black Hat Hacker zu adressieren, soll die Basis der Rekrutierungsstrategie bilden. Bereits vor rund 50 Jahren gelang es Widom (1977), über Zeitungsannoncen nicht-institutionalisierte Psychopathen zu finden und zu gewinnen, sodass dies auch bei Hackern mit Triadeeigenschaften möglich sein könnte.

Der nächste Schritt bestand in der Entwicklung einer ansprechenden Videokampagne sowie von Bild- und Textbeiträgen, die diese Teilnahmeargumente aufgreifen und mögliche Motive von Black Hat Hackern, wie Neugier, Stolz auf die eigenen Fähigkeiten oder den eigenen Narzissmus, adressieren.

Eine Grundsatzentscheidung war, inwiefern vor Teilnahme im Rekrutierungsvideo bereits transparent über den wahren Zweck der Studie (Untersuchung der Dunklen Triade bei Black Hats und White Hats) aufgeklärt werden sollte oder dies allgemeiner und dennoch wahrheitsgemäß formuliert werden sollte, z.B. als „Untersuchung zur Psychologie von Hackern“. Da das Wort ‚Psychopathie‘ im allgemeinen Sprachgebrauch negativ konnotiert ist, bestand die Gefahr, dass potentielle Teilnehmer sich durch die Verwendung des Begriffs voreilig etikettiert fühlen könnten. Das könnte sich potentiell negativ auf die Teilnahmebereitschaft oder das Antwortverhalten auswirken (Problem der *sozialen Erwünschtheit*). Andererseits sind Hacker intelligent und tätigkeitsbedingt extrem skeptisch. Ein Wesensmerkmal des Hackings ist die Freude daran, hinter die Fassade zu schauen und herauszufinden, wie etwas im Inneren funktioniert. Eine kurze Google-Suche eines

beliebigen Items der Short Dark Triad (SD3) offenbart die Skala, zu der es gehört, und somit auch die Konstrukte, die es erheben soll. Den Zweck der Studie zu verschleiern, in der Hoffnung, dass Teilnehmer dies nicht merken, wäre eine dramatische Unterschätzung des Intellekts von Hackern. Außerdem sind zahlreiche Items der SD3 und LSRP wenig subtil und zielen deutlich auf antisoziales Verhalten ab, z.B. „It's true that I can be mean to others“ (Jones & Paulhus, 2014, S. 38). Der Fragebogen enthält (inklusive des Blocks, der nur Black Hat Hackern angezeigt wird) insgesamt 81 Items, wovon sich 74 Items explizit und wenig subtil auf Triadeeigenschaften oder kriminelles Verhalten beziehen. Den Zweck der Studie offen zu kommunizieren, war daher alternativlos. Auch im Sinne der Forschungsethik ist eine ehrliche und umfassende Aufklärung über den *wahren* Zweck der Studie wichtig, um den Standards der Deutschen Gesellschaft für Psychologie zu entsprechen (DGPs, 2018, S. 153).

Das Ziel war es also, bereits im Rekrutierungsvideo den Zweck der Studie transparent darzustellen, jedoch auch Psychopathie positiver zu ‚framen‘, um dem Problem der sozialen Erwünschtheit proaktiv zu begegnen.

Es wurde dargestellt, dass Psychopathie keineswegs nur mit Gewaltkriminalität assoziiert wird, sondern es zahlreiche „Successful Psychopaths“ (Mullins-Sweatt et al., 2010, S. 554) im Top-Management gibt. *Furchtlose Dominanz* und eine ‚Coolness unter Stress‘ ist in vielen Branchen von Vorteil, z.B. bei Chirurgen, Bombenentschärfern oder Wall Street Bankern. Durch die Nennung dieser Beispiele, welche allgemein mit Erfolg und gesellschaftlichem Ansehen assoziiert werden, sollte die negative Konnotation des Begriffs der Dunklen Triade und insbesondere Psychopathie neu gerahmt bzw. kontextualisiert werden. Abbildung 22 zeigt eine Bildschirmaufnahme des Rekrutierungsvideos. Das verwendete Video wurde nach der Erhebung zum Zwecke der Dokumentation und im Sinne der intersubjektiven Nachvollziehbarkeit auf die Plattform *Vimeo* hochgeladen und ist unter folgendem Link oder QR-Code abrufbar URL: <https://vimeo.com/1116157544/de11dadced>



Abbildung 22. QR-Link zum Rekrutierungsvideo

Tabelle 7 enthält das wörtliche Videotranskript und die jeweiligen methodischen Überlegungen und Ziele hinter dem verwendeten Wortlaut. Einblendungen sind durch eckige Klammern im Transkript gekennzeichnet.

Tabelle 7: Transkript des Rekrutierungsvideos und methodische Überlegungen

Transkript Rekrutierungsvideo	Ziele und methodische Überlegungen
“Dear Hackers, I am looking for participants for a short scientific Online-Survey about the so called ‘Dark Triad of Personality’, which consists of Narcissism, Machiavellianism and Psychopathy [Einblendung Schaubild Dunkle Triade].”	Transparente Aufklärung über den wahren Zweck der Studie aus ethischen Gründen und weil Hacker eine intelligente und extrem skeptische Zielgruppe sind. Einer Verschleierung des wahren Zwecks könnte Vertrauen brechen.
“If most people hear the term <i>Psychopathy</i> they immediately have something like this [Einblendung Symbolbild Dr. Lecter] in mind, - like Serial Killers.”	Einstieg mit dem Klischee und der typischen Assoziation zwecks Aufmerksamkeit und Klicks, um dieses im Anschluss zu entkräften.
“And yes, while most serial killers are psychopaths, there is another side of psychopathy which is less known: ‘Functional Psychopathy’ or ‘Successful Psychopathy’. Yes, many top managers are known to score very high on these dark traits. I mean... think about it: Having no emotions, being fearless and being very calm under extreme pressure? In some professions this could be very useful. Think about surgeons or wall street bankers or bomb disposal experts.”	Lenkung des Fokus auf funktionelle Psychopathie und die positive Seite von Psychopathie. Bewusste Nennung von Berufsgruppen mit erhöhten Psychopathie-Scores, die einen hohen gesellschaftlichen Status genießen und/oder als besonders mutig gelten (Bombenentschärfer, Chirurgen, ...).

Transkript Rekrutierungsvideo	Ziele und methodische Überlegungen
“But what is known about the Dark Triad and hacking? The answer is: Almost nothing. That’s why I am looking for my research for 100 Black Hat Hackers and 100 White Hat Hackers, who are willing to participate in a 5-minute scientific Online-Study.”	Überleitung zum Forschungsthema. Indirekter Appell an die eigene Bedeutsamkeit bei Teilnahme, da kaum etwas bekannt ist und man zu den ersten 100 Probanden gehören kann.
“It just takes 5 minutes, you will see your personal results, your dark scores, right after and you can see how you compare. It’s 100 % anonymous. I don’t care who you are, I just try to find out how you are. And you would really help to push the research in this field. So, I will post the link somewhere over under or next to this video and if you have any questions about the research you can contact me anonymously here [Einblendung Kontakt-E-Mail-Adresse]. Thank you very much and this helps a lot.“	Auflistung der vier Teilnahmeargumente: ▪ Bearbeitungszeit nur ca. 5 Minuten ▪ Die eigenen Ergebnisse (persönlichen Scores) sind direkt im Anschluss sichtbar (Motiv: Neugier, Selbsterkenntnis) ▪ Betonung der Anonymität und Respektierung der OpSec ▪ Eigene Teilnahme hat positiven Einfluss auf die Forschung in diesem Feld (Motiv: Eigene Bedeutsamkeit, das Motiv, zu helfen) + Danksagung und Möglichkeit der anonymen Kontaktaufnahme für Rückfragen.

Im Rekrutierungsvideo wurde bewusst offen das eigene Gesicht gezeigt, um Vertrauen aufzubauen. Das ist in Hacker-Foren, insbesondere im Darknet, absolut unüblich, aber war ein gezielt gewähltes Mittel. Aus Sicherheitsgründen wurden jedoch weder der vollständige Name noch die Universität Tübingen im Rekrutierungsvideo selbst genannt. Diese Informationen, einschließlich des Klarnamens des Forschenden, der betreuenden Universität sowie des Zwecks der Studie (Dissertation), werden transparent auf der Einstiegs- und Einwilligungsseite der Online-Befragung und im Impressum bereitgestellt. Das bedeutet, sobald ein Proband den Befragungslink angeklickt hat, wurden alle Informationen zum Datenschutz, dem Zweck der Studie und die eigene Identität vollständig transparent offengelegt. So wurde gewährleistet, dass potentielle Teilnehmer bei tatsächlichem Interesse

umfassend informiert werden, ohne bereits im Rekrutierungsvideo die eigene Identität vollständig offenzulegen. Dieses Vorgehen schaffte eine Balance zwischen Offenheit und Sicherheit in diesem sensiblen Rekrutierungskontext im Clear- und Darknet.

Nicht alle Plattformen und Darknet-Foren erlauben das Format eines Videobeitrages, und oftmals ist die erlaubte Zeichenzahl (ähnlich wie bei dem sozialen Medium X, vormals *Twitter*) stark begrenzt. Deshalb wurden die wesentlichen Teilnahmegründe auch in Textform verfasst und mit KI-Software (Canva und ChatGPT) einige lizenzfreie Bilder generiert, die urheberrechtlich nicht geschützt sind und somit frei verwendet werden können. Abbildung 23 zeigt Beispiele für vorbereitete Text- und Bildbeiträge, die ebenfalls das Ziel verfolgen, Aufmerksamkeit zu erregen, Neugier zu wecken und zentrale Teilnahmegründe hervorzuheben.

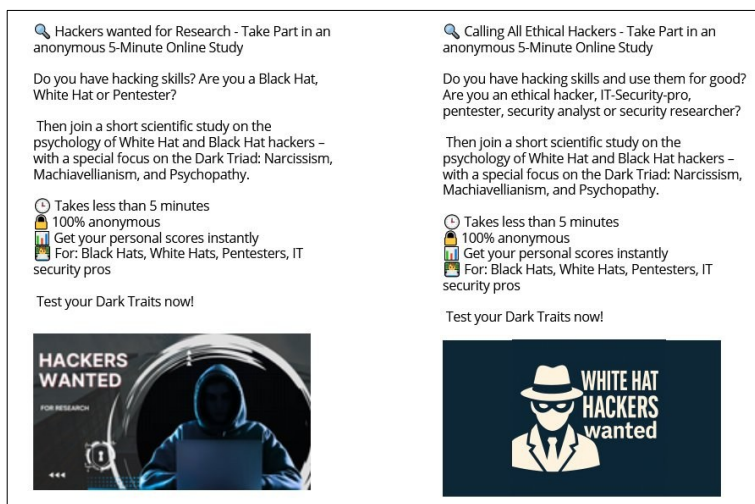


Abbildung 23. Beispiel Text- und Bildbeiträge zur Rekrutierung von Hackern

5.6 Rechtliche Aspekte, Ethik und besondere Sicherheitsvorkehrungen

Forschung mit Hackern im Darknet stellt ein gewisses Novum und sensibles Forschungsfeld dar, sodass umfangreiche Sicherheitsmaßnahmen ergriffen wurden, zum Schutz der Probanden und auch zum Eigenschutz. Obwohl keine personenbezogenen Daten im Sinne einer Identifizierbarkeit gemäß DSGVO erhoben wurden, wurden zahlreiche und umfassende Schritte zur Absicherung unternommen (z.B. kryptografisch verschlüsselte Kommunikation

über PGP), die weit über das normalerweise nötige Maß hinausgehen. Bezogen auf die Forschung im Darknet galt selbstverständlich das Strafgesetzbuch als Regelwerk, wobei zusätzlich eine Strafrechtskanzlei zur Beratung und Stellungnahme beauftragt wurde, um hier besonders verantwortungsvoll, ethisch und transparent zu handeln. Forschungsethisch wurde sich an den Vorgaben der DGPs für „Ethisches Handeln in der psychologischen Forschung“ (2018, Titel) orientiert, sowie an den Leitlinien der Deutschen Gesellschaft für Online-Forschung (DGOF e.V.).

Sich im Darknet zu bewegen, ist nicht per se verboten, aber mit Risiken verbunden, wie das Bundesamt für Sicherheit in der Informationstechnologie deutlich ausführt:

„Das Bewegen im Darknet alleine ist nicht illegal, es stellt jedoch ein Sicherheitsrisiko dar. Durch die vielen Geschichten, die rund um das Darknet kursieren und die Anonymität der Nutzerinnen und Nutzer kommt leicht der Eindruck auf, das Netzwerk sei per se unzulässig. Straffällig werden Sie allerdings nur, wenn Sie illegale Inhalte konsumieren, herunterladen oder rechtswidrige Waren und Dienstleistungen erwerben oder anbieten“ (BSI, 2025a).

Umso wichtiger ist es, die rechtlichen Grenzen genau zu kennen und diese im Vorfeld klar zu definieren und Maßnahmen zu ergreifen, sich auf mögliche Cyberangriffe vorzubereiten. Seriöse Forschung muss hier klare Regeln definieren und konsequent beachten. Zur Dokumentation der Grenzen dessen, was im Rahmen von Forschung erlaubt ist, wurde zusätzlich die Kanzlei *Kujus Strafverteidigung* aus Leipzig mit einer kurzen Stellungnahme beauftragt, die vollständig in Anhang 3 aufgeführt ist. Hierin führt Fachanwalt für Strafrecht Kujus aus:

„Das hartnäckige Missverständnis, schon das Betreten des Darknets sei strafbar, ist nicht zutreffend. Maßgeblich für eine mögliche Strafbarkeit ist nicht der Ort oder die Technik, sondern das konkrete Verhalten. Das Strafrecht kennt keinen eigenständigen Tatbestand ‚Darknet‘. Wer Anonymität sucht oder geschützt kommunizieren möchte, kann hierfür grundsätzlich Tor und vergleichbare Anonymisierungsdienste ebenso nutzen wie Seiten im sog. ‚Darknet‘ aufrufen. Das bloße Aufrufen von .onion-Adressen, das Lesen von Foren oder der Betrieb rechtmäßiger, eigener Angebote bewegt sich im zulässigen Bereich. Auch Recherchen zu wissenschaftlichen, journalistischen oder forensischen Zwecken sind

möglich, solange auf frei zugängliche Informationen zurückgegriffen wird und keine Zugangssperren überwunden werden. Die zulässige Nutzung setzt jedoch klare Selbstbeschränkung voraus.“ (Kujus Strafverteidigung, 2025, Anhang 3)

Es versteht sich von selbst, dass jegliche Form der aktiven Beteiligung an kriminellen Handlungen strafbar ist, also z.B. illegale Waren zu kaufen oder anzubieten, Hacking-Dienstleistungen als Auftraggeber zu buchen, gestohlene Daten herunterzuladen oder weiterzuverbreiten, kriminelle Aktivitäten jeglicher Art zu unterstützen etc. Relevante Gesetze sind in diesem Zusammenhang z.B. § 202a StGB (Ausspähen von Daten), § 202d StGB (Datenhehlerei), § 202b StGB (Abfangen von Daten) oder § 303b StGB (Computersabotage).

Strafverteidiger Kujus resümiert: „Wer seriös forscht, trennt strikt Beobachtung von Teilnahme“ (siehe Anhang 3).

Zu jedem Zeitpunkt der Erhebung (in allen durchgeführten Studien) wurden die nachfolgenden Darknet-Verhaltensregeln selbst definiert und strikt eingehalten:

- Regel 1: Keine Straftaten, keine Beteiligung an Straftaten, keine ‚Testkäufe‘ oder Ähnliches: Selbstverständlich wurden weder § 263a StGB (Computerbetrug) oder § 303b StGB (Computersabotage) noch Datenhehlerei begangen, vorbereitet oder unterstützt. Es wurden auch keine Datensätze (sogenannte Leaks) heruntergeladen, keine Inhalte, bei denen bereits das Ansehen strafbar wäre, gesehen oder heruntergeladen und grundsätzlich keine Links, Anhänge oder Downloads im Darknet angeklickt. Es erfolgte eine strikte, verantwortungsvolle und professionelle Trennung zwischen legaler Beobachtung von Hacking-Foren, aber niemals einer aktiven, illegalen Beteiligung.
- Regel 2: Kein wahlloses ‚Herumsurfen‘ im Darknet. Über eine Recherche zu *Cyber Threat Intelligence* per Google-Suche und *Github* wurden vorab relevante *.onion*-Links zu Hacker-Foren identifiziert und ausschließlich diese Seiten gezielt und direkt (ohne Umwege über Darknet-Suchmaschinen) aufgerufen.
- Regel 3: Beschränkung auf reine Hacker-Foren und nur diejenigen, die sich strikt auf das Hacking beschränken und keinerlei Diskussionen zu Waffen, Drogen und insbesondere kinderpornografisches Material beinhalten oder dulden. Pädokriminelle haben in Hacker-

Foren eine ähnliche Reputation wie in Gefängnissen, sodass sich diese Bereiche glücklicherweise nicht mischen oder überschneiden. Zu keinem Zeitpunkt wurde während der Recherchen und Probandengewinnung auf entsprechendes Material in Hacker-Foren gestoßen.

- Regel 4: Keine Undercover-Recherche, sondern transparente, offene Kommunikation der Rolle als Forschender. Zu keinem Zeitpunkt wurde der Eindruck erweckt, selbst Hacker zu sein. Es wurde sich zu keinem Zeitpunkt als Hacker ausgegeben, sondern offen kommuniziert, dass es sich um eine akademische Studie/ Dissertation handelt. Es wurde sofort und unmissverständlich klargemacht, dass es sich um ein Forschungsinteresse handelt und freiwillige Probanden gesucht werden. Im Rekrutierungsvideo ist der Forschende mit Gesicht identifizierbar, im Impressum des Fragebogenlinks dann auch mit Klarnamen und Kontakt identifizier- und kontaktierbar, auch wenn das mit persönlichen Sicherheitsrisiken einherging.

- Regel 5: Den Umfang auf die absolute Notwendigkeit beschränken. Die Grundregel lautete hier: So viel wie nötig, so wenig wie möglich. Die Zeit, der Umfang und die Anzahl der Darknet-Besuche und Beiträge wurde auf das zur Studiendurchführung nötige Maß beschränkt.

- Regel 6: Keine Kenntnis von Identitäten, keine Kenntnis von konkreten Taten. Das Studieninteresse beschränkt sich auf psychologische Dimensionen und allgemeine Hacking-Motive. Es wurden weder Identitäten noch konkrete Taten erfasst oder davon Kenntnis erlangt. Ebenfalls wurde keine Kenntnis von geplanten schweren Straftaten (z.B. Cyberterrorismus) erlangt, denn auch dies würde nach § 138 StGB zur Anzeige verpflichten.

- Regel 7: Keine Zugangsbeschränkungen umgehen oder illegale Hürden nehmen. Einige Hacking-Foren verlangen eine Zugangsgebühr oder den Beleg, 'einer von ihnen zu sein', also eine entsprechende Reputation als Hacker. Diese Foren wurden ausgeschlossen, da der Zugang daran gekoppelt ist, selbst zu hacken oder die Foren finanziell zu unterstützen. Diese Hürde ist für polizeiliche Undercover-Ermittlungen möglich, aber nicht im Rahmen akademischer, ethischer Forschung.

▪ Regel 8: Konsequenter Eigenschutz. Da sich offen als Forscher zu erkennen gegeben wurde, wurde eine gesicherte anonyme Kontakt-E-Mailadresse (cyberpsych.study@protonmail.com) erstellt und selbstverständlich nicht die universitäre E-Mail-Adresse genutzt. Die Kommunikation mit Hackern fand zudem primär PGP-verschlüsselt statt. Für Darknet-Forschung wurde ein eigener Laptop nur zu diesem Zweck temporär beschafft (falls dieser gehackt wird), sowie separate WLAN-Verbindungen und VPN-Dienste verwendet. Bevor mit Hackern in Kontakt getreten wurde, wurde die eigene Cybersicherheit bestmöglich aufgerüstet, sowie eine Rechtsschutz- und Cyberversicherung abgeschlossen.

Vor Beginn der Befragung wurden die Teilnehmer über den Zweck, die Dauer, die Freiwilligkeit sowie die anonyme Datenverarbeitung informiert. Die Operational Security der Black Hat Hacker musste gewährleistet werden, um Vertrauen aufzubauen, das heißt, es wurden keine Informationen erhoben, die auf Identitäten oder konkrete begangene Delikte (in Bezug auf Fragen wie was, wann oder wo) abzielen. Insbesondere wurden keine IP-Adressen oder andere Arten des ‚Fingerprinting‘ oder verdeckten Profilings betrieben.

Da Teilnahmeaufrufe als Beiträge in Hacker-Foren geteilt wurden, fand eine freiwillige Selbstselektion statt. Genaue Regionen, Sprachen, Altersgruppen etc. ließen sich vorab nicht selektieren. Klarheit und Verständlichkeit der informierten Einwilligung war daher das oberste Prinzip. Der Text sollte in englischer Sprache so simpel und klar wie möglich formuliert werden, damit Personen jeder Altersgruppe und Nationalität - von Indien bis Deutschland - im gleichen Maße verstehen, was der Zweck der Studie ist, wie die Daten verwendet werden und dass die Teilnahme anonym und freiwillig ist.

Die erhobenen Daten wurden 2 Monate nach Abschluss der Erhebung von den SoSci-Servern gelöscht. Auch die Darknet-Rekrutierungsaufrufe wurden, sofern dies möglich war, aus den Darknet-Foren gelöscht, um den eigenen Namen und das eigene Gesicht hier nicht länger als unbedingt notwendig verfügbar zu haben.

Den Betreuern wurde bei mit Abgabe der Dissertation der vollständig anonyme SPSS-Datensatz auf einem USB-Datenträger ausgehändigt.

Zahlreiche Hacker beginnen bereits als Kinder oder Jugendliche damit, erste technische Fähigkeiten zu erlernen. Sie werden in der Szene oft als *Script Kiddies* bezeichnet und belächelt. Chiesa et al. (2009, S. 74) berichten, dass 61 % der befragten Hacker ihre ersten Hacking-Fähigkeiten im jungen Alter zwischen 10 und 15 Jahren erworben haben. Es ist daher naheliegend, dass auch in fortgeschritteneren Darknet-Foren nicht nur Erwachsene, sondern zumindest einige Teenager aktiv sind, die bereits über fundiertere technische Kompetenzen verfügen.

Die technische Einstiegshürde ins Darknet ist vergleichsweise hoch. Es ist nicht möglich, ‚aus Versehen‘ durch einen einfachen Klick im Darknet zu landen. Vielmehr muss der Tor-Browser installiert und eine spezifische *.onion-Adresse* gezielt angesteuert werden. Wer diese Schritte durchführt, weiß genau, was er oder sie da tut, handelt mit klarem Bewusstsein und zeigt eine gewisse Einsichtsfähigkeit. Selbst die meisten Erwachsenen wissen nicht, was das Darknet ist oder wie man dort hineinkommt.

Innerhalb der Hacker-Foren fand eine freiwillige Selbstselektion statt, es wurden also weder gezielt bestimmte Personengruppen angesprochen und erst recht nicht gezielt Minderjährige kontaktiert. Da jedoch bei einer freiwilligen, anonymen Selbstselektion keine Kontrolle darüber möglich ist, wer genau teilnimmt, konnte nicht ausgeschlossen werden, dass auch Personen unter 18 Jahren den Online-Fragebogenlink anklicken und ausfüllen. Diese grundsätzlich auszuschließen, wäre jedoch auch forschungsethisch bedenklich. Dass sich Minderjährige - ohne Wissen ihrer Eltern - in kriminellen Darknet-Foren aufhalten, ist ein besorgniserregendes gesellschaftliches Phänomen. Gerade deshalb darf es empirisch nicht ignoriert werden, sondern muss wissenschaftlich und objektiv beschrieben werden. Ein Ziel dieser Arbeit ist es, Hackerprofile besser zu verstehen, auch im Hinblick auf die Möglichkeit *selektiver Prävention* (Bürger & Kaess, 2024). Gerade bei Jugendlichen besteht noch die Chance, sie ‚auf die gute Seite‘ zu holen, bevor sie sich dauerhaft radikalisieren.

Im Rahmen einer Online-Befragung mit anonymer Selbstselektion ist es nicht praktikabel und realitätsfern, Hacker zu verpflichten, ihr Alter offenzulegen, und im Falle der Minderjährigkeit

die schriftliche Einwilligung der Eltern einzuholen. Die vier Vereine Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V. (ADM), die Arbeitsgemeinschaft Sozialwissenschaftlicher Institute e.V. (ASI), der Berufsverband Deutscher Markt- und Sozialforscher e.V. (BVM) sowie die Deutsche Gesellschaft für Online-Forschung e.V. (DGOF) haben eine gemeinsame Richtlinie publiziert, in der sie darauf hinweisen, dass Personen ab 14 Jahren auch ohne elterliche Einwilligung befragt werden dürfen, sofern Anonymität gewährleistet ist und keine bekannten Risiken für die Befragten bestehen (DGOF, 2021). Auch wenn die Dissertation an einer deutschen Universität durchgeführt wird, kommen die Mehrzahl der Teilnehmer aus allen möglichen Teilen der Welt, doch auch auf EU-Ebene wird das Mindestalter zur Einwilligung in die Verarbeitung personenbezogener Daten in den meisten Ländern auf 13 oder 14 Jahre festgelegt (European Union Agency for Fundamental Rights, 2017).

In Anlehnung an diese Richtlinien wurden in der vorliegenden Studie bei der Auswertung ausschließlich Personen ab 14 Jahren einbezogen. Jüngere Personen wurden im Schritt der Datenbereinigung (siehe Kapitel 5.8) ausgeschlossen, betroffen waren hiervon jedoch lediglich neun Fälle (0,75 %), die aufgrund des Alters nicht in die Analyse einbezogen wurden (siehe Kapitel zur Datenbereinigung).

Auch wenn es sich lediglich um eine freiwillige, anonyme Online-Befragung handelt, wurden also zahlreiche Schritte unternommen, um auch in diesem besonderen Kontext gesetzliche und forschungsethische Grundlagen einzuhalten und die ‚Opsec‘ der Hacker zu jedem Zeitpunkt sicherzustellen.

Es sei nochmals hervorgehoben, dass die radikale und kompromisslose Anonymität das oberste Leitprinzip war und dem Forschenden zu keinem Zeitpunkt die Identitäten der cyberkriminellen Black Hat Hacker bekannt waren und diese - selbst unter Zwang - nicht preisgegeben werden könnten.

5.7 Durchführung der Befragung

5.7.1 Die Rekrutierung von Hackern

Es konnten während der Feldphase 1.562 abgeschlossene Befragungen realisiert werden (vor Datenbereinigung), was für diese schwierige Gruppe an Probanden eine hohe Fallzahl darstellt. Die Feldphase der Online-Befragung lief (nach ausführlicher Vorbereitung und Tests) vom 16.04.25 bis 03.07.2025. Die Zielsetzung waren mindestens 100 Hacker pro Kategorie, was deutlich überschritten wurde. Nach Datenbereinigung lag die finale Fallzahl bei 851 White Hat Hackern und 334 Black Hat Hackern, also insgesamt konnten $N = 1.185$ Hacker befragt werden, was somit eine der bisher umfangreichsten Befragung von Hackern darstellt.

Der wesentliche Beitrag dieser Arbeit zum Forschungsstand liegt in der Rekrutierung von Black Hat Hackern außerhalb des Strafvollzugs. Es handelte sich dabei um ein schwieriges Vorhaben, das bisher selten gelungen ist. Aus diesem Grund wird die Rekrutierung der Probanden im Detail beschrieben, um das Vorgehen damit transparent und intersubjektiv nachvollziehbar aufzuzeigen.

Grundbausteine der Rekrutierungsstrategie waren ein sehr kurzes Befragungsinstrument (‘5 Minute Online Study’) und Rekrutierungsvideo, Bild- und Textbeiträge, die Motive, wie Neugier, bei Hackern ansprechen und sie so von einer freiwilligen Teilnahme überzeugen sollten.

Die Herausforderung im nächsten Schritt bestand darin, mit dem erstellten Video- und Bildmaterial eine möglichst große Reichweite zu erzielen, dabei jedoch ausschließlich Black Hat Hacker und White Hat Hacker (ohne Streuverluste) zu erreichen.

Öffentliche Facebook-Posts oder Distribution über den E-Mail-Verteiler der Universität wären hierbei nicht sinnvoll, da mit großer Wahrscheinlichkeit nur Personen erreicht werden, die nichts mit dem Hacking zu tun haben und somit nicht zur Grundgesamtheit zählen.

Um die Validität der Stichprobe zu sichern, wurde der Befragungslink also *nicht* breit öffentlich verteilt, sondern so, dass nur Personen aus der Hacking-Subkultur Zugang zur Studie erhielten. Das ist eines der bedeutsamsten Qualitätsmerkmale zur Sicherstellung, dass es sich um ‚echte Hacker‘ handelt. Dies wurde über zwei Methoden realisiert: Die Distribution des Befragungslinks in spezialisierten Hacker-Foren (Forenmethode) und durch Anzeigen bei Reddit, LinkedIn oder Facebook mit Targetingparametern, die z.B. nur Personen bestimmter Berufsbezeichnungen oder Mitglieder bestimmter Telegramgruppen oder Subreddits einschließen (Anzeigen-Targeting-Methode).

Hacker-Foren im Darknet sind schwer zugänglich (Tor-Browser, komplexe passwortähnliche URLs), hochspezialisiert und widmen sich fast vollständig kriminellen Aktivitäten. Auch Telegram-Gruppen oder Hacking-Subreddits sind hochspezialisiert und Außenstehenden kaum bekannt. Die Mehrzahl der Menschen weiß weder, was das Darknet ist, noch, wie man dorthin gelangt. Der Grundgedanke ist: Wer in diesen (kriminellen) Hacker-Foren aktiv ist, ist mit an Sicherheit grenzender Wahrscheinlichkeit Black Hat Hacker oder mindestens Teil der Subkultur im weitesten Sinne.

Es lässt sich zwar nicht pauschal sagen, dass alle Personen in Hacker-Foren im Darknet Cyberkriminelle sind, doch die kriminellen Themen, Aktivitäten und kriminelle Akteure dominieren deutlich. Die Foren sind schwer zu finden, die Gefahren hoch und die technischen Hürden anspruchsvoll, sodass Hacker hier unter sich sind und erstaunlich offen kommunizieren. Bei Tor-Seiten im Darknet handelt es sich um sogenannte *Hidden Services*. Das bedeutet, die Adressen im Darknet folgen keiner intuitiven Logik oder Struktur wie herkömmliche Webseiten, die häufig in einem leicht zu merkenden Format, wie *forum-beispieladresse.de*, aufgebaut sind. Die Adressen der Hacker-Foren im Darknet ähneln eher komplexen Passwörtern, z.B. ist das der Zugangslink des XSS-Hackerforums:

<http://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/>

Hier wird ersichtlich, dass es kaum möglich ist, sich diese Zugangs-URL intuitiv zu merken. Die Seite an sich fungiert also in gewisser Weise selbst wie ein Passwort. Nur wer den

konkreten Zugangslink besitzt, kann den *Hidden Service* aufrufen. Es ist zudem erneut darauf hinzuweisen, dass *Hidden Services* im Tor-Netzwerk auf *.onion* enden und nicht über normale Browser erreichbar sind, sodass es nicht möglich ist, aus Versehen durch einen falschen Klick im Darknet zu landen. Kombiniert man diese hohen technischen Hürden mit der Tatsache, dass *Google* im Darknet nicht existiert, wird ersichtlich, dass der Aufwand, diese Darknet-Foren zu finden und zu besuchen, relativ hoch ist. Es ist daher nicht anzunehmen, dass Unbeteiligte außerhalb der Subkultur sich in diesen Bereich des Internets verirren. Ausnahmen könnten FBI-Agenten, andere Forscherinnen und Forscher oder Investigativjournalisten sein, die aber kein Interesse daran haben dürften, akademische Forschung zu verfälschen.

Durch eine Google- und KI-Recherche zu Begriffen wie *Cyber Threat Intelligence* wurden die derzeit aktivsten und relevantesten Hacker-Foren identifiziert. Die Fluktuation in diesem Bereich ist hoch. *RaidForums* war eines der größten englischsprachigen Black-Hat-Foren und wurde vom FBI und weiteren Strafverfolgungsbehörden geschlossen; als Alternative etablierte sich *BreachForums*, das jedoch nach der Festnahme des Betreibers ebenfalls abgeschaltet wurde. Unter dem Titel ‚Breachform‘ (statt *BreachForum*) wurde wiederum eine von zahlreichen Alternativen gegründet. Auch diese Seite ging im Erhebungszeitraum wieder offline. Diese hohe Fluktuation von Hacker-Foren ist ein sich wiederholendes Muster, das einerseits auf erfolgreiche Maßnahmen der Strafverfolgungsbehörden zurückzuführen ist, andererseits aber auch auf die Resilienz der cyberkriminellen Akteure, die dieselben Strukturen unter neuem Namen neu aufbauen.

In identifizierten Darknet-Foren wurde nach weiteren Forenempfehlungen gefragt. Diese Hinweise von Hackern führten zu weiteren Foren, in denen wiederum nach weiteren Foren gefragt wurde, bis sich der Kreis zunehmend schloss. Auf diese Weise konnte im Sinne eines Schneeballsystems eine Liste aktiver Plattformen zusammengestellt werden, darunter Darknet- und Clearnet-Foren, hackingspezifische Subreddits sowie Telegram-Gruppen. Die Selektion der Hacker-Foren für die Stichprobenziehung basierte primär auf den Kriterien der

Relevanz und Verfügbarkeit, wobei auch rechtliche Aspekte und die Sprache des Forums eine Rolle spielten.

Einige Administratoren der Hacker-Foren im Darknet verlangen einen Beweis, ‚einer von ihnen‘ zu sein, um Zugang zu den Foren zu bekommen. So verlangt etwa das Hacker-Forum *Exploit.in* Belege über eigene Hacks oder eine Reputation als Hacker aus anderen einschlägigen Foren. Derartige Eintrittsbarrieren mögen für verdeckte Ermittler von Strafverfolgungsbehörden überwindbar sein, sind aber für Forschungszwecke ethisch, rechtlich und moralisch unvertretbar. Es wurde sich ausdrücklich zu keinem Zeitpunkt als Hacker ausgegeben (keine Undercover-Recherche), sondern immer klar, transparent und offen kommuniziert, dass es sich um ein akademisches Forschungsvorhaben handelt. Außerdem wurden lediglich Hacker-Foren gewählt, die sich auf das Hacking beschränken und strikt Inhalte zu Drogen, kinderpornografische Inhalte und Diskussionen zu Waffenhandel ohne jegliche Ausnahmen unterbinden (siehe Kapitel 5.6).

Auch die Sprachbarriere spielte bei der Auswahl der Hacker-Foren eine zentrale Rolle. Viele der Foren und Telegram-Gruppen sind russischsprachig. Zwar wurde in Einzelfällen auch dort in russischer Sprache nach Teilnehmenden gesucht, der Fokus lag jedoch bewusst auf englischsprachigen Hacker-Communities, aus praktischen Gründen der Kommunikation, da auch die Erhebung auf Englisch durchgeführt wurde. Neben dem Darknet spielen auch Clearnet-Foren und Messenger-Dienste, wie Telegram, Discord, Reddit und Github, eine wichtige Rolle in der Subkultur.

Insgesamt wurden Probanden gesucht in:

- 8 Hacker-Foren und Netzwerken im Darknet (BlackHatChat, Best Carding World, Breachform, CryptBB, DarknetArmy, Defcon Dark, Dread und Pitch)
- 7 Hacker-Foren im Clearnet mit eindeutig kriminellem Fokus (crashed.sh, hackforums, lolz.live, nulledBB, patched.to, sinister.ly und xforums.st)

- 13 Auftragshacker im Darknet wurden direkt per Darknet-Kontaktformular oder anderen verschlüsselten, anonymen Kommunikationsmitteln kontaktiert
- 17 einschlägige Telegram-Gruppen wurden selektiert und Mitglieder direkt kontaktiert und zur freiwilligen Teilnahme eingeladen
- 10 hacking- und darknetbezogene Subreddits wurden targetiert
- 5 Ethical Hacking- und Cybersecurity-Gruppen bei LinkedIn wurden targetiert
- Werbeanzeigen bei Reddit (hochpräzises Targeting, ausgerichtet auf Black- und White Hats durch Mitgliedschaft in hackingbezogenen Unterforen)
- Bannerwerbung bei 4chan im *Technology Board* (beliebt in der Hacking-Subkultur)

Bezahlte Werbeanzeigen wurden eigenständig und ohne Drittmittel finanziert. Die Entscheidung für bezahlte Werbung war methodischer Natur, da bei bezahlten Anzeigen ein präzises Targeting möglich ist. Das heißt, der Werbetreibende kann aus unzähligen Parametern auswählen, wer das entsprechende Video ausgespielt bekommen soll und wer nicht. Die Beiträge sind demnach nicht breit öffentlich sichtbar, sondern werden lediglich an die zuvor definierte Zielgruppe ausgespielt. Bei Reddit beispielsweise ließ sich bestimmen, dass das Rekrutierungsvideo nur Personen angezeigt werden soll, die z.B. aktives Mitglied in der Gruppe *r/hacking* sind. Auch dieser Rekrutierungsweg ist der Forenmethode sehr ähnlich, da auch hier die Mitgliedschaft in bestimmten Hacking-Unterforen die Voraussetzung dafür war, den Zugangslink zur Studie angezeigt zu bekommen.

Die Grundgesamtheit sind alle White- und Black Hat Hacker gemäß der genannten Definition.

Bewusst ausgewählt wurden also relevante und aktive Foren, Subreddits und Telegram-Gruppen; innerhalb dessen erfolgte dann eine Selbstselektion.

Es handelt sich folglich um eine nicht-probabilistische Stichprobenziehung, bei der keine Zufallsauswahl erfolgte, sondern die Teilnehmer auf Basis ihrer Selbstselektion innerhalb

gezielt ausgewählter Hacker-Foren und Communities in die Studie aufgenommen wurden. Im Diskussionsteil werden mögliche Effekte dieser Selbstselektion kritisch gewürdigt.

Zwecks intersubjektiver Nachvollziehbarkeit wird die Probandengewinnung im Clear- und Darknet im Folgenden im Detail aufgeführt. Hierzu werden die entsprechenden Foren oder Netzwerke kurz beschrieben sowie die Texte und Targetingparameter offengelegt, mit denen Probanden gesucht wurden. Bei den genutzten Darknet-Foren handelt es sich um Seiten, die ausschließlich über das Tor-Netzwerk (Darknet) zugänglich sind. Sofern möglich, wurden die Gesuche nach Abschluss der Feldphase aus den Darknet-Foren und sozialen Medien gelöscht, um die eigenen Daten (und das eigene Gesicht in einigen Fällen) nicht länger als unbedingt nötig online zu belassen.

Darknetarmy hat nach eigener Forenstatistik zum Erhebungszeitpunkt über 78.000 Mitglieder und über 24.000 Threads (Diskussionsbeiträge) und wirbt mit dem untenstehenden Slogan (Abb. 24), Zugang zu tausenden Hacking-Werkzeugen zu gewährleisten, von gestohlenen Daten über Carding-Tools, Zugang zu Netflix-Accounts bis hin zu Ransomware- und Malware-Builders.

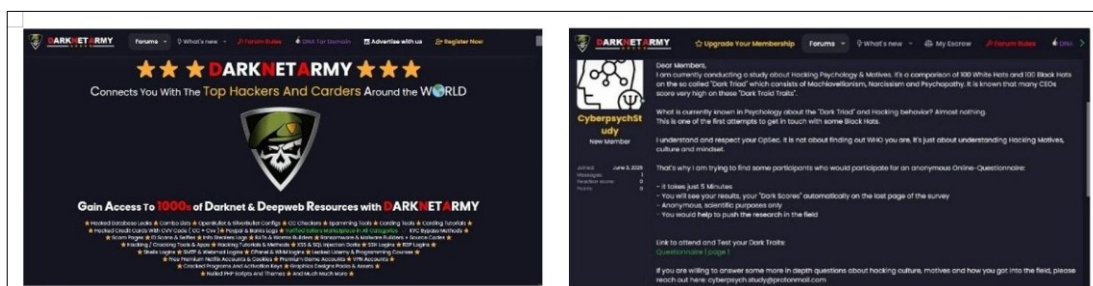


Abbildung 24. Screenshot Hacker-Forum DarknetArmy (2025) (Darknet)

CryptBB befasst sich als Forum mit Hacking, Carding, Fraud, Datenleaks, Malware-Entwicklung und weiteren Diskussionen über das Darknet und ist derzeit ein beliebtes Ziel für Fortgeschrittene und Anfänger.

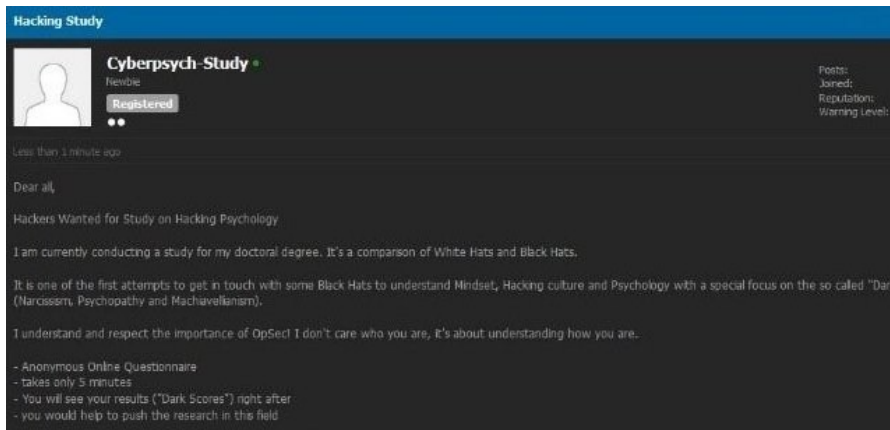


Abbildung 25. Screenshot Hacker-Forum CryptBB (2025)

Dread ist ein 2018 gegründetes Darknet Forum und eine der derzeit bekanntesten Anlaufstellen zum anonymen Austausch zu Themen des Hackings und wird in der Szene häufig als ‚Reddit des Darknets‘ bezeichnet. Dread ist (wie Reddit) eine Mischung aus Diskussionsforum und sozialem Netzwerk mit Mitgliederzahlen von rund 482.000 Nutzern (Stand 2025). Nach Selbstbeschreibung ist Dread eine „online based free speech platform and forum“ (Dread, 2025b). Struktur und Optik der Seite erinnert an Reddit, wobei einige Subforen und Kategorien sich wenig subtil mit strafbaren Inhalten befassen (d/DarkNetMarkets, 172.000 Mitglieder, d/fraud, 108.000 Mitglieder). Beliebte Hacking-Subforen sind d/carding (93.000 Mitglieder) oder d/SocialEngineering (62.000 Mitglieder).

Pitch wurde 2021 gegründet als Social-Media Plattform, die exklusiv über das Tor-Netzwerk (Darknet) zu erreichen ist. Pitch erinnert in Struktur und Aufbau an X (vormals Twitter) und wird auch in der Szene als ‚Twitter des Darknets‘ bezeichnet. Die genaue Mitgliederzahl von Pitch ist unbekannt, doch Administratorenaccounts wie @pitch haben rund 18.000 Follower und einige der populärsten Accounts rund 2000 Follower (Stand 2025). Es ist, verglichen mit Dread, eine deutlich kleinere, aber aktive Community. Gerade bei Pitch ist zu betonen, dass dies erst einmal nur ein soziales Netzwerk mit starker Verschlüsselung und Anonymität ist. Alle Black Hat Hacker haben ein Interesse, anonym zu sein, aber nicht alle, die ein Interesse haben, anonym zu sein, sind Black Hat Hacker.



Abbildung 26. Screenshot Darknet-Netzwerk Pitch (2025)

Auch im Clearnet (Definition siehe Kapitel 2.2.3) wurden relevante Foren identifiziert und für die Probandengewinnung genutzt:

Cracked.sh ist ein Hackingforum, das Cracking-Tutorials, Hacking Werkzeuge, Datenleaks und einen Marktplatz anbietet. Nach selbstveröffentlichter Statistik (Stand 2025) zählt das Forum 4,72 Mio. registrierte Nutzer und 1,27 Mio. Threads (veröffentlichte Diskussionsthemen). Cracked.sh setzt Aktivitäten von cracked.io nach behördlicher Abschaltung fort.

nulledBB.com ist ein Forum, das sich ebenfalls mit dem Handel und der Veröffentlichung von Datenlecks befasst, aber auch andere Social Engineering und Technologiethemen abdeckt. Es zählt nach selbstveröffentlichter Statistik (Stand 2025) 721.000 Mitglieder und 279.000 Beiträge.

patched.to hat nach eigener Statistik (Stand 2025) über 541.000 Mitglieder und ca. 160.000 Threads (Diskussionsthemen). Fokusthemen sind Hacking, Cracking, Computerspiele und Kryptowährungen, aber auch das persönliche Leben, Entertainment und Filme/Serien gehören zu den diskutierten Themen.

xforums.st ist ein kleineres, aber wachsendes Forum mit Themen wie Hacking, Cracking, Spamming und Carding (Kreditkartenbetrug). Es zählt nach eigener Statistik (Stand 2025) 4200 Mitglieder und 183.000 Threads.

Hackforums.net besteht seit 2007 und ist thematisch breit gestreut von Hacking-Themen bis Coding, Computerspielen oder Kryptowährungen.

Lolz.live ist ein großes, russischsprachiges Hacker-Forum mit 6,98 Millionen Mitgliedern nach eigenen statistischen Angaben (Stand 2025) und 5,98 Millionen Diskussionsbeiträgen rund um Themen des Hackings, Crackings und der Programmierung.

sinister.ly ist bzw. war ein Hackingforum, das besonders bei Personen beliebt ist, die sich mit dem Social Engineering befassen, also dem Manipulieren von Menschen. Während noch am 16. Juni 2025 auf sinister.ly ein Gesuch gepostet wurde, ist das Forum (Stand 2025) aus unbekannten Gründen offline und wurde wahrscheinlich von Strafverfolgungsbehörden abgeschaltet.

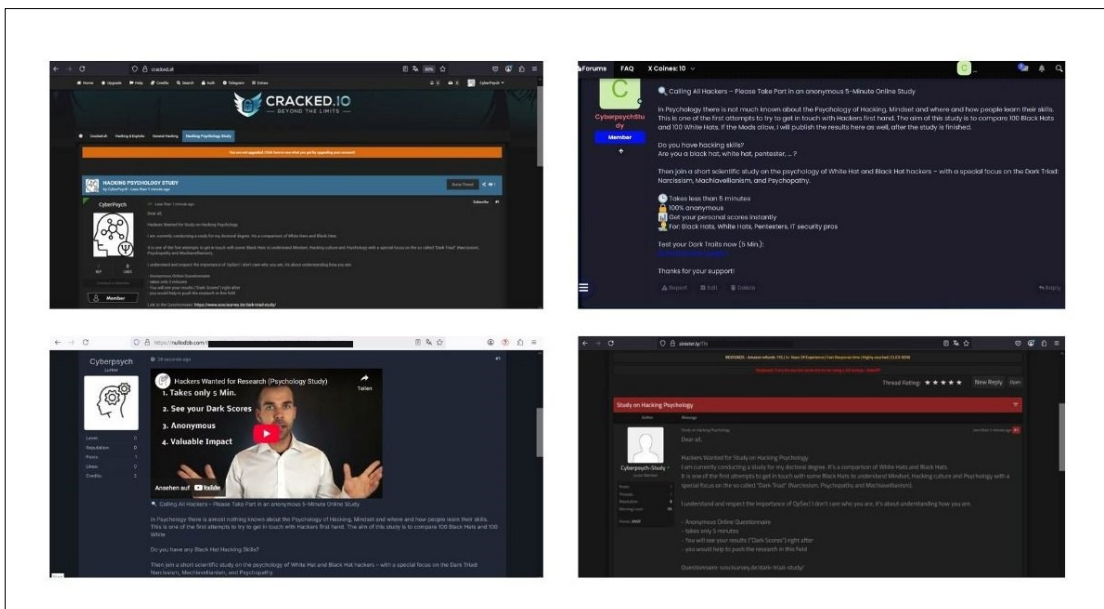


Abbildung 27. Screenshots Clearnet Hacker-Foren

Quellen: Cracked (2025), NulledBB (2025), SinisterLY (2025)

Mitglieder in Telegram-Gruppen

Telegram ist eine Messenger-App, ähnlich wie WhatsApp, die jedoch besonders für Privatsphäre und Anonymität bekannt ist und sich somit auch bei Kriminellen großer Beliebtheit erfreut, weshalb die BBC Telegram als „The dark web in your pocket“ (Tidy, 2024) beschrieb. Diese mediale Beschreibung deckt sich mit der Feststellung des Bundeskriminalamtes im Bundeslagebild Cybercrime 2024. Unter den relevanten

Phänomenbereichen wird Telegram explizit als integraler Bestandteil der Dark Economy genannt:

„Gemeinsamer Nenner der meisten Bedrohungen im Cyberraum ist die Underground Economy. [...] Dabei beschränken sich Anbieter längst nicht mehr nur auf Darknet-Marktplätze, um ihre jeweiligen Waren zu vertreiben. Auch Messenger-Dienste wie Telegram gehören mittlerweile zu etablierten Verkaufsplattformen.“ (BKA, 2025a, S. 10)

Es wurden über eine Recherche zu *Cyber Threat Intelligence* 16 Telegram-Gruppen identifiziert und einzelne Mitglieder zur Teilnahme eingeladen, teils russischsprachig, teils englischsprachig. Ein Tracking, bei dem einzelne Klicks Mitgliedern zugeordnet werden können, fand nicht statt. Die ausgewählten Telegram-Gruppen waren Anonsec, Lazarus Group, Ghostsec, UserSec, Killnet, Mirai, Xaknet, From Russia with Love, BearITArmy, Darknet, Darkforums, DDoS Services, Official Dumped.to Channel, Malware Forums, Redstresser (Meris Botnet) und Breachforums Chat. Die kombinierte Mitgliederzahl der Gruppen zum Erhebungszeitraum war 38.566. Abbildung 28 zeigt Bildschirmaufnahmen einzelner Telegram-Gruppen.

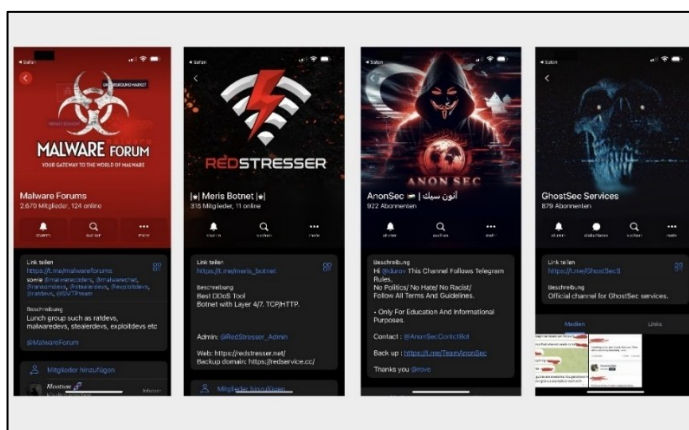


Abbildung 28. Screenshots Telegram-Hackergruppen

Quellen: Telegram-Gruppen: MalwareForums (2025), MerisBotnet (2025), AnonSec (2025), GhostSec (2025)

Hacking-Subreddits

Innerhalb der Hacking-Subkultur sind X (früher Twitter) und Reddit beliebte soziale Netzwerke, sowohl bei Black Hat Hackern als auch bei White Hat Hackern. Entsprechende Hacking-Subreddits haben - Stand 2025 - oft hunderttausende bis mehrere Millionen Mitglieder, z.B. *r/darknet* (361.501 Mitglieder) oder *r/malware* (86.881 Mitglieder). Es existieren auch schwerpunktmäßige White-Hat Communities wie *r/ethicalhacking* (53.673 Mitglieder). Das Rekrutierungsvideo und der Befragungslink wurden in dreizehn relevanten Hacking-Subreddits verbreitet.

Um die Reichweite weiter zu erhöhen, wurden ebenfalls bezahlte Anzeigen bei Reddit geschaltet, jedoch ausschließlich sichtbar für Mitglieder der nachfolgenden abgebildeten Hacking-Subreddits (Abbildung 29). Diese Gruppen sind thematisch und technisch so spezialisiert, dass davon ausgegangen werden darf, dass Gruppemitglieder Teil der Hacking-Community sind (also White- oder Black Hats) oder mindestens starkes Interesse am Einstieg in diese Themenfelder haben. Innerhalb von rund 3 Monaten erzielte der Beitrag so über 460.000 Ansichten. Das bedeutet nicht, dass das Video 460.000 Mal angesehen wurde, es bedeutet aber, dass der Beitrag einer entsprechenden Anzahl an Nutzern angezeigt wurde.

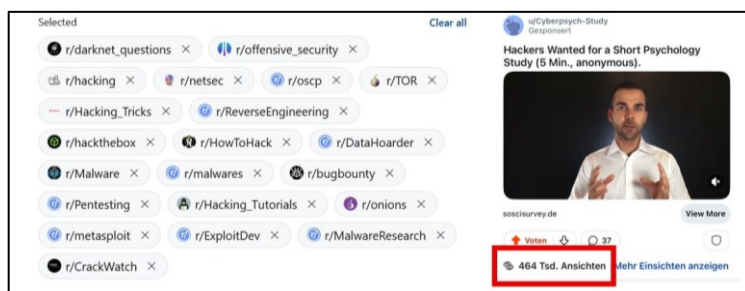


Abbildung 29. Screenshot Login-Bereich: Targeting Reddit Hacker-Foren (Subreddits)

4chan

Chiesa et al. (2009) nennen als eines der Kernergebnisse ihrer Untersuchung von Hackern „They rebel against all symbols or expressions of authority“ (2009, S. XXII). Auch in anderen empirischen Untersuchungen (z.B. Gaia et al., 2021) ist das Ablehnen von Autoritäten ein

sich wiederholendes Motiv. 4chan ist ein anonymes und selbstverwaltetes Imageboard. Da kein Konzern, wie Meta, hinter dem Netzwerk steht, sind die Inhalte oft unregulierter und unzensurierter, als dies in anderen sozialen Medien üblich ist. 4chan ist beliebt in der Hacking-Subkultur, z.B. das Hackerkollektiv Anonymous ist aus 4chan heraus entstanden (Stryker, 2011). Insbesondere die Unterseite */g/ - Technology* behandelt Hacking- und Technologiethemen. Es wurde für fünf Tage im 4chan Technology-Board (<https://boards.4chan.org/g/>), beginnend am 18. Mai 2025, die abgebildete Bannerwerbung geschaltet (Abb. 30).

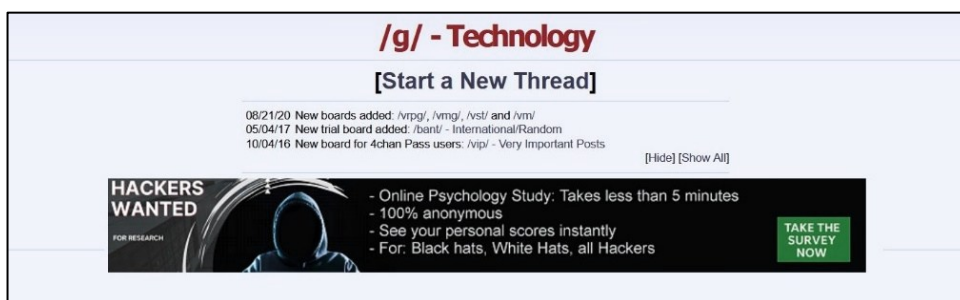


Abbildung 30. Screenshot Bannerwerbung Imageboard 4chan (2025)

Rekrutierungsmethode: Berufsbezeichnung

White Hat Hacker agieren legal und sind auf Plattformen wie LinkedIn unter Berufsbezeichnungen wie *Ethical Hacker*, *Sicherheitsforscher* oder *Penetrationstester* auffindbar. Dadurch ergaben sich Rekrutierungsmöglichkeiten, die bei Black Hats nicht möglich wären. Über LinkedIn und Facebook wurden gezielt Personen mit entsprechenden Berufsbezeichnungen über Anzeigen targetiert. Zudem wurde ein Vortrag auf einer Cybersecurity-Messe in Berlin (die GITEX 2025) genutzt, um White Hats zur Studienteilnahme einzuladen. Ergänzend kamen Kontakte aus dem eigenen beruflichen Netzwerk zum Einsatz.

LinkedIn

Je anonymere eine Plattform ist, desto deutlicher die Black Hat-Affinität der Nutzer und Themen. Je weniger anonym eine Plattform ist, desto mehr geraten Black Hat-Themen und -Nutzer in den Hintergrund oder geben sich zumindest nicht mehr als solche zu erkennen. Während Darknet-Foren in der Hand der Black Hat Community liegen, dominieren auf LinkedIn Cybersecurity-Spezialisten, die ihre Qualifikationen unter Klarnamen präsentieren.

LinkedIn war bei der Probandengewinnung vor allem ein Werkzeug, um White Hat Hacker zu rekrutieren. Teilnahmeaufrufe wurden im eigenen Netzwerk (über 3.200 Kontakte, Mehrzahl aus den Branchen IT- und Cybersicherheit), sowie in fünf großen LinkedIn-Gruppen mit White Hat Bezug geteilt:

- Cybersecurity and Artificial Intelligence (AI) Frameworks and Maturity Models (> 304.000 Mitglieder)
- CYBER SECURITY FORUM INITIATIVE - CSFI (> 659.000 Mitglieder)
- CyberSecurity Community (> 275.000 Mitglieder)
- Ethical Hacking | Kali Linux (> 1.800 Mitglieder)
- IT Specialist Cybersecurity Network (> 114.000 Mitglieder)

Zusätzlich wurden über LinkedIn mehrere Werbekampagnen geschaltet, die gezielt Personen mit White-Hat-Berufsbezeichnungen oder entsprechenden Kenntnissen im Bereich Cybersecurity ansprachen. Dabei wurden internationale wie auch deutschsprachige White Hat Hacker adressiert. Insgesamt führten die Kampagnen zu 578 Klicks auf den Befragungslink.

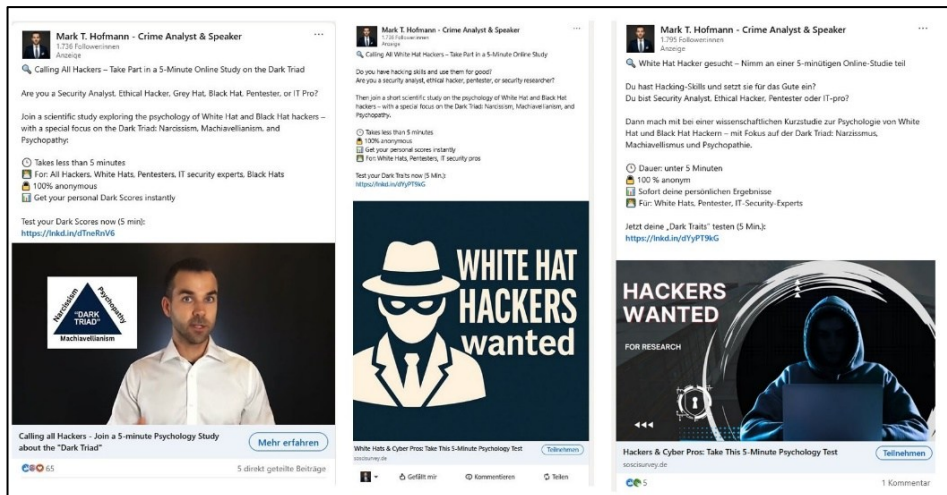


Abbildung 31. Screenshot LinkedIn Probandengewinnung

Quelle: LinkedIn (2025), Unternehmensseite Mark T. Hofmann

Facebook

Es wurde auf öffentliche Facebook Posts verzichtet, da die Streuung zu groß wäre und kaum Personen der eigentlichen Grundgesamtheit erreicht würden. Es wurde jedoch eine bezahlte Anzeige mit dem Rekrutierungsvideo und den folgenden Targetingparametern geschaltet: Alle Länder, alle Geschlechter, ab 18 Jahre, mit mindestens einer der folgenden Interessen: Certified Ethical Hacker, Computersicherheit (Computer und Elektronik), DefCon⁷, Hackernews⁸, Hackathon⁹. Es konnten 3.535 Klicks auf den Befragungslink verzeichnet werden, wovon jedoch nur ein kleiner Teil tatsächlich an der Befragung teilgenommen hat.

Direktkontakte, Unternehmenskontakte, Vortrag GITEX Europe

Am 22. Mai 2025 fand auf dem Messegelände Berlin die Cybersecurity Messe GITEX Europe statt. Besucher sind hier vor allem Cybersecurity-Verantwortliche von Unternehmen. Im Rahmen eines eigenen Vortrages wurde dazu aufgerufen, dass White- und Black Hat Hacker an der Befragung teilnehmen können und der Befragungslink als QR-Code gezeigt. Zusätzlich wurden Personen aus dem eigenen beruflichen Netzwerk direkt eingeladen.

⁷ DefCon ist eine bekannte Hackerkonferenz (Veranstaltung).

⁸ The Hacker News (www.thehackernews.com) ist ein Online Medium, die Facebook Seite hat 1,8 Mio. Gefällt-Mir-Angaben (Stand 2025).

⁹ Wortneuschöpfung aus ‚Hacking‘ und ‚Marathon‘, die Hacking Wettbewerbe beschreibt.

(ausschließlich White Hat Hacker) und eigene persönliche Unternehmenskontakte wurden gebeten, den Befragungslink an ihre internen Cybersecurity-Abteilungen weiterzuleiten.

5.7.2 Rücklaufstatistik und Plausibilitätscheck

Über SoSci-Survey wurden im Befragungszeitraum 126.380 Klicks registriert, wobei diese Zahl wenig aussagekräftig ist, da dies doppelte Klicks und Zugriffe von Suchmaschinen und Bots beinhaltet. 2287 Personen haben die Online-Befragung gestartet (ab Seite 2 nach erfolgter Einwilligung) und 1403 Teilnehmer haben die Befragung vollständig bis zur letzten Seite abgeschlossen (= 61,35 %).

Als gültige Fälle ($N = 1.562$) wurden alle Teilnehmer definiert, die mindestens Seite 5 des Fragebogens abgeschossen haben (= 68,3 %), dies beinhaltet die grundlegenden soziodemografischen Angaben und die *Short Dark Triad*, also die Mindestinformationen zur Beantwortung der Hauptforschungsfragen.

Die Abbruchquote liegt mit 31,7 % bei rund einem Drittel, was zwar hoch ist, jedoch bei diesen sensiblen Themen und dieser speziellen Stichprobe wahrscheinlich unvermeidlich ist. Während der Feldphase konnten $N = 1.562$ abgeschlossene Befragungen realisiert werden (vor Datenbereinigung).

Bei SoSci-Survey können Befragungslinks mit Trackingparametern versehen werden (z.B. ,?r=1'), die später als Variable im Datensatz erscheinen. Ein Versuch, damit die Herkunft aus verschiedenen Foren zu erfassen, scheiterte jedoch, da Hacker diese Zusätze sofort erkannten und misstrauisch reagierten.

Es kam zudem zu Vorwürfen, dies sei keine Studie, sondern eine angebliche Geheimdienst-Operation. Im Zuge dessen wurde durch einen Hacker die Büroadresse und Identität des Forschenden im Darknet veröffentlicht. Diese Praxis nennt sich *Doxxing*. (Siehe Kapitel 5.11.1 zu sonstigen Felderfahrungen).

Ein exaktes Tracking, welche Klicks aus welcher Quelle kamen, fand nicht statt.

Stattdessen erstellt die Software SoSci-Survey automatisch eine Rücklaufstatistik. Sie zeigte im Erhebungszeitraum deutliche Wellen, die zeitlich mit Postings in verschiedenen Foren übereinstimmten. Nach Postings in Hacker-Foren war ein stärkerer Zustrom von Black Hats zu verzeichnen, während nach Postings oder Anzeigen auf LinkedIn ein stärkerer Zustrom von White Hats zu verzeichnen war. Eine klare Abgrenzung oder Schwarz-Weiß-Kategorisierung war jedoch nicht erkennbar, und besonders Reddit und Facebook scheinen einen Graubereich darzustellen und sowohl bei Black Hat Hackern als auch White Hat Hackern beliebt zu sein. Dennoch stützte die Rücklaufstatistik insgesamt die Plausibilität der Selbstzuschreibungen als Black Hat bzw. White Hat.

5.8 Datenbereinigung

Als Auswahlkriterium für gültige Fälle in der Software SoSci-Survey galten alle Interviews (nach Pretest), bei denen der Online-Fragebogen mindestens bis einschließlich Seite 5 vollständig bearbeitet wurde. Dieser Abschnitt umfasst die grundlegenden soziodemografischen Angaben, die Gruppenzugehörigkeit (Black Hat oder White Hat) sowie das Instrument der Short Dark Triad (SD3). Insgesamt erfüllten 1.562 Fälle diese Kriterien.

Im Rahmen der Datenbereinigung wurden zuerst eigene Testläufe ausgeschlossen ($n = 6$).

Ebenfalls wurde die Gruppe der Nicht-Hacker ausgeschlossen ($n = 338$). Neben den Auswahlmöglichkeiten ‚Black Hat Hacker‘ und ‚White Hat Hacker‘ bot der Fragebogen die dritte Antwortkategorie „I have nothing to do with any form of Coding, Hacking or Cybersecurity“. Da der Link ausschließlich in Hacking-Communities verbreitet wurde, haben sich 80 % der Teilnehmer selbst der Gruppe der White Hats oder Black Hats zugeschrieben, rund 20 % ($n = 338$ Fälle) haben angegeben, nichts mit dem Hacking oder der Cybersicherheit zu tun zu haben. Zwar ist davon auszugehen, dass hierin einige Black Hat Hacker enthalten sind, die dies aus Sicherheitsbedenken nicht selbst angeben möchten, jedoch kann dies nicht einfach angenommen werden. Es ist nicht eindeutig klar, ob diese Personen tatsächlich nichts mit dem Hacking zu tun haben oder welcher Gruppe sie zuzuordnen sind, weshalb diese Fälle vollständig ausgeschlossen wurden. Die

durchschnittliche Bearbeitungszeit der Fälle nach Datenbereinigung ($n = 1194$) betrug 497 Sekunden ($SD = 211$), also ca. 8 Minuten und 17 Sekunden. Einige Fragen wurden nur Black Hats angezeigt, sie hatten also eine längere Fragebogenversion als White Hat Hacker.

Durch eigene Tests wurden 2 Minuten (selbst bei der kürzeren Fragebogenversion) als minimal nötige Bearbeitungszeit definiert. Wer den Fragebogen in unter 2 Minuten durchgeklickt hat, kann weder die Anweisungen noch die Items in der Zeit gelesen und wahrheitsgemäß beantwortet haben. Fälle mit einer Bearbeitungszeit unter 120 Sekunden wurden daher ebenfalls ausgeschlossen ($n = 14$).

Im nächsten Schritt wurden ‚Fake-Klicks‘ identifiziert, also Teilnehmer, die beispielsweise bei *allen* 27 Fragen der SD3 unabhängig vom Inhalt immer die 5 (= höchstmögliche Ausprägung) oder immer die 1 (= niedrigstmögliche Ausprägung) angeklickt haben. Da einige Items der Short Dark Triad und auch der LSRP reverse-codiert sind, waren diese Fälle relativ leicht im Datensatz zu identifizieren und wurden ausgeschlossen ($n = 10$).

Da eine Selbstselektion stattfand, konnte nicht kontrolliert werden, Personen welchen Alters an der Befragung teilnehmen. Gemäß der Richtlinie der DGOF können Personen ab 14 ohne Einwilligung der Eltern anonym online befragt werden. Fälle, die 13 oder jünger waren, wurden gelöscht und nicht in die Analyse einbezogen. Dies betraf jedoch lediglich 9 Fälle (also 0,75%).

Reverse-codierte Items wurden umcodiert, Subskalenmittelwerte als neue Variablen berechnet und uneinheitliche Schreibweisen zur Nationalität (z. B. „germany“, „German“, „DE“) in eine einheitliche englische Schreibweise überführt.

5.9 Beschreibung der Stichprobe

Nach der Datenbereinigung verblieben 1.185 gültige Fälle, bestehend aus einer Stichprobe von 334 Black Hat Hackern und 851 White Hat Hackern.

Überwiegend männlich

91,6 % der befragten Hacker ($N = 1.185$) gaben an, männlich zu sein, während lediglich 8,4 % weiblich waren. In der Gruppe der White Hats lag der Männeranteil mit 92,4 % etwas höher als bei den Black Hat Hackern, bei denen 89,5 % männlich waren. Diese eindeutige Geschlechterverteilung deckt sich exakt mit dem bestehenden empirischen Forschungsstand, wie in Kapitel 3.3 beschrieben. So berichtet auch das Bundeskriminalamt (2015b, S. 10) in einer Literaturanalyse von Männeranteilen zwischen 76 % und 94 % über verschiedene Studien hinweg.

Diese Übereinstimmung stellt einen wichtigen Validitätsindikator dar, sie spricht dafür, dass die Teilnehmer, einschließlich der Black Hats, ihre Angaben weitgehend wahrheitsgemäß gemacht haben. Wäre der Frauenanteil hingegen deutlich höher als die Referenzwerte der Literatur ausgefallen, hätte dies Zweifel an der Datenqualität bzw. an der Authentizität der Antworten nahegelegt.

Mehrheit unter 28 Jahre alt

Das Alter wurde zum Schutz der Identitäten nicht exakt, sondern in Blöcken von je 5 Jahren erfasst. Die Fälle im Alter von 13 Jahren oder jünger ($n = 9$) wurden ausgeschlossen.

Die Altersverteilung über beide Gruppen hinweg ($N = 1.185$) zeigt deutlich, dass Hacker mehrheitlich jung sind (83,1 % in der Altersspanne 14-37). Mehr als die Hälfte der Teilnehmer (53 %) gab an, unter 28 zu sein. Es zeigten sich hier jedoch erkennbare Unterschiede in der Altersverteilung der Black Hats (links) und White Hats (rechts).

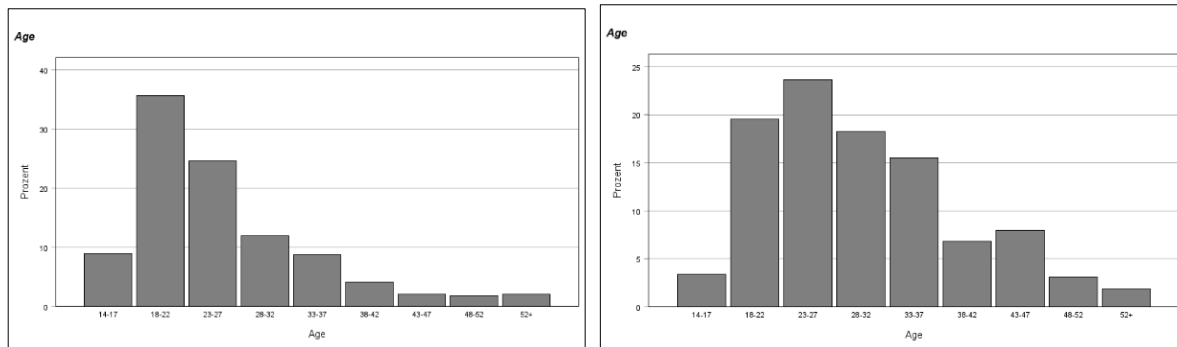


Abbildung 32. Histogramme Altersverteilung in Prozent

Anmerkung. $n = 334$ Black Hats (l.) und $n = 851$ White Hats (r.)

In der Gruppe der Black Hat Hacker ($n = 334$) stellt die Altersgruppe der 18- bis 22-Jährigen mit 35,6 % den größten Anteil dar. Insgesamt sind 69,2 % der Black Hats unter 28 Jahre alt. Die Altersverteilung der Hackergruppen deckt sich somit mit den empirischen Ergebnissen von Chiesa et al. (2009, S. 74), die ebenfalls feststellten, dass 80 % der Probanden ($N = 553$) unter 30 waren. Auch das Bundeskriminalamt resümiert zum Alter von Hackern, es sei „von einer in hohem Maße jungen Hackerpopulation auszugehen“ (BKA, 2015b, S. 8). Bei den White Hat Hackern ($n = 851$) ist die Altersgruppe der 23- bis 27-Jährigen mit 23,6 % am stärksten vertreten. Insgesamt sind 46,5 % der White Hats unter 28 Jahre alt.

Dass die Stichprobe der White Hat Hacker im Gesamtbild etwas älter ist als die der Black Hats, dürfte wahrscheinlich keine Verzerrung darstellen, sondern vielmehr eine realistische Abbildung der Grundgesamtheit. White Hat Hacker sind häufig als Sicherheitsforscher, Pentester oder anderweitig in der Cybersicherheitsbranche tätig, also Berufsfelder, die in der Regel eine gewisse Ausbildung, Berufserfahrung und damit ein höheres Alter voraussetzen. Mit 15 ist es (noch) nicht möglich, entsprechende Positionen in Unternehmen zu besetzen.

Zudem ist es plausibel oder zumindest nicht ausgeschlossen, dass viele White Hats in ihrer Jugend selbst Regeln gebrochen haben (Black Hats waren), bevor sie sich später für einen legalen Weg entschieden. Umgekehrt ist es denkbar (und zu hoffen), dass ein Teil der heutigen jungen Black Hats mit zunehmendem Alter den Übergang in legale Tätigkeitsfelder und entsprechende Karrieren vollzieht.

Gut gebildet

In Übereinstimmung mit den beobachteten Altersunterschieden zwischen Black- und White Hats variiert auch der höchste abgeschlossene akademische Grad zwischen den Gruppen (siehe Abbildung 33).

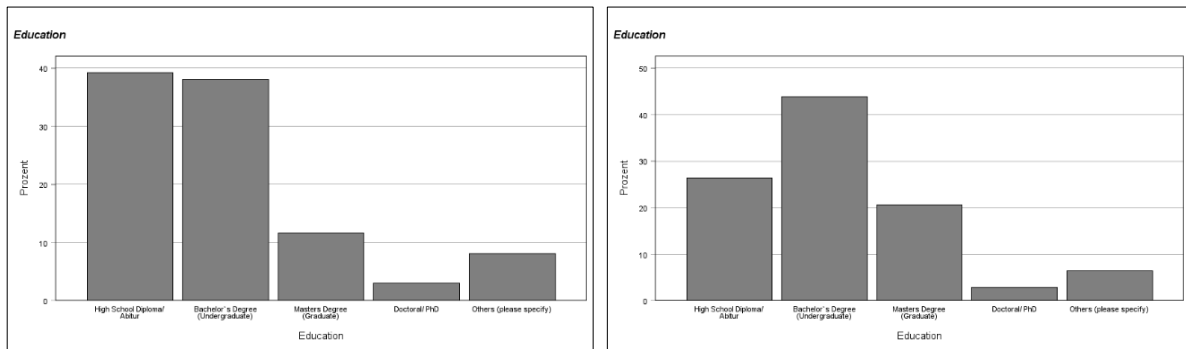


Abbildung 33. Histogramm akademischer Abschluss in Prozent

Anmerkung. $n = 334$ Black Hats (l.) und $n = 851$ White Hats (r.)

In der Gruppe der Black Hats haben 39,2 % Abitur bzw. High School abgeschlossen, 38 % einen abgeschlossenen Bachelor und mit deutlichem Abstand nur 11,7 % einen Masterabschluss. In der Gruppe der White Hats sind es mit 20,6 % fast doppelt so viele Masterabsolventen. Auch wenn die Gruppe der White Hats (bedingt durch das leicht höhere Alter) auf dem akademischen Weg leicht fortgeschritten ist, ist insgesamt bei Hackern von einem hohen Anteil an Akademikern auszugehen und solchen, die auf dem Weg dahin sind.

93,2 % aller Hacker ($N = 1.185$) gaben an, entweder ein Abitur (30 %), Bachelor (42,2 %), Master (18,1 %) oder ein Doctoral Degree/PhD (2,9 %) abgeschlossen zu haben.

6,9 % wählten die Freitextoption ‚Sonstiges‘ und trugen hier meist Computerkurse, Selbststudium, Schulabbruch oder andere Zusatzangaben ein (z.B. „Industry relevant certifications“, „Middle school“, „Highschool dropout“, „Almost finished with MSc“, „Intelligence school pensacola FL“¹⁰). Es ist zudem hervorzuheben, dass nach dem höchsten

¹⁰ Bezieht sich auf das *Center for information Warfare Training in Pensacola, FL* der US Navy <https://www.netc.navy.mil/CIWT/>.

abgeschlossenen Grad gefragt wurde, sodass einige *noch* kein Abitur/High School Diploma haben, es aber voraussichtlich noch erreichen werden („Still in High School“). Einer der Black Hat Hacker antwortete „knowledge .. not degrees“, da Wissen und formelle Bildung nicht äquivalent sind und gerade Kriminalität keinen formellen Abschluss voraussetzt.

Insgesamt ergab sich in der selbstselektierten Stichprobe ein überraschend homogenes, zugleich jedoch realistisches Bild: Bei Hackern handelt es sich in Übereinstimmung mit der ersten Studie, früheren empirischen Befunden, sowie der Metanalyse des BKAs (2015b), überwiegend um junge, gut qualifizierte Männer.

In der Stichprobe der Black Hats sind 91,9 % Akademiker oder auf dem Weg dorthin, in der Stichprobe der White Hats sind es 93,5 %.

Diverse Nationalitäten

Aus Schutz der Anonymität und Respekt der Operational Security war die Angabe zur Nationalität optional.

63,5 % aller Hacker ($N = 1.185$) haben *keine* Angabe zur Nationalität gemacht. Innerhalb derjenigen, die eine Angabe gemacht haben ($n = 432$), waren 84 unterschiedliche Nationalitäten vertreten.

In der Gruppe der Black Hats ($n = 334$) haben 66,2 % keine Angabe zur Nationalität gemacht, die sechs häufigsten genannten Länder (Nationalitäten) waren Indien (6,9 %), USA (3,9 %), Nigeria (2,1 %), United Kingdom (1,8 %), Deutschland (1,5 %) und Russland (1,2 %).

Bei den White Hats ($n = 851$) haben 62,5 % keine Nationalität angegeben. Unter den genannten Nationalitäten waren die häufigsten Indien (6,8 %), Germany (3,8 %), United States (2,9 %), Nigeria (1,4 %) und South Africa (1,3 %).

Dass in Indien zahlreiche Cyberkriminelle, aber auch IT-Fachkräfte zu finden sind, ist ein seit langer Zeit bekanntes Phänomen (siehe z.B. Kshetri, 2016). Auch dass Nigeria und Russland zu den genannten Nationalitäten der Black Hat Hacker gehören, deckt sich mit Ergebnissen

der ersten Studie und anderen empirischen Befunden, beispielsweise dem von Bruce et al. (2024) publizierten globalen Cyberkriminalitätsindex.

5.10 Ergebnisse und Hypothesenprüfung

5.10.1 Validität der Gruppenzugehörigkeit: Black Hats und White Hats

Die meisten der zu prüfenden Hypothesen beziehen sich auf Gruppenunterschiede zwischen Black Hat- und White Hat Hackern. Dass es sich tatsächlich um Hacker handelt, wurde nicht primär durch Selbstauskunft verifiziert, sondern vor allem über die gezielte Distribution des Links: Der Fragebogen wurde nicht breit öffentlich, sondern ausschließlich in einschlägigen Cybersicherheits-Communities, Hacker-Foren und über Anzeigentargeting verbreitet. Dadurch konnte davon ausgegangen werden, dass nur Personen aus entsprechenden Hacker-Communities Zugang zur Befragung hatten. Die Teilnahmewellen erlaubten zudem eine grobe Zuordnung bzw. Plausibilitätsprüfung. Unmittelbar nach Postings des Teilnahmeaufrufs in Darknet-Foren nahmen zahlreiche Black Hats teil, während nach gezielten Teilnahmeaufrufen bei LinkedIn vermehrt White Hats teilnahmen. Die finale Gruppenzuordnung basierte auf Selbsteinschätzung, sollte aber zusätzlich empirisch validiert werden.

Zur Überprüfung der Validität der Hackergruppenzugehörigkeit (Black Hats vs. White Hats) können drei Items des Fragebogens herangezogen werden, die explizit nach cyberkriminellen Handlungen fragten:

- I would stream movies illegally
- I would hack someone's bank account
- I would hack companies for profit

Die befragten Hacker gaben ihre Zustimmung zu den als Statements formulierten hypothetischen Taten („*ich würde...*“) auf einer 5-stufigen Likert-Skala an (1 = *Strongly Disagree* bis 5 = *Strongly Agree*). Aus diesen drei Zustimmungswerten wurde dann eine

gemeinsame Skala gebildet, die zusammen als Maß für die ‚Online-Skrupellosigkeit‘ einer Person interpretiert werden kann. Der Cronbachs Alpha-Wert¹¹ lag bei $\alpha = .66$, was als akzeptabel zu bewerten ist, da die drei Items nicht den Anspruch haben, dasselbe zu messen, sondern drei verschiedene Cyberstraftaten, die in Summe einen Durchschnittswert der digitalen Kriminalitätsbereitschaft der befragten Hacker abbilden.

Um die Validität der Gruppeneinteilung (Black Hat- vs. White Hat Hacker) zu überprüfen, wurde ein *t*-Test für unabhängige Stichproben auf Basis der Skala der *Online-Skrupellosigkeit* durchgeführt. Der Levene-Test war nicht signifikant ($p = .731$), womit die Voraussetzung der Varianzhomogenität erfüllt ist. Wie zu erwarten war, trat ein deutlicher Unterschied zwischen den Hackergruppen zutage. Die Gruppe der Black Hat Hacker ($M = 3.65$, $SD = 0.99$) zeigte höhere Werte in ihrer Online-Skrupellosigkeit als die Gruppe der White Hats ($M = 2.73$, $SD = 0.97$); die Unterschiede waren signifikant $t(1153) = 14.29$, $p < .001$. Die Effektstärke lag bei $d = 0.94$ und ist somit als starker Effekt gemäß Cohen (1988) einzustufen.

Die Gruppe der Black Hat Hacker wurde also erstens in einschlägigen Hacker-Foren rekrutiert, hat sich zweitens per Selbstauskunft als Black Hat Hacker identifiziert („any form of unauthorized illegal hacking within last 12 months“), und drittens zeigen auch die Ergebnisse des *t*-Tests, dass sich diese Gruppe in der Online-Kriminalitätsbereitschaft stark von den White Hats unterscheidet.

Das Ergebnis des *t*-Tests liefert empirische Evidenz für die Trennschärfe und Validität der selbstberichteten Gruppenzuordnung. Die hohe Effektstärke nach Cohen (1988) zeigt, dass die beiden Gruppen sich nicht nur theoretisch, sondern auch praktisch bedeutsam in ihrer Bereitschaft zu rechtswidrigem Online-Verhalten (Cyberkriminalität) unterscheiden.

¹¹ Siehe Anhang 4 zur Übersicht aller Reliabilitätswerte aller verwendeten und gebildeten Skalen.

5.10.2 Statistische Analysen

Im Folgenden werden die statistischen Verfahren in SPSS aufgeführt, die zur Prüfung der 18 Hypothesen verwendet wurden.

Einige Hypothesen bezogen sich auf rein deskriptive Sachverhalte innerhalb der Stichprobe (z.B., welche und wie viele Motive Black Hat Hacker für ihre Taten angeben).

Die meisten Hypothesen bezogen sich jedoch auf Gruppenunterschiede zwischen Black Hats und White Hats (z.B. „Black Hats sind psychopatischer“, „Black Hats sind machiavellistischer“ etc.). Für diese Art der gruppenbezogenen Hypothesen wurde jeweils ein *t*-Test für unabhängige Stichproben durchgeführt. Es wurden wegen der höheren Aussagekraft ausschließlich zweiseitige Signifikanztests in den durchgeführten Analysen verwendet, unabhängig davon, ob die Hypothesen gerichtet oder ungerichtet formuliert waren. Cronbachs Alpha diente als Reliabilitätskoeffizient der verwendeten Skalen (siehe Anhang 4), und der Levene-Test wurde zur Prüfung der Voraussetzung der Varianzhomogenität eingesetzt.

Die Gruppen wurden nicht nur miteinander hinsichtlich der Dunklen Triade verglichen, sondern ihre Mittelwerte auch jeweils gegen Normwerte für die Allgemeinbevölkerung aus der Literatur getestet. Hierfür kam jeweils ein One-Sample *t*-Test zum Einsatz, bei dem geprüft wird, inwiefern sich ein Gruppenmittelwert von einem angegebenen Referenzwert signifikant unterscheidet.

Einige Hypothesen bezogen sich auf Unterschiede zwischen zwei Variablen innerhalb derselben Hackergruppe (z.B. „Primäre Psychopathie ist bei Black Hats stärker ausgeprägt als sekundäre Psychopathie“). Für diese Hypothesen wurde der *t*-Test für abhängige Stichproben verwendet.

Zwei Hypothesen bezogen sich auf Zusammenhänge: Gibt es Zusammenhänge zwischen Motiven und Triademerkmale? Gibt es Zusammenhänge zwischen der bevorzugten Angriffsart (Modus Operandi) und Triademerkmale? Für diejenigen Fragen und

Hypothesen, die sich auf Zusammenhänge beziehen, wurde das Verfahren der *punktbiserialen Korrelation* verwendet, da die Logik dieser Fragestellungen weniger auf Gruppenunterschiede als vielmehr auf Korrelationen abzielt.

Um zu beurteilen, welche Konstrukte der Dunklen Triade am relevantesten in Bezug auf Black Hat Hacking sind, wurden ebenfalls punktbiserielle Korrelationen berechnet, sowie eine binäre logistische Regression, um zu prüfen, wie gut die metrisch-skalierten Variablen Psychopathie, Narzissmus und Machiavellismus die dichotome Gruppenzugehörigkeit (Black Hat vs. White Hat) vorhersagen.

Allgemein kamen also je nach Art der Hypothese verschiedene Arten von *t*-Tests, punktbiserielle Korrelationen, deskriptive Statistiken und eine binäre logistische Regression zum Einsatz. Alle relevanten Ergebnisse sind sortiert nach Art der statistischen Tests in Anhang 4 beigefügt. Dem Anhang sind auch die jeweiligen 95 %-Konfidenzintervalle der ermittelten Effektstärken (*Cohen's d*) und mittleren Differenzen der *t*-Tests zu entnehmen.

5.10.3 Psychopathie

Die Reliabilität der SD3-Subskala für Psychopathie (9 Items) beträgt $\alpha = .73$. Cronbachs Alpha-Werte ab $\alpha = .7$ gelten nach George & Mallery (2003) allgemein als akzeptabel. Der Reliabilitätswert liegt damit exakt im Bereich, den auch die Autoren der Originalstudie zur Skalenentwicklung berichten. Für die Subskala berichten Jones & Paulhus (2014, S. 34, Tabelle 4) Reliabilitätswerte von $\alpha = .72$ (Study 2) und $\alpha = .73$ (Study 3).

Da die Hackergruppen nicht nur untereinander, sondern auch mit der Allgemeinbevölkerung verglichen werden sollen, wurde ein Referenzwert aus der Literatur verwendet. Jones und Paulhus (2014, S. 33, Table 3) ermittelten in drei Studien mit insgesamt $N = 998$ Teilnehmern Normwerte für die Allgemeinbevölkerung. Durch Mittelung der Studienergebnisse über beide Geschlechtsgruppen der drei Studien ergibt sich für Psychopathie ein Referenzwert von $M = 2.18$ ($SD = 0.59$), der hier als Norm- und Vergleichswert dienen soll. Tabelle 8 zeigt die

Psychopathie-Mittelwerte der beiden Hackergruppen und den Referenzwert der Allgemeinbevölkerung.

Tabelle 8: Deskriptive Statistiken: Psychopathie-Mittelwerte (SD3-Subskala)

	<i>n</i>	<i>M</i>	<i>SD</i>
Black Hat Hacker	334	3.10	0.72
White Hat Hacker	851	2.62	0.65
Allgemeinbevölkerung	998	2.18	0.59

Deskriptiv wird hier bereits ein Muster deutlich, dass die Gruppe der Black Hat Hacker erwartungsgemäß höhere Psychopathie-Scores aufweist als die Gruppe der White Hat Hacker. Überraschenderweise liegt aber auch der Psychopathie-Mittelwert der Gruppe der White Hats über dem Normwert der Allgemeinbevölkerung.

Auch beim deskriptiven Vergleich der Mittelwerte der Einzelitems (Black Hats vs. White Hats) zeigt sich über alle 9 Items eine Tendenz, dass Black Hat Hacker durchweg psychopathischer sind als White Hat Hacker (siehe Abb. 34).

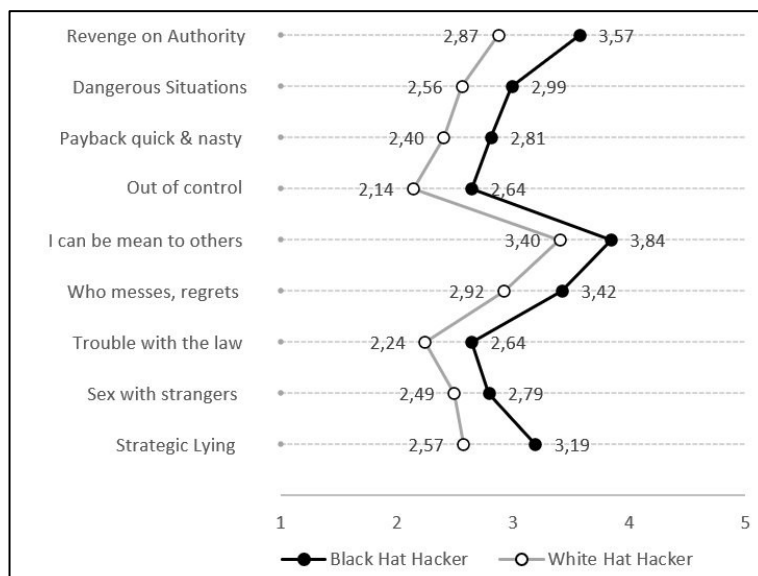


Abbildung 34. Visualisierung der Mittelwerte der Einzelitems: Psychopathie (SD3)

Anmerkung. Black Hats ($n = 334$), White Hats ($n = 851$). Items 2 und 7 (Reverse-Codierung) wurden umcodiert, sodass alle Items in dieselbe inhaltliche Richtung weisen: Höhere Werte entsprechen höheren Psychopathie-Werten.

Die Linien der Hackergruppen verlaufen im ähnlichen Muster, jedoch ist deutlich erkennbar, dass die Linie der Black Hats über alle Items hinweg rechts der Linie der White Hats verläuft. Es fallen besonders die hohen Ausprägungen beider Gruppen bei dem Item *It's true that I can be mean to others* auf. Im nächsten Schritt wird geprüft, inwiefern sich diese deskriptiv erkennbaren Unterschiede auch inferenzstatistisch bestätigen lassen.

H1: Black Hat Hacker sind signifikant psychopathischer als White Hat Hacker.

Zur Hypothesenprüfung wurde ein zweiseitiger t -Test für unabhängige Stichproben gewählt. Obwohl es sich um eine gerichtete Hypothese handelt, wurde auch hier zweiseitig getestet, aufgrund der höheren Aussagekraft und zwecks Fehlervermeidung durch einseitige Tests. Die Voraussetzungen für die Durchführung des t -Tests für unabhängige Stichproben sind die Unabhängigkeit der Stichproben, eine Normalverteilung und Varianzhomogenität. Da die Fallzahlen in den Stichproben deutlich über 300 bzw. 800 liegen, wurde keine gesonderte Prüfung der Normalverteilung durchgeführt. Bei Stichprobengrößen von deutlich mehr als 30 kann (gemäß dem zentralen Grenzwertsatz) von einer annähernden Normalverteilung ausgegangen werden (siehe z.B. Bortz & Schuster, 2010, S. 85-86). Diese Annahme der Normalverteilung wird auch bei allen weiteren t -Tests beibehalten. Da der Levene-Test in diesem Fall signifikant war ($F(1, 1183) = 4.58, p = .033$), wird der t -Test unter der Annahme ungleicher Varianzen berichtet (Welch-Test). Die Hypothese konnte bestätigt werden; die Gruppe der Black Hat Hacker ($M = 3.1, SD = 0.72$) zeigte im Vergleich zu White Hat Hackern ($M = 2.62, SD = 0.65$) signifikant höhere Psychopathie-Werte $t(559.64) = 10.53, p < .001$ (zweiseitig). Im Mittel unterscheiden sich die Hackergruppen um 0.48 Skalenpunkte auf der PSYCH-Subskala. Die Effektstärke lag bei $d = 0.71$, was als ein Effekt mittlerer Stärke zu deuten ist (Cohen, 1988). Zugehörige 95-% Konfidenzintervalle sind in Anhang 4b beigefügt.

H2: Black Hat Hacker sind signifikant psychopathischer als die Allgemeinbevölkerung, während White Hat Hacker unauffällig sind.

Zur Überprüfung der Hypothese wurde je Hackergruppe ein t -Test bei einfacher Stichprobe durchgeführt und gegen den ermittelten Normwert der Literatur von $M = 2.18$ geprüft. Der

verwendete Referenzwert entspricht dem durchschnittlichen Psychopathie-Score der drei Originalstudien zur Skalenentwicklung für Männer und Frauen (Jones & Paulhus, 2014, S. 33, Tabelle 3). Der t -Test für eine Stichprobe ergab einen signifikanten Mittelwertunterschied ($t(333) = 23.32, p < .001$, zweiseitig). Im Vergleich zum Normwert der Allgemeinbevölkerung zeigte die Gruppe der Black Hat Hacker einen signifikant erhöhten Psychopathie-Score ($M = 3.10, SD = 0.72$), die durchschnittliche Differenz betrug hier 0.92 Skalenpunkte. Die Effektgröße ist demnach als sehr groß einzuschätzen ($d = 1.28$).

Black Hat Hacker sind also signifikant psychopathischer als die Allgemeinbevölkerung.

Es ist jedoch zu berücksichtigen, dass der Vergleich auf einem Normwert aus der Literatur basiert, der nicht unter identischen Erhebungsbedingungen gewonnen wurde. Damit ist die direkte Vergleichbarkeit eingeschränkt, da die Unterschiede und die Effektstärke jedoch derartig groß sind ($d = 1.28$), liefert dies ein wichtiges Indiz, dass Black Hat Hacker deutlich psychopathischer sind als die Allgemeinbevölkerung und psychopathischer als White Hats.

Dasselbe statistische Verfahren des *One-Sample t*-Tests wurde auch für die Gruppe der White Hats ($n = 851$) durchgeführt. Auch die White Hat Hacker zeigten überraschenderweise im Vergleich zur Allgemeinbevölkerung signifikant höhere Psychopathie-Werte, $t(850) = 19.74, p < .001$, zweiseitig. Die mittlere Differenz zwischen dem PSYCH-Score der White Hats und dem Referenzwert lag bei 0.44 Skalenpunkten. Bei den White Hats lag die Effektstärke bei $d = 0.68$ und ist somit als mittlerer Effekt einzustufen, auch wenn die Stärke des Effektes nur ca. halb so groß ist wie in der Gruppe der Black Hats ($d = 0.68$ im Vergleich zu $d = 1.28$).

Die Hypothese kann somit teilweise bestätigt werden. Black Hat Hacker sind signifikant psychopathischer als die Allgemeinbevölkerung, aber überraschenderweise sind auch White Hat Hacker signifikant psychopathischer als die Bevölkerung, wenngleich die Unterschiede hier deutlich schwächer ausfallen. Im Mittelwertvergleich zu Psychopathie zeigt sich beim Vergleich der Gruppen ein eindeutiges Muster:

Black Hats > White Hats > Allgemeinbevölkerung.

Es bestünde die Möglichkeit, dass es sich bei den Unterschieden zur Allgemeinbevölkerung um eine Scheinkorrelation bzw. einen Geschlechtereffekt handelt. Während der Männer-Frauen-Anteil in der Bevölkerung gleich verteilt ist, waren es bei Hackern 91,6 % Männer.

Um dies zu prüfen, wurde nochmals ein t -Test bei einer Stichprobe durchgeführt, diesmal jedoch gegen eine reine Männerstichprobe getestet. Jones & Paulhus (2014, S. 33) berichten in drei Studien die Normwerte der Samples aufgeteilt nach Männern und Frauen. Über die drei Studien hinweg ergibt sich für die Männer ein etwas höherer Psychopathie-Mittelwert von $M = 2.35$ ($SD = 0.62$).

Black Hat Hacker zeigten im Vergleich zum rein männlichen Sample noch immer signifikant höhere Psychopathie-Werte, $t(333) = 19.00$, $p < .001$. Die mittlere Differenz auf der Subskala betrug 0.75 Skalenpunkte. Auch hier zeigte sich ein starker Effekt von $d = 1.04$. Auch die Stichprobe der White Hats zeigte im Vergleich zum Männersample signifikant höhere Psychopathie-Scores, $t(850) = 12.15$, $p < .001$, mittlere Differenz 0.27. Hier lag die Effektstärke im Bereich eines kleinen Effektes ($d = 0.42$).

Die Ergebnisse zeigen, dass Hacker (Black- und White Hats) signifikant psychopathischer als die Allgemeinbevölkerung sind; der Effekt lässt sich nicht durch Unterschiede in der Geschlechterverteilung in den Stichproben erklären.

5.10.4 Machiavellismus

Im nächsten Schritt wurden die Hackergruppen hinsichtlich machiavellistischer Tendenzen verglichen. Zunächst wurde die Reliabilität der SD3-Machiavellismus-Subskala überprüft. Mit einem Cronbachs Alpha-Wert von $\alpha = .78$ zeigte die Skala eine akzeptable bis gute interne Konsistenz, die damit nahe an den Werten der Originalstudie lag ($\alpha = .74$ in Study 1, $\alpha = .76$ in Study 2) (Jones & Paulhus, 2014, S. 34, Tabelle 4).

Die Tabelle 9 zeigt die Machiavellismus-Mittelwerte und Standardabweichungen der Black Hats ($n = 334$), der White Hats ($n = 851$), sowie den von Jones und Paulhus (2014, S. 33)

ermittelten Normwert auf Basis von drei Studien mit insgesamt $N = 998$ Personen aus der Allgemeinbevölkerung.

Tabelle 9: Deskriptive Statistiken: Machiavellismus-Mittelwerte (SD3-Subskala)

	<i>n</i>	<i>M</i>	<i>SD</i>
Black Hat Hacker	334	4.10	0.61
White Hat Hacker	851	3.72	0.64
Allgemeinbevölkerung	998	3.15	0.57

Insgesamt lässt sich beobachten, dass die Stichprobe der Black Hat Hacker deutlich höhere Machiavellismus-Scores zeigt als die Gruppe der White Hats und die Allgemeinbevölkerung. Auffällig ist jedoch, dass auch der Mittelwert der White Hat Hacker deutlich über dem Skalenmittelpunkt und dem Referenzwert für die Allgemeinbevölkerung liegt. Dieses deskriptive Muster, dass Black Hats machiavellistischer sind als White Hats, zeigt sich auch deutlich bei den Visualisierungen der einzelnen Items. Wie bereits bei der Subskala für Psychopathie, liegen die Machiavellismus-Werte der Black Hats bei allen Items über denen der White Hats.

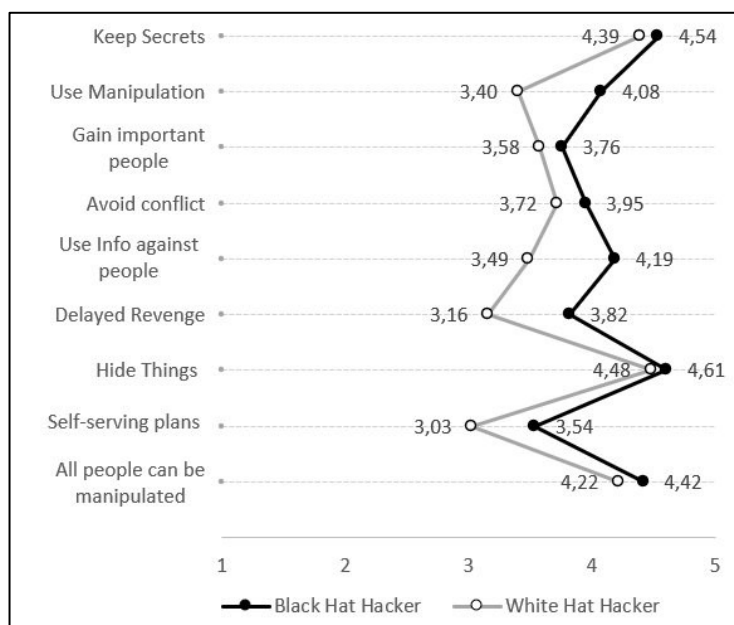


Abbildung 35. Visualisierung der Mittelwerte der Einzelitems: Machiavellismus (SD3)

Anmerkung. Black Hats ($n = 334$), White Hats ($n = 851$)

Ob die deskriptiv beobachtbaren Unterschiede zwischen Black- und White Hats auch statistisch signifikant sind, wird im folgenden Abschnitt anhand inferenzstatistischer Analysen überprüft (t -Tests).

H3: Black Hat Hacker sind signifikant machiavellistischer als White Hat Hacker.

Die Stichproben der Black Hats ($n = 334$) und White Hats ($n = 851$) wurden daraufhin überprüft, ob sie sich in machiavellistischen Persönlichkeitsdispositionen unterscheiden. Es wurde dazu ein t -Test für unabhängige Stichproben durchgeführt (zweiseitig, da konservativer). Die Voraussetzung für den t -Test (Varianzhomogenität) wurde auch hier durch den Levene-Test überprüft, der zeigte, dass die Voraussetzung erfüllt ist $F(1, 1183) = 2.48, p = .115$.

Die Hypothese H3 kann bestätigt werden, das Ergebnis des t -Tests ist signifikant ($t(1183) = 9.41, p < .001$). Black Hats ($M = 4.10, SD = 0.61$) besitzen signifikant machiavellistischere Persönlichkeitsmerkmale als die Stichprobe der White Hat Hacker ($M = 3.72, SD = 0.64$). Die mittlere Differenz auf der Likert-Skala lag bei 0.39 Punkten und die Effektstärke ($d = 0.61$) kann nach Cohen (1988) als moderat eingestuft werden.

H4: Black Hat Hacker sind signifikant machiavellistischer als die Allgemeinbevölkerung, während White Hat Hacker unauffällig sind.

Zur Hypothesenprüfung wurden je Hackergruppe separate t -Tests für eine Stichprobe (zweiseitig) berechnet, wobei der jeweils gemessene Gruppenmittelwert mit dem Normwert bzw. Referenzwert von $M = 3.15$ aus den Studien von Jones und Paulhus (2014, S. 33) verglichen wurde.

Black Hat Hacker ($M = 4.10, SD = 0.61$) sind signifikant machiavellistischer im Vergleich zum Referenzwert der Allgemeinbevölkerung ($M = 3.15$). Die gemessenen Unterschiede sind signifikant, $t(333) = 28.49, p < .001$ (zweiseitig) mit einer mittleren Differenz von 0.95 Skalenpunkten. Die Effektstärke ist mit $d = 1.56$ als sehr hoch zu werten. Black Hat Hacker weisen somit eine signifikant stärkere Ausprägung machiavellistischer Tendenzen auf als die Normstichprobe.

Auch für die Gruppe der White Hat Hacker ($n = 851$) wurde ein *One-Sample t-Test* durchgeführt. Im Vergleich zur Allgemeinbevölkerung zeigten auch sie signifikant höhere Machiavellismus-Werte, $t(850) = 25.56$, $p < .001$ (zweiseitig). Die mittlere Differenz betrug 0.56 Punkte. Auch in der Gruppe der White Hats zeigte sich ein starker Effekt ($d = 0.88$), auch wenn dieser geringer als bei der Gruppe der Black Hats ist.

Die Hypothese H4 kann teilweise bestätigt werden. Bei Machiavellismus zeigt sich ein vergleichbares Muster, wie bereits zuvor bei subklinischer Psychopathie. Black Hat Hacker unterscheiden sich signifikant von der Allgemeinbevölkerung und weisen deutlich höhere Werte auf ($d = 1.56$). Gleichzeitig zeigt sich jedoch, dass auch White Hat Hacker signifikant machiavellistischer sind als die Allgemeinbevölkerung und auch hier ein starker Effekt vorliegt ($d = 0.88$). Beim Mittelwertvergleich der Gruppen ergibt sich auch bei Machiavellismus ein konsistentes Bild:

Black Hats > White Hats > Allgemeinbevölkerung.

Zur Kontrolle von Geschlechtereffekten wurde auch hier ein weiterer *One-Sample t-Test* durchgeführt, diesmal gegen den Machiavellismus-Normwert der männlichen Probanden ($M = 3.24$, $SD = 0.60$) aus den Studien von Jones & Paulhus (2014, S. 33).

Black Hat Hacker zeigten im Vergleich zum männlichen Sample immer noch signifikant höhere Machiavellismus-Werte, $t(333) = 25.80$, $p < .001$ (zweiseitig). Der Effekt von $d = 1.41$ liegt trotzdem im Bereich eines starken Effektes. Auch White Hat Hacker zeigten im Vergleich zum Männersample signifikant höhere Machiavellismus-Werte, $t(850) = 21.49$, $p < .001$. Die Effektstärke lag im oberen Bereich eines mittleren Effektes ($d = 0.74$).

Auch beim Gruppenvergleich mit einem reinen Männersample der Allgemeinbevölkerung zeigt sich ein ähnliches Muster wie bei Psychopathie, allerdings bei Machiavellismus mit noch größeren Gruppenunterschieden (Effektstärken): Sowohl Black Hats als auch White Hats sind signifikant machiavellistischer als die Allgemeinbevölkerung.

5.10.5 Narzissmus

Während sich die Hackergruppen erwartungsgemäß hinsichtlich Psychopathie und Machiavellismus unterscheiden, war die Hypothese, dass sich im subklinischen Narzissmus weniger starke Unterschiede zeigen. Die Reliabilität der SD3-Subskala für Narzissmus (9 Items) lag bei Cronbachs $\alpha = .65$ und damit tendenziell im grenzwertigen Reliabilitätsbereich. Da es sich jedoch um eine etablierte Standardskala handelt, wurde die Subskala in die Analysen einbezogen. Auch in der Originalpublikation zur Skalenentwicklung (Jones & Paulhus, 2014, S. 34. Table 4) berichten die Autoren Reliabilitätswerte der Subskala für Narzissmus, die je nach Studie im akzeptablen Bereich liegen ($\alpha = .78$) oder leicht darunter ($\alpha = .68$). Die Narzissmus-Mittelwerte der Gruppen sind in Tabelle 10 aufgeführt.

Tabelle 10: Deskriptive Statistik: Narzissmus-Mittelwerte (SD3-Subskala)

	<i>n</i>	<i>M</i>	<i>SD</i>
Black Hat Hacker	334	3.05	0.63
White Hat Hacker	851	2.96	0.60
Allgemeinbevölkerung	998	2.82	0.53

Verglichen mit den vorherigen deutlichen Gruppenunterschieden bei subklinischer Psychopathie und Machiavellismus, liegen die Mittelwerte für Narzissmus dichter beieinander und auch dichter am Referenzwert der Allgemeinbevölkerung. Abbildung 36 zeigt die grafische Darstellung der Mittelwerte der Einzelitems.

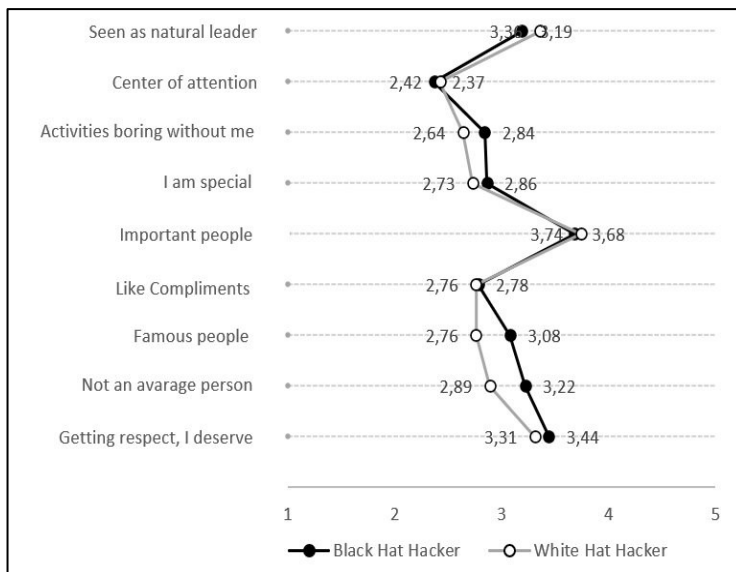


Abbildung 36. Visualisierung der Mittelwerte der Einzelitems: Narzissmus (SD3)

Anmerkung. Black Hats ($n = 334$), White Hats ($n = 851$). Drei reverse-codierte Items wurden entsprechend umcodiert, sodass alle Items in die gleiche Richtung weisen (höhere Werte stehen für stärkeren Narzissmus).

Die Linien der Black Hats und White Hats verlaufen dicht beieinander, überlagern sich zum Teil und die Unterschiede fallen insgesamt klein aus. Ob diese Unterschiede inferenzstatistisch bedeutsam sind, wird im Folgenden geprüft.

H5: Zwischen Black Hat Hackern und White Hat Hackern bestehen keine signifikanten Unterschiede im Narzissmus.

Die Hacker-Stichproben wurden daraufhin überprüft, ob sie sich signifikant in Bezug auf die SD3-NARC-Scores unterscheiden. Den Ergebnissen des Levene-Tests zufolge kann von Varianzhomogenität in den Stichproben ausgegangen werden ($F(1, 1183) = 0.94, p = .332$). Die Hypothese H5 wurde mit einem zweiseitigen t -Test für unabhängige Stichproben geprüft.

Die Mittelwertdifferenz im Narzissmus zwischen den Hackergruppen war signifikant ($t(1183) = 2.38, p = .018$). Die Hypothese, dass *kein* Unterschied zwischen den Gruppen in narzisstischen Persönlichkeitsmerkmalen besteht wird somit verworfen. Black Hats besitzen leicht ausgeprägtere narzisstische Persönlichkeitsdispositionen ($M = 3.05, SD = 0.63$) als White Hats ($M = 2.96, SD = 0.60$). Die Differenzen zwischen den Gruppen sind jedoch

minimal; es zeigte sich in den Daten lediglich eine mittlere Differenz von 0.09 Skalenpunkten. Diese Abweichung entspricht auf einer 5-stufigen Likert-Skala nur ca. 2 % der Skalenbreite. Diese kleine, aber signifikante, Differenz ist gemäß Cohen (1988) als sehr geringen Effekt einzustufen ($d = 0.15$). In großen Stichproben können selbst kleinste Effekte statistisch signifikant werden, wobei hier zwischen statistischer Signifikanz und praktischer Relevanz unterschieden werden sollte. Zwischenmenschlich und fernab von Skalenwerten ist die Tatsache unbedeutend, dass Black Hats 2 % narzisstischer sind und es kann angenommen werden, dass sich die Gruppen in der Realität nicht relevant voneinander unterscheiden. In Übereinstimmung mit dem aktuellen Forschungsstand scheinen besonders Psychopathie und Machiavellismus mit antisozialen- oder kriminellen Verhaltensweisen verbunden zu sein, während die Ergebnisse zu Narzissmus weniger eindeutig sind.

H6: Black Hat Hacker und White Hat Hacker sind signifikant narzisstischer als die Allgemeinbevölkerung.

Je Hackergruppe wurde zur Prüfung der Hypothese ein t -Test bei einer Stichprobe (zweiseitig) durchgeführt und wiederum mit dem Normwert der Allgemeinbevölkerung von $M = 2.82$, $SD = 0.53$ aus den drei Studien ($N = 998$) von Jones & Paulhus (2014, S. 33) verglichen.

Black Hat Hacker sind signifikant narzisstischer als die Allgemeinbevölkerung $t(333) = 6.72$, $p < .001$ (zweiseitig). Die mittlere Differenz lag bei 0.23 Skalenpunkten. Es handelt sich dabei um einen kleinen Effekt ($d = 0.37$).

Doch auch die Stichprobe der legal agierenden White Hats ist signifikant narzisstischer als die Normalbevölkerung mit $t(850) = 6.64$, $p < .001$ und durchschnittlicher Differenz von 0.14 Skalenpunkten. Nach Cohen (1988) handelt es sich ebenfalls um einen kleinen Effekt ($d = 0.23$). Auch in Bezug auf Narzissmus wurde - zur Vermeidung von Scheinkorrelationen durch Geschlechtereffekte - ein weiterer *One-Sample t*-Test je Hackergruppe durchgeführt, diesmal mit dem Referenzwert einer rein männlichen Stichprobe. Beim Mittelwertvergleich der White-Hat-Stichprobe mit dem männlichen Sample der Bevölkerung, bleibt der Unterschied im

subklinischen Narzissmus zwar signifikant ($t(850) = 2.76, p = .006$), aber die Effektstärke verschwindet fast vollständig (Cohen's $d = 0.10$). Bei den Black Hats bleibt auch beim Vergleich mit dem männlichen Normwert ein signifikanter ($t(333) = 4.39, p < .001$), aber kleiner Unterschied ($d = 0.24$) bestehen.

Die Hypothese kann damit bestätigt werden. Black Hat Hacker und White Hat Hacker sind signifikant narzisstischer als die Allgemeinbevölkerung, jedoch handelt es sich um einen minimalen Gruppenunterschied. Zur Einordnung im Kontext der anderen Triademerkmale lagen die Unterschiede beim Machiavellismus zur Allgemeinbevölkerung im Bereich von $d = 1.56$ (Black Hats) und $d = 0.88$ (White Hats), die Unterschiede bei Narzissmus von lediglich $d = 0.37$ (Black Hats) und $d = 0.23$ (White Hats) sind weit geringer und somit auch in praktischer Hinsicht weniger relevant.

5.10.6 Dunkle Triade (Gesamt)

H7: Das kriminelle Hacking (Black Hat Hacking) ist am stärksten mit Psychopathie und Machiavellismus verbunden und am schwächsten mit Narzissmus, sowohl in Gruppenvergleichen, Korrelationen als auch in Vorhersagemodellen.

Kernhypothese der Arbeit ist, dass kriminelle Hacker sich von White Hats in den Triademerkmale unterscheiden, diese Unterschiede aber unterschiedlich groß sind. Durch t -Tests für unabhängige Stichproben wurden pro Subskala jeweils signifikante, unterschiedlich starke Effektgrößen nach Cohen (1988) identifiziert. Die größten Gruppenunterschiede zwischen Black Hat- und White Hat Hackern bestehen bei Psychopathie ($d = 0.71$) und Machiavellismus ($d = 0.61$). Im subklinischen Narzissmus zeigte sich nur ein sehr geringer Unterschied zwischen den ethischen und kriminellen Hackern ($d = 0.15$). Die Hypothese wurde jedoch vor dem Hintergrund formuliert, dass White Hats weitestgehend unauffällig sind. Es wurde erwartet, dass legal handelnde White Hat Hacker in Bezug auf die Dunkle Triade weitestgehend der Allgemeinbevölkerung entsprechen. Der Befund, dass Black- und White Hats z.B. in Bezug auf machiavellistische Persönlichkeitsdispositionen ‚nur‘ einen mittleren Gruppenunterschied aufweisen ($d = 0.61$),

hat primär damit zu tun, dass White Hats ebenfalls deutlich machiavellistischer sind als die Allgemeinbevölkerung ($d = 0.88$). Vergleicht man die SD3-Scores der Black Hat Hacker mit den Normwerten der Allgemeinheit, ergibt sich eine andere Rangfolge der Konstrukte: Am stärksten unterscheiden sich Black Hats von der Allgemeinbevölkerung in Machiavellismus ($d = 1.56$), gefolgt von Psychopathie ($d = 1.28$) und Narzissmus ($d = 0.37$). Sowohl beim Vergleich mit den White Hats, als auch der Allgemeinbevölkerung wurde deutlich, dass Machiavellismus und Psychopathie deutlich mit dem kriminellen Hacking verbunden sind. Dass besonders Psychopathie und Machiavellismus mit antisozialem oder kriminellen Verhalten verbunden sind, ist empirisch gut abgesichert, während die Ergebnisse zu Narzissmus abweichen (siehe Kapitel 3.1).

Cohen's d und Korrelationskoeffizienten lassen sich direkt ineinander umrechnen. Die Hypothese wurde zusätzlich im Sinne der Korrelationslogik überprüft. Hierzu wurde die Gruppenzugehörigkeit als $0 = \text{White Hat}$ und $1 = \text{Black Hat}$ umcodiert, sodass positive Korrelationen inhaltlich für Zusammenhänge mit kriminellen Hacking stehen. Wie auch bei den Gruppenunterschieden nach Cohen (1988), zeigte sich eine deutliche Rangfolge der Stärke der Korrelationen. Die stärksten Korrelationen mit Black Hat Hacking zeigten sich bei Psychopathie, $r(1183) = .30, p < .001$, gefolgt von Machiavellismus $r(1183) = .26, p < .001$. Der Zusammenhang mit Narzissmus fiel hingegen sehr schwach aus und kann vernachlässigt werden, $r(1183) = .07, p = .018$.

Eine dritte Möglichkeit zur Überprüfung der Hypothese, dass die Dimensionen der Dunklen Triade eine unterschiedliche prädiktive Kraft für kriminelles Black Hat Hacking besitzen, besteht in der binären logistischen Regression. Analysiert wurde, in welchem Ausmaß die metrisch skalierten Merkmale der Dunklen Triade (SD3-Scores) die Zugehörigkeit zur Gruppe der Black Hats oder White Hats vorhersagen.

Hierbei wurde die Variable der Gruppenzugehörigkeit umcodiert als $0 = \text{White Hat Hacker}$ und $1 = \text{Black Hat Hacker}$. Das Modell war signifikant besser als ein Nullmodell ohne

Prädiktoren, $\chi^2(3) = 141.37$, $p < .001$. Die Modellgüte beträgt nach Cox & Snell $R^2 = 0.11$ und nach Nagelkerke $R^2 = 0.16$, was auf eine kleine Erklärungskraft hindeutet.¹²

Die Klassifikationsgüte des Modells lag bei 74,3 % korrekt vorhergesagter Fälle. White Hat Hacker wurden dabei in 94,2 % der Fälle korrekt klassifiziert, Black Hat Hacker hingegen nur in 23,7 % der Fälle. Zum Teil könnte dies auf die unterschiedlich großen Stichproben zurückzuführen sein. Bei Betrachtung der einzelnen Prädiktoren waren höhere Werte in Machiavellismus ($B = 0.68$, Wald(1) = 25.28, $p < .001$, OR = 1.96) und Psychopathie ($B = 0.83$, Wald(1) = 47.38, $p < .001$, OR = 2.28) erwartungsgemäß mit einer erhöhten Chance für eine Black Hat-Zugehörigkeit verbunden. Dieser Befund passt zu den vorher identifizierten Korrelationen und Ergebnissen der t -Tests. Im Gegensatz zum vorherigen Ergebnis, dass Narzissmus auch leicht mit dem Black Hat Hacking korreliert, zeigte sich in der binären logistischen Regression ein anderer Befund: Narzissmus ($B = -0.27$, Wald(1) = 4.93, $p = .026$, OR = 0.76) war ebenfalls signifikant, allerdings in umgekehrter Richtung. Bei isolierter Betrachtung erhöht Narzissmus leicht die Chance, White Hat Hacker zu sein, nicht Black Hat Hacker.

Während Narzissmus also in der Korrelation und t -Tests leicht positiv mit dem Black Hat Hacking assoziiert war, zeigte sich im Regressionsmodell ein gegenteiliger Effekt, der sich dadurch erklären lässt, dass Narzissmus, Machiavellismus und Psychopathie deutlich interkorreliert sind. Die Korrelation der Triadebestandteile untereinander ist der Grund, warum Paulhus & Williams (2002) sie zur Triade gebündelt haben und sie gemeinsam als solche untersucht werden. Das bedeutet, dass höhere Narzissmus-Scores im Durchschnitt auch mit höheren Psychopathie- und Machiavellismus-Scores einhergehen, die wiederum deutlich mit *Cyberkriminalität im engeren Sinne* (Black Hat Hacking) verbunden sind. Bei der isolierten Betrachtung von Narzissmus verbleibt kein positiver Beitrag mehr zur Vorhersage von Black Hat Hacking.

¹² Es handelt sich hierbei um eine binäre logistische Regression und somit um Pseudo- R^2 -Werte, die nicht direkt mit R^2 einer linearen Regression vergleichbar sind, aber eine grobe Einschätzung der Modellgüte erlauben.

Die Hypothese kann bestätigt werden. Sowohl bei den Effektstärken nach Cohen (1988), Korrelationen und im Vorhersagemodell (binäre logistische Regression) sind Psychopathie und Machiavellismus am bedeutsamsten bei der Erklärung von Black Hat Hacking. Narzissmus hingegen zeigt mit Black Hat Hacking entweder sehr schwache Zusammenhänge oder keine Zusammenhänge und bei isolierter Betrachtung sogar einen leicht gegenteiligen Effekt. Wer also primär durch einen narzisstischen Geltungsdrang motiviert ist, ohne aber machiavellistisch oder psychopathisch zu sein, wählt eher eine Karriere als White Hat Hacker (z.B. Sicherheitsforscher) im Licht der Öffentlichkeit als eine kriminelle Karriere im Darknet.

5.10.7 Primäre und sekundäre Psychopathie (LSRP)

Die SD3-Subskala erfasst subklinische Psychopathie mit nur 9 Items und wird damit nicht der Komplexität und Breite des Psychopathiekonstruktes gerecht. Daher wurde zusätzlich die LSRP-Skala verwendet, welche eine Differenzierung zwischen den Subskalen primärer und sekundärer Psychopathie ermöglicht. Die Levenson Self-Report Psychopathy-Scale stellte jedoch das Ende des Erhebungsinstrumentes dar. Da nicht alle befragten Hacker den SoSci-Survey-Fragebogen bis zum Ende ausgefüllt hatten, ist die Fallzahl mit $n = 639$ White Hat Hackern und $n = 258$ Black Hat Hackern etwas geringer als bei den vorherigen Fragestellungen. Einbezogen wurden also nur diejenigen Fälle, die beide Subskalen vollständig abgeschlossen haben. Die Reliabilität der LSRP Gesamt- und Subskalen wurde mittels Cronbachs Alpha überprüft (siehe Tabelle 11).

Tabelle 11: Alpha-Reliabilitäten der LSRP ($n = 897$)

Skala	Cronbachs Alpha	Anzahl der Items
Gesamtskala	0.86	26
Primäre Psychopathie	0.88	16
Sekundäre Psychopathie	0.64	10

Während die Gesamtskala und Subskala für primäre Psychopathie eine gute interne Konsistenz zeigten ($\alpha > .8$), lag die interne Konsistenz für die Subskala der sekundären Psychopathie im fragwürdigen Bereich. Die schlechtere Reliabilität der Subskala für sekundäre Psychopathie ist jedoch ein bekanntes Phänomen in anderen empirischen Untersuchungen. Zahlreiche Validierungsstudien der LSRP fanden für sekundäre Psychopathie Cronbachs Alpha-Werte im Bereich von $\alpha = .6$ (Psederska, Yankov, Bozgunov, Popov, Vasilev & Vassileva, 2020, S. 1110, Table 3). Levenson und Kollegen schrieben selbst dazu: „The .63 alpha for secondary psychopathy is probably acceptable for a 10-item scale“ (Levenson et al., 1995, S. 153). Die Skala findet daher Anwendung, da sie ein etabliertes Standard-Erhebungsinstrument darstellt und die Reliabilität der LSRP-Gesamtskala als hoch einzustufen ist.

H8: Black Hat Hacker sind signifikant psychopathischer als White Hat Hacker in Bezug auf primäre und sekundäre Psychopathie.

Im ersten Schritt sollen die Hacker-Stichproben der Black Hats ($n = 258$) und White Hats ($n = 639$) untereinander verglichen werden in Bezug auf die Gesamtskala und beide Subskalen. Bei dem Instrument der LSRP ist es teilweise üblich, Summenwerte zu bilden. Es werden im Folgenden jedoch Mittelwerte auf der 4-stufigen Likert-Skala berichtet, weil die Subskalen eine unterschiedliche Anzahl der Items aufweisen und die Mittelwerte somit eine bessere direkte Vergleichbarkeit erlauben.

Der Mittelwert der Gruppe der Black Hat Hacker für die LSRP-Gesamtskala lag bei $M = 2.55$ ($SD = 0.45$). Die Werte für die Subskala der primären Psychopathie, welche für die planend, strategische Seite steht, sind dabei höher ($M = 2.66$, $SD = 0.62$) und gemäßigter bei sekundärer Psychopathie ($M = 2.44$, $SD = 0.51$). Sekundäre Psychopathie repräsentiert eher die defizitäre Selbstkontrolle und impulsive Seite von Psychopathie. Auch in der Stichprobe der ethischen White Hat Hacker lag der Mittelwert der LSRP-Gesamtskala über dem Skalenmittelpunkt $M = 2.23$ ($SD = 0.42$). Zwischen den deskriptiven Mittelwerten für primäre Psychopathie ($M = 2.19$, $SD = 0.56$) und sekundäre Psychopathie ($M = 2.28$, $SD = 0.46$)

zeigten sich nur leichte Unterschiede. Im Gegensatz zu den Black Hats war jedoch sekundäre Psychopathie ausgeprägter.

Es folgte die Prüfung auf statistische Signifikanz der Unterschiede. Dazu wurden drei zweiseitige t -Tests für unabhängige Stichproben berechnet, jeweils für die Gesamtskala und beide Subskalen. Der Levene-Test ergab, dass in allen drei Tests von Varianzhomogenität ausgegangen werden kann ($F(1, 895) = 1.88, p = .171$ für die Gesamtskala, $F(1, 895) = 2.58, p = .109$ für primäre Psychopathie und $F(1, 895) = 1.07, p = .301$ für die Subskala der sekundären Psychopathie).

Eine deutliche Verbindung zwischen Psychopathie und Cyberkriminalität zeigte sich auch in Bezug auf die LSRP-Skala: Black Hats sind signifikant psychopathischer als White Hats in Bezug auf beide Subskalen und die LSRP-Gesamtskala. Für die Gesamtskala ($t(895) = 9.87, p < .001$) ergab sich eine mittlere Differenz von 0.31. Es wurden jedoch Unterschiede zwischen den Subskalen deutlich. Die mittlere Differenz in Bezug auf primäre Psychopathie ($t(895) = 10.93, p < .001$) war mit 0.47 mehr als doppelt so groß wie bei sekundärer Psychopathie ($t(895) = 4.56, p < .001$, mittlere Differenz: 0.16). Damit zeigte sich auch bei den Effektstärken ein eindeutiges Bild: Für die Gesamtskala liegt der Unterschied zwischen Black Hats und White Hats im mittleren Bereich ($d = 0.73$). Differenziert man jedoch nach primärer & sekundärer Psychopathie, ergibt sich ein starker Effekt bei primärer Psychopathie ($d = 0.81$) und ein schwacher Effekt bei sekundärer Psychopathie ($d = 0.34$).

Die Hypothese kann somit bestätigt werden: Black Hats sind in beiden Dimensionen signifikant psychopathischer als White Hats.

Bemerkenswert ist, dass die Effekte bei primärer Psychopathie ($d = 0.81$) mehr als doppelt so stark ausfallen wie bei sekundärer Psychopathie ($d = 0.34$), was ebenfalls ein Indiz dafür ist, dass Psychopathie de facto aus zwei distinkten Faktoren besteht und diese Differenzierung unbedingt erfolgen sollte. Black Hats sind demnach psychopathischer als White Hats, das gilt besonders für die Dimension der Furchtlosigkeit, aber weniger für die Impulsivität.

H9: Primäre Psychopathie (planvolles, empathieloses Handeln) ist bei Black Hats stärker ausgeprägt als sekundäre Psychopathie (Impulsivität, Aggression).

Hypothese H9 zielt nicht auf einen Vergleich der Hackergruppen untereinander, sondern ein Vergleich der Psychopathiefaktoren innerhalb der Gruppe der Black Hats, um das Profil auszudifferenzieren und die Frage zu beantworten, ob Black Hats eher dem Profil erfolgreicher oder krimineller Psychopathen entsprechen. Deskriptiv zeigte sich bereits, dass die Mittelwerte der Black Hats bei primärer Psychopathie über denen der sekundären Psychopathie liegen (bei White Hats zeigte sich ein umgekehrtes Verhältnis). Ob dies signifikant ist, wurde mit einem t -Test für abhängige Stichproben getestet (zweiseitig). Hierbei wurden innerhalb der Gruppe der Black Hats ($n = 258$) die Mittelwerte der beiden Subskalen verglichen. H9 kann bestätigt werden: Primäre Psychopathie ist bei Black Hat Hackern signifikant ausgeprägter als sekundäre Psychopathie ($t(257) = 5.28, p < .001$). Es handelt sich um einen kleinen Effekt ($d = 0.33$) mit einer mittleren Differenz von 0.22.

H10: Black Hat Hacker sind signifikant psychopathischer als die Allgemeinbevölkerung in Bezug auf primäre und sekundäre Psychopathie, während White Hat Hacker unauffällig sind.

Zur Überprüfung der Hypothese wurden die Gruppen auch hier mit einem Normwert aus der Allgemeinbevölkerung verglichen. Da die Normwerte in der Literatur als Summenscores angegeben sind, wird im Folgenden damit gerechnet. Die 26 Items der LSRP werden auf einer 4-stufigen Likert-Skala (1 = *Strongly Disagree* bis 4 = *Strongly Agree*) bewertet. Der Summenscore kann somit zwischen minimal 26 und maximal 104 liegen. Es ist wichtig zu betonen, dass das Instrument speziell für nicht-institutionalisierte Populationen entwickelt wurde und Psychopathie subklinisch für Forschungszwecke erfasst. Dies stellt keine Diagnose dar und zudem gibt es keinen objektiv definierbaren Grenzwert, ab wann von Psychopathie ausgegangen werden kann. In einer Validierungsstudie mit $N = 549$ Probanden wählten Brinkley et al. (2001) einen Score von 58 als Grenzwert, um von einer

hochpsychopathischen Gruppe auszugehen: „Those participants scoring in the top third of the distribution were considered psychopathic (scores of 58 or more)“ (2001, S. 1025).

Der durchschnittliche LSRP-Summenscore der Black Hat Hacker ($n = 258$) lag bei $M = 66.88$ ($SD = 12.31$) und der durchschnittliche Summenscore der White Hat Hacker bei $M = 57.83$ ($SD = 11.42$). Gemäß der genannten Einstufung (High Psychopathy ≥ 58) lag die Stichprobe der Black Hats deutlich im Bereich hoher Psychopathie. Auch White Hats zeigten deskriptiv jedoch hohe Werte. Ob sie ebenfalls in die hoch-psychopathische Gruppe fallen, wird zur Rundungsfrage, da sie mit 57,83 nur sehr knapp unter dem definierten Grenzwert von 58 lagen. Der Cut-Off-Score von 58 wurde jedoch willkürlich festgelegt. Von größerer Relevanz und Aussagekraft ist die Frage, ob sich die Gruppen signifikant von den Mittelwerten der Allgemeinbevölkerung unterscheiden. Brinkley et al. (2001, S. 1026) ermitteln für ihr Sample von $N = 549$ einen mittleren Summenwert von $M = 54.66$, $SD = 11.58$ (Gesamtskala), $M = 32.99$, $SD = 8.19$ (primäre Psychopathie) und $M = 21.68$, $SD = 5.05$ (sekundäre Psychopathie). Um die Hypothese zu überprüfen, ob Black Hats und White Hats signifikant psychopathischer sind, wurden je Hackergruppe t -Tests bei einer Stichprobe (zweiseitig) durchgeführt und gegen die genannten Normreferenzwerte der Skalen getestet.

Der LSRP-Gesamtscore der Black Hat Hacker ($M = 66.38$, $SD = 12.74$) liegt signifikant über dem Testwert der Allgemeinbevölkerung ($t(257) = 15.95$, $p < .001$). Die mittlere Differenz liegt für die Gesamtskala bei 12.22 Skaleneinheiten, was einem starken Effekt ($d = 0.99$) entspricht.

Differenziert man nach den Subskalen, zeigen sich jedoch unterschiedlich starke Effekte. Während bei primärer Psychopathie ($M = 42.49$, $SD = 9.8$) ein signifikanter ($t(257) = 15.54$, $p < .001$) großer Unterschied vorliegt ($d = 0.97$), ist die Effektstärke bei sekundärer Psychopathie ($M = 24.35$, $SD = 5.07$) nur im Bereich eines mittleren Effektes ($t(257) = 8.47$, $p < .001$, $d = 0.53$). Black Hats sind demnach besonders auffällig hinsichtlich primärer Psychopathie (Empathie- und Furchtlosigkeit).

Doch auch der LSRP-Gesamtscore der White Hats ($M = 57.47$, $SD = 11.81$) liegt signifikant über dem Normwert ($t(638) = 7.02$, $p < .001$). Die mittlere Differenz liegt hier jedoch nur bei

3.17 Punkten auf der Skala, die von 26-104 reicht. Es handelt sich demnach um einen schwachen Effekt von $d = 0.28$. Die Unterschiede bei primärer Psychopathie ($M = 35.07$, $SD = 9.04$) sind signifikant ($t(638) = 5.9$, $p < .001$) und im Bereich eines kleinen Effektes ($d = 0.23$). Bei sekundärer Psychopathie ($M = 22.75$, $SD = 4.64$) ($t(638) = 5.83$, $p < .001$) lag die Effektstärke ebenfalls bei $d = 0.23$.

Die Hypothese kann zum Teil bestätigt werden. Kriminelle Black Hat Hacker sind im Sinne der Hypothese signifikant psychopathischer als die Allgemeinbevölkerung in Bezug auf primäre Psychopathie ($d = 0.97$) und sekundäre Psychopathie ($d = 0.53$). Entgegen der Hypothese sind White Hats jedoch nicht unauffällig. Auch die Gruppe der ethischen Hacker unterscheidet sich signifikant von der Norm in Bezug auf primäre und sekundäre Psychopathie ($d = 0.23$ für beide Subskalen), wobei diese nach Cohen (1988) als schwache Effekte zu deuten sind.

5.10.8 Quelle der Fähigkeiten

H11: White Hat Hacker haben ihre Fähigkeiten häufiger durch formelle Bildungsquellen (z. B. Universität) erworben, während Black Hat Hacker diese häufiger über informelle Quellen (z.B. Darknet) erlernt haben.

Mittels fünf Wahloptionen mit Beispielen und einer Freitextoption wurden Hacker gefragt, wo bzw. wie sie ihre Hackingfähigkeiten gelernt haben.

Tabelle 12: Deskriptive Statistik: Prozentuale Häufigkeiten, Quelle der Hackingfähigkeiten (Mehrfachauswahl möglich)

	Black Hats ($n = 333$)	White Hats ($n = 850$)
Self Study (e.g. Books, Blogs, YouTube)	91 %	90 %
Hacker Communities (e.g. Forums, Darknet, Telegram)	69 %	56 %
Mentor	14 %	16 %
Hands-On Challenges (CTFs, Hackathons)	44 %	59 %
Formal Education (University, Courses)	23 %	42 %
Others	7 %	4 %

Die Hypothese bezieht sich - im Kontext von Lerntheorien - darauf, dass White Hats ihre Fähigkeiten öfter auf der ‚hellen Seite‘ lernen (z.B. formelles Universitätsstudium) und Black Hats eher auf der ‚dunklen Seite‘ (z.B. Darknet-Foren).

Die Hypothese kann bestätigt werden: Die größten Prozentsatzdifferenzen der Stichproben zeigten sich in den Kategorien der Hacker-Foren und formeller Ausbildung. 69 % der Black Hats geben an, dass auch Online-Hacker-Communities beim Erwerb der Hackingfähigkeiten eine Rolle spielten, wobei es bei den White Hats nur 56 % sind (Prozentsatzdifferenz = 13). Noch etwas größer ist die Differenz bei der formellen Bildung; diese hat bei 23 % der Black Hats und 42 % der White Hats eine Rolle gespielt (Prozentsatzdifferenz = 19).

Die Unterschiede sind jedoch nicht so groß wie erwartet. Auch die Mehrheit der White Hats lernt ihre Fähigkeiten u.a. in Hacker-Foren im Darknet. Dass Black Hats ihre Fähigkeiten weniger oft durch das Studium lernen, kann auch auf die Altersdifferenz zurückzuführen sein, da Black hat Hacker jünger sind und noch am Anfang der akademischen Laufbahn stehen.

Dies liefert einen Hinweis und Präventionsansatz, dass auch die Quelle der Fähigkeiten eine Rolle spielen kann, wobei die Daten grundsätzlich keine Kausalschlüsse zulassen.

5.10.9 Der Online Disinhibition Effect

H12: Die Anonymität des Internets führt zu einer Enthemmung im Online-Verhalten bei Black Hat- und White Hat Hackern.

Im Befragungsinstrument wurden drei kriminelle Verhaltensweisen beschrieben (englischsprachig), jeweils in ihrer Online- und Offline-Variante: (1) Illegal Filme streamen vs. ohne Ticket in ein Kino schleichen, (2) das Bankkonto von Einzelpersonen hacken vs. Einzelpersonen die Geldbörse stehlen und (3) Unternehmen hacken vs. Unternehmen offline bestehlen. Moralisch unterscheiden sich die Taten nicht, jedoch im zur Tatausführung genutzten Medium oder Tatmittel. Zu jeder hypothetischen Tat wurde die Zustimmung, ob Hacker dies tun würden, auf einer 5-stufigen Likert-Skala von 1 (= *Strongly Disagree*) bis 5 (= *Strongly Agree*) erfasst, (z.B. „I would hack someone's bank account“).

Zur Prüfung der Hypothese, ob eine Enthemmung besteht, wurde aus den drei Online-Verhaltensweisen ein Mittelwert gebildet (= Online-Skrupellosigkeit) und aus den 3 Offline-Taten (= Offline-Skrupellosigkeit). Die Reliabilitätskoeffizienten (Cronbachs Alpha) sind in Anhang 4 aufgeführt.

Tabelle 13: Deskriptive Statistik: Online-Disinhibition Effect

Hackergruppe	<i>M (SD)</i> Online-Skrupellosigkeit	<i>M (SD)</i> Offline-Skrupellosigkeit	Differenz
Black Hats (<i>n</i> = 321)	3.65 (0.99)	2.65 (1.14)	1
White Hats (<i>n</i> = 834)	2.73 (0.97)	1.90 (0.89)	0.83

Bestünde ein Disinhibition Effect, müsste es eine Diskrepanz zwischen der berichteten Online-Skrupellosigkeit und Offline-Skrupellosigkeit geben. Das bedeutet hier ist nicht primär der Vergleich *zwischen* den Gruppen von Interesse, da zu erwarten war, dass Black Hats skrupelloser und enthemmter sind. Interessant ist der Vergleich online vs. offline innerhalb der Hackergruppen. Obwohl es sich moralisch um identische Taten handelt, scheinen Hacker im Cyberraum enthemmter zu agieren, als sie es offline tun würden. Sowohl bei Black Hats als auch bei White Hats zeigt sich deskriptiv eine deutliche Differenz zwischen der Skrupellosigkeit online vs. offline.

Um zu überprüfen, ob es sich dabei um signifikante Unterschiede handelt, wurde je Hackergruppe ein *t*-Test für abhängige Stichproben durchgeführt (zweiseitig) und die Mittelwerte der beiden Variablen ‚Online-Skrupellosigkeit‘ und ‚Offline-Skrupellosigkeit‘ verglichen. Black Hats (*n* = 321) verhalten sich im Cyberspace signifikant skrupelloser, als sie es in der analogen Welt tun würden ($t(320) = 18.17, p < .001$), mit einer mittleren Differenz von einem Skalenpunkt auf einer 5-stufigen Likert-Skala (95 %-CI [0.89, 1.10]). Cohen's *d* liegt bei $d = 1.01$ und fällt demnach in die Kategorie eines starken Effektes. Doch auch White Hat Hacker (*n* = 834) agieren signifikant enthemmter im Cyberspace ($t(833) = 29.80, p < .001$) mit einer mittleren Differenz von 0.83 Skalenpunkten. Auch dies ist ein starker Effekt in derselben Größenordnung mit $d = 1.03$.

Die Hypothese kann bestätigt werden. Es besteht ein Online Disinhibition Effect, also eine enthemmende Wirkung des Cyberraums. Es konnten gemäß Cohen (1988) starke Unterschiede zwischen der Online-Skrupellosigkeit und Offline-Skrupellosigkeit bei Black Hats ($d = 1.01$), aber im gleichen Maße auch bei White Hats ($d = 1.03$), gefunden werden. Da der Effekt bei beiden Gruppen gleich stark auftritt, dient er im Sinne der Kriminalätiologie weniger als Erklärung für Black Hat Hacking.

H13: Black Hats schätzen das Entdeckungsrisiko geringer ein als White Hats.

Das subjektiv wahrgenommene Entdeckungsrisiko wurde durch zwei Items operationalisiert („The police are incompetent when it comes to handling Cybercrime“ und „I believe there is a very low chance of being caught when engaging in illegal hacking activities“). Gemeinsam bilden diese Items die *wahrgenommene Entdeckungswahrscheinlichkeit*. Der Cronbachs Alpha-Wert von .57 ist in Anbetracht der Tatsache, dass die ‚Skala‘ aus nur zwei Items besteht, akzeptabel. Es wurde ein t -Test für unabhängige Stichproben (zweiseitig) durchgeführt, um Black Hats ($n = 321$) und White Hats ($n = 834$) zu vergleichen. Der Levene-Test war nicht signifikant ($F(1, 1153) = 3.61, p = .058$).

Die Hypothese kann bestätigt werden: Black Hat Hacker schätzen die Chance, *nicht* von Strafverfolgungsbehörden entdeckt zu werden, höher ein ($M = 3.71, SD = 1.03$) als White Hats ($M = 3.32, SD = 0.98$). Der Unterschied ist signifikant mit $t(1153) = 5.94, p < .001$ und mittlerer Differenz von 0.39. Es handelt sich um einen schwachen Effekt von $d = 0.39$.

H14: Der Einstellung, dass Opfer ‚selbst schuld‘ seien, wenn sie gehackt werden, stimmen Black Hats signifikant stärker zu als White Hats.

Das Konstrukt der Schuldexternalisierung wurde durch ein Item operationalisiert, das die Zustimmung zu der Aussage abfragt, ob Opfer selbst schuld seien, gehackt zu werden, wenn sie schwache Passwörter nutzen. Der Mittelwert der Zustimmung der Black Hats ($n = 321$) liegt bei $M = 4.02$ (Agree), $SD = 1.2$. Erstaunlicherweise stimmen aber auch White Hats der Aussage in ähnlichem Maße zu ($M = 3.76, SD = 1.23$). Zur Prüfung auf Signifikanz der

Unterschiede wurde erneut ein zweiseitiger t -Test für unabhängige Stichproben durchgeführt. Es kann Varianzhomogenität angenommen werden (Levene-Test: $F(1, 1153) = 0.996, p = .319$). Die Mittelwertsunterschiede zwischen den Gruppen waren signifikant, $t(1153) = 3.26, p = .001$. Die Effektstärke nach Cohen (1988) lag bei $d = 0.21$ und entsprach somit einem kleinen Effekt. Die Hypothese kann bestätigt werden, auch wenn es sich nur um einen kleinen Effekt handelt.

5.10.10 Motive von Hackern und Korrelationen mit Triademerkmale

H15: Hacking ist nicht nur durch finanziellen Gewinn motiviert, es liegen zeitgleich mehrere Motive vor.

Black Hat Hacker wurden aufgefordert, aus einer Liste mit 10 aus der Literatur abgeleiteten übergeordneten Motivkategorien alle Motive auszuwählen, die zutreffen, wobei eine Mehrfachauswahl möglich war. Black Hat Hacker nannten im Durchschnitt 4-5 Motive ($M = 4.46, SD = 2.17$). Finanzieller Gewinn wurde zwar von 48.8 % der Black Hats als Motiv genannt, noch deutlich häufiger gaben Hacker jedoch an, dass Challenge (76,3 %), Thrill (59,3 %), Spaß/Trolling (55,7 %) und Machtgefühle (50,9%) sie motivieren, zu hacken. Abbildung 37 zeigt die prozentualen Häufigkeiten der Nennungen je Motivkategorie.

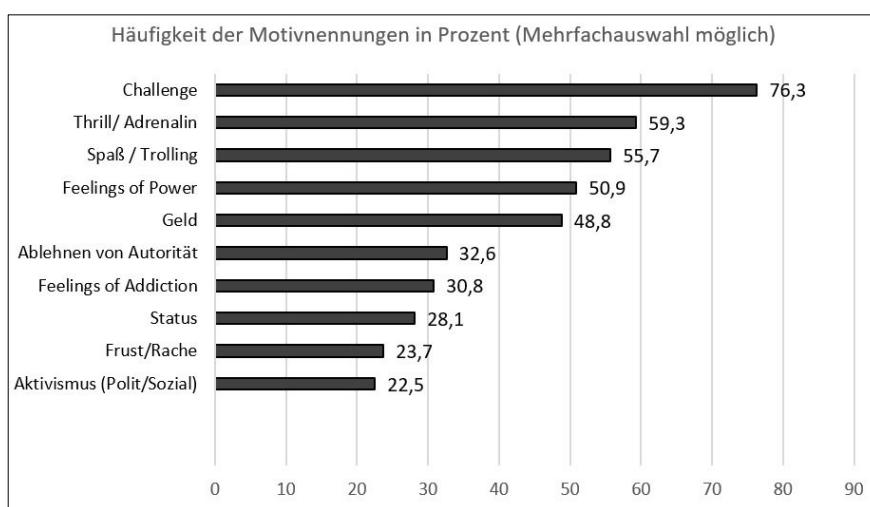


Abbildung 37. Prozentuale Häufigkeiten der Nennungen: Motive von Black Hat Hackern

Anmerkung. Die Frage nach kriminellen Hacking-Motiven wurde nur der Gruppe der Black Hats gestellt ($n = 321$), Mehrfachnennungen waren möglich.

Auch das Motiv ‚Sucht‘ („Feelings of Addiction“) haben 30,8% der Black Hats als Motivkategorie angegeben. In Anbetracht der durchschnittlichen Anzahl, Rangfolge und inhaltlichen Diversität der Motive lässt sich die Hypothese bestätigen, dass Black Hat Hacking (*Cybercrime im engeren Sinne*) nicht nur durch Geld motiviert ist, sondern bei Hackern von Motivbündeln von 4-5 Motiven auszugehen ist, die gleichzeitig vorliegen.

H16: Es bestehen signifikante Korrelationen zwischen Merkmalen der Dunklen Triade und Motiven von Black Hat Hackern.

Im Gegensatz zu vorherigen Hypothesen bezieht sich diese nicht auf Gruppenunterschiede, sondern auf Zusammenhänge zwischen Tatmotiven und Persönlichkeitsmerkmalen (Zusammenhangshypothese). Die 10 Motivkategorien konnten jeweils entweder ausgewählt (2 = *checked*) oder nicht ausgewählt (1 = *not checked*) werden (dichotom). Die Merkmale der Dunklen Triade (SD3) und primären & sekundären Psychopathie (LSRP) sind metrisch skaliert. Die Hypothese wurde daher mit der punktbiserialen Korrelation überprüft, die wiederum einen Spezialfall der Pearson-Korrelation darstellt. Die Frage nach den Motiven bezog sich ausschließlich auf kriminelles Hacking und wurde nur der Stichprobe der Black Hats gestellt. Da die Fallzahl mit $n = 321$ deutlich über 30 liegt, kann gemäß des Grenzwertsatzes von Normalverteilung ausgegangen werden (Bortz & Schuster, 2010). In beiden dichotomen Ausprägungen aller 10 Motive war die Fallzahl pro Ausprägung mindestens $n > 65$.

Es wurden punktbiserielle Korrelationen zwischen den fünf metrischen Persönlichkeitskonstrukten Psychopathie (SD3), Machiavellismus (SD3), Narzissmus (SD3), primärer Psychopathie (LSRP), sekundärer Psychopathie (LSRP) und 10 dichotomen Motivkategorien untersucht. Im Fragebogen wurden ausführlichere deskriptive Beschreibungen der Motive aufgeführt (z.B. „Peer recognition in hacking culture/ Status“ oder „I enjoy the „Thrill“/ adrenaline“), während hier zwecks Lesbarkeit folgende Kurzlabels für Hacking-Motive verwendet werden: (1) Geld, (2) Challenge, (3) Anerkennung, (4) Macht, (5) Sucht, (6) Thrill, (7) Anti-Autorität, (8) Aktivismus, (9) Spaß und (10) Rache.

Die Hypothese kann bestätigt werden. Es bestehen signifikante (schwache) Korrelationen zwischen Persönlichkeitsmerkmalen und Motiven. Der vollständige SPSS-Output findet sich in Anhang 4. Die Abbildung 38 zeigt pro Persönlichkeitsmerkmal die drei stärksten Motiv-Korrelationen als Pfeil (r_{pb} -Werte), sofern diese zweiseitig signifikant waren.

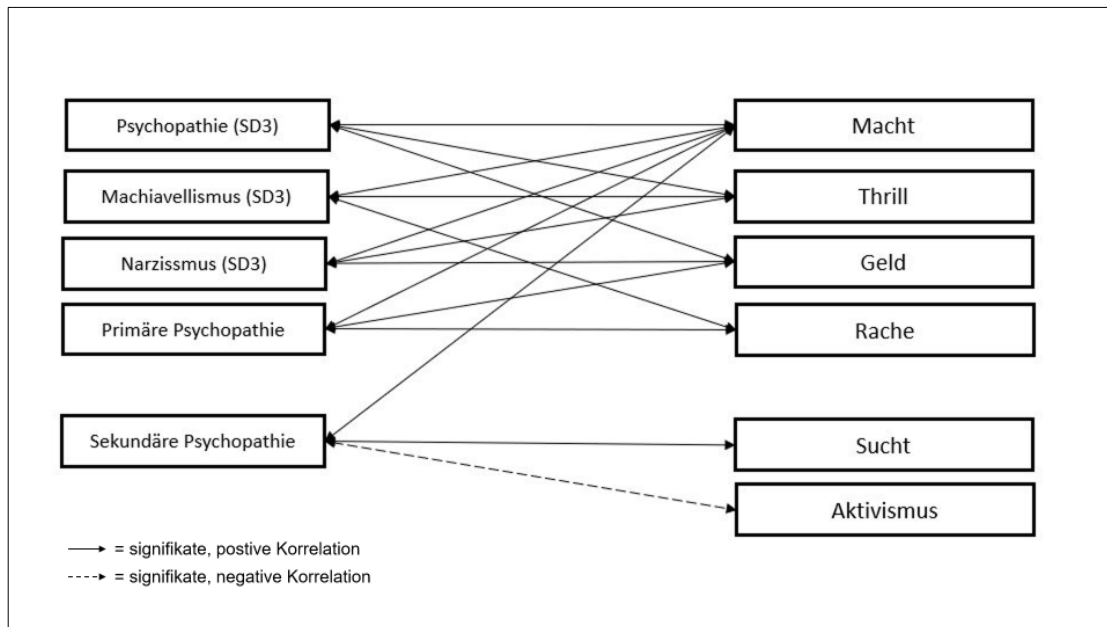


Abbildung 38. Darstellung der stärksten Korrelationen zwischen Triademerkmale und Hacking-Motiven

Anmerkung. $n = 321$ Black Hat Hacker haben die Frage nach Motiven beantwortet.

Machiavellismus (SD3) korrelierte am stärksten positiv mit den Motiven Macht ($r_{pb}(321) = 0.23, p < .001$), Thrill ($r_{pb}(321) = 0.21, p < .001$) und Rache ($r_{pb}(321) = 0.20, p < .001$).

Psychopathie (SD3) korrelierte am stärksten positiv mit den Motiven Macht ($r_{pb}(321) = 0.26, p < .001$), Geld ($r_{pb}(321) = 0.26, p < .001$) und Thrill ($r_{pb}(321) = 0.26, p < .001$).

Narzissmus (SD3) korrelierte am stärksten positiv mit den Motiven Macht ($r_{pb}(321) = 0.24, p < .001$), Geld ($r_{pb}(321) = 0.22, p < .001$) und Thrill ($r_{pb}(321) = 0.13, p < .017$).

Primäre Psychopathie (LSRP) korrelierte am stärksten positiv mit den Motiven Geld ($r_{pb}(321) = 0.30, p < .001$), Rache ($r_{pb}(321) = 0.21, p < .001$) und Macht ($r_{pb}(321) = 0.21, p < .001$).

Sekundäre Psychopathie (LSRP) korrelierte am stärksten positiv mit den Motiven Macht ($r_{pb}(321) = 0.18, p < .003$), aber auch Sucht ($r_{pb}(321) = 0.14, p < .028$) und negativ mit dem Motiv Aktivismus ($r_{pb}(321) = -0.18, p < .005$).

5.10.11 Persönlichkeitsmerkmale und Angriffsmethoden

H17: Es gibt Korrelationen zwischen Persönlichkeitsmerkmalen der Täter und dem bevorzugten Modus Operandi bei Cyberangriffen, die damit eine Grundlage für psychologisches Cyberprofiling bilden.

Der bevorzugte Modus Operandi bei Cyberangriffen wurde dichotom in den Kategorien *Social Engineering* vs. *Technische Hacks* erfasst. Es geht hier also um den bevorzugten Angriffsvektor Mensch vs. Technik (dichotom) und Merkmale der Dunklen Triade (metrisch). Zur Prüfung des Zusammenhanges zwischen den dichotomen und metrischen Variablen wurde die punktbiseriale Korrelation (zweiseitig) gewählt, da die Hypothese auf Zusammenhänge abzielt. Auch hier wurden nur Black Hat Hacker in die Berechnung einbezogen und bei einer Fallzahl von $n = 332$ kann von einer Normalverteilung ausgegangen werden.

Die Variable ‚Type_of_Attack‘ wurde so umcodiert (1 = *Technische Hacks*, 2 = *Angriffsvektor Mensch*), dass positive Korrelationen als Vorliebe für den Angriffsvektor Mensch zu deuten sind.

Primäre Psychopathie (LSRP) korreliert schwach positiv mit einer Vorliebe für Social Engineering ($r_{pb}(263) = .22, p < .001$). Ähnlich schwache, positive Korrelationen konnten für die SD3 Subskalen Machiavellismus ($r_{pb}(332) = .21, p < .001$) und Psychopathie identifiziert werden ($r_{pb}(332) = .17, p = .002$). Für Narzissmus und sekundäre Psychopathie wurden keine signifikanten Korrelationen mit dem bevorzugten Modus Operandi bei Cyberangriffen gefunden.

Die Hypothese kann bestätigt werden. Es bestehen signifikante, positive Zusammenhänge zwischen dem Modus Operandi und einigen Persönlichkeitsmerkmalen der Dunklen Triade. Primäre Psychopathie und Machiavellismus sind leicht, aber signifikant mit der Angriffsart des Social Engineerings assoziiert.

5.10.12 KI-Nutzung

H18: Mehr als 50 % der Hacker haben bereits künstliche Intelligenz für Hacking-Aktivitäten eingesetzt.

$n = 333$ Black Hats und $n = 850$ White Hats haben die Frage beantwortet, ob sie bereits Künstliche Intelligenz konkret für Hacking-Aktivitäten eingesetzt haben und wenn ja, welche KI-Anwendungen oder LLMs. Die Hypothese kann nicht bestätigt werden. 42% der Black Hat Hacker und 41.5 % der White Hat Hacker gaben an, bereits KI für Hacking-Aktivitäten genutzt zu haben. Glücklicherweise hat die kriminelle Seite hier keinen Vorsprung, die Stichprobe der White Hat Hacker und Black Hat Hacker unterscheidet sich nicht bedeutsam. Für die Zukunft der Cybersicherheit ist besonders bedeutsam, welche KI-Tools die kriminellen Hacker nutzen. Während einige Black Hats legitime KI-Modelle (wie ChatGPT) missbrauchen, z.B. durch so genannte Jailbreak-Prompts, gibt es im Darknet auch KI-Modelle wie *WormGPT*, die ausschließlich für Zwecke der Cyberkriminalität geschaffen wurden.

Insgesamt haben Black Hat Hacker 21 unterschiedliche, identifizierbare KI-Modelle genannt, die sie zum Zweck des Hackings einsetzen. Am häufigsten genannt wurden ChatGPT (57 Nennungen), Deepseek (28 Nennungen), WormGPT (8 Nennungen), Copilot, Gemini und Claude mit je 3 Nennungen. Weitere Nennungen waren PentestGPT, HackerGPT, ChaosGPT, Grok, WhiteRabbitNeo, Roo Code, Manus, DanGPT, Ollama, Codegen, BlackBoxAI, Qwen, HuggingFace, CursorIDE sowie Open Source-Lösungen auf der Plattform GitHub.

Das populärste KI-Modell in der Stichprobe der Black Hats war also ChatGPT, einige Black Hat Hacker präzisierten, wofür sie ChatGPT einsetzen:

„I've used ChatGPT to automate some things and learn more about 'human hacking'”

„ChatGPT for malware reinforcement”

„I've used chatgpt to generate me scripts for certain work”

„Chatgpt used to discuss exploit ideas”

„I use ai to help me in hacking and finding vulnerabilities”

„Not for social engineering but to make research more specific and to narrow down focus”

„I've used deepseek to clone social media sites for phishing”

Insgesamt lässt sich festhalten, dass 42% der Black Hats (Stand 2025) bereits KI-Modelle für Hacking-Aktivitäten einsetzen. Während ChatGPT und Deepseek am beliebtesten sind, ist das Spektrum eingesetzter KI-Modelle breit. Die Einsatzmöglichkeiten sind dabei primär Recherche und fachliche Diskussionen, aber auch Malwareentwicklung, Generierung von Phishing-Seiten und Automatisierung.

5.11 Diskussion

5.11.1 Sonstige Felderfahrungen

Neben den quantitativen Ergebnissen traten im Verlauf der Feldphase auch eine Reihe von Beobachtungen und Kontextinformationen auf, die nicht unmittelbar Teil des Erhebungsinstrumentes waren, jedoch interessante Einblicke in die Realität und Innenperspektive der Zielgruppe bieten und daher ebenfalls transparent dokumentiert werden sollen.

OpSec-Paranoia, Doxxing, Cyberangriffe

Black Hats achten penibel auf ihre *Operational Security*. Dokumente wie die *OpSec Bible* oder „The Hitchhiker’s Guide to Online Anonymity” (Anonymous Planet, 2023, S.1) bieten auf hunderten Seiten Anleitungen zur vollständigen Online-Anonymität. Darin enthalten sind Tipps zu PGP-Verschlüsselung (Anonymous Planet, 2023, S. 78), die Empfehlung, Geräte in Taschen aufzubewahren, die als faradaysche Käfige fungieren (S. 85) oder, dass das Smartphone selbst im ausgeschalteten Zustand Signale senden könne (Anonymous Planet, 2023, S. 33). In Darknet-Foren wie *Dread* heißt es im Titelbild des Subforums *d/OpSec*: „Distrust and caution are the parents of security“ (Dread, 2025c).

Probiert man als Forscher, in diesem Kontext Daten für wissenschaftliche Zwecke zu gewinnen, gerät man schnell in den Verdacht, dass die Studie eine Täuschung sei und es sich in Wahrheit um eine verdeckte Operation von Polizei oder Nachrichtendiensten handele. Hacker sprechen oft von ‚den FEDs‘ oder ‚den Federals‘, womit sie die Federal Agencies meinen (also vor allem Bundesbehörden der USA, wie CIA, FBI, NSA etc.). Tritt man proaktiv mit Black Hats in Kontakt und lädt sie ein, anonym für Forschungszwecke an einer Studie teilzunehmen, ist eine häufige Antwort: „Nice try, feds“.

Das Rekrutierungsvideo und die entsprechende Kampagne hatte eine größere Reichweite erzielt als erwartet, was zu einer guten Fallzahl führte, aber auch eine Gegenreaktion provozierte. Ein Nutzer verbreitete im Darknet die Warnung bzw. den Vorwurf, dass es sich um eine verdeckte Operation handeln würde (Abb. 39).

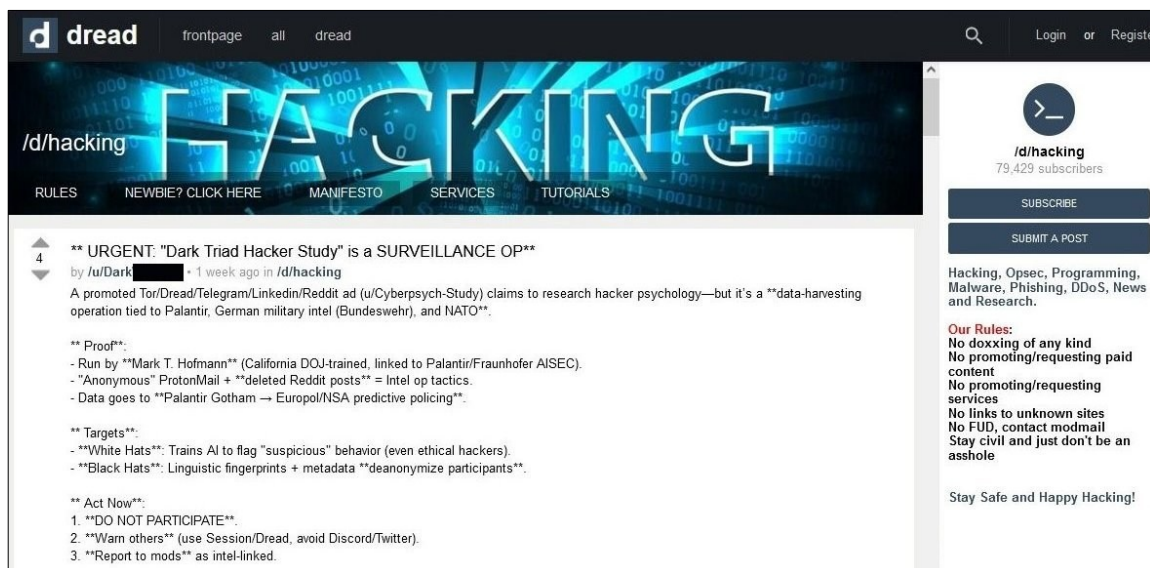


Abbildung 39. Screenshot Dread (Darknet): Surveillance-Operation-Vorwurf und Doxxing

Quelle: Dread (2025e) (Darknet-Unterforum d/hacking)

Als angebliche Beweise wurden die Identität des Forschenden sowie wahre und teils konstruierte Verbindungen zu Strafverfolgungsbehörden und Nachrichtendiensten aufgezeigt. Alle Black Hats wurden aufgefordert, (1) auf keinen Fall teilzunehmen, (2) andere zu warnen und (3) alle Beiträge und Teilnahmeaufrufe sofort an die Moderatoren der Foren zu melden. In einem Kommentar führte derselbe Nutzer weiter aus:

„This is not a PhD project. This is a federated surveillance operation, masquerading as academic research and whether you are white hat, black hat or just spectate from the sidelines - you're a target. They want your patterns, your tendencies, your weaknesses. And they're pushing hard to get it - on reddit, Linkedin, Telegram, Dread and everywhere else where hackers speak freely. I am just doing my part to protect whoever I can. This affects everyone in our space - red team, blue team, grey zone, whatever. Doesn't matter if you're a bug bounty pro or darknet op. Hofmann's operation aims to profile anyone with hacking ability - not just behavior but mindset.” (Dread, 2025e)

In Verbindung mit diesem Vorwurf, es sei eine verdeckte Operation, wurde ein Darknet-Download-Link zu einem vollständigen Bericht geteilt, dieser enthielt Fotos des Forschenden, Social Media-Profile, die eigene Büroadresse, Website sowie alle Plugins (technische Module), die auf der persönlichen Website genutzt werden.

In einem Darknet-Hackerforum Fotos, Adresse, Social Media-Profile und technische Komponenten der Website einer Person zu teilen, ist als indirekter Aufruf zum Angriff zu verstehen. Diese Praxis nennt sich Doxxing. Infolgedessen wurde die eigene Cybersicherheit nochmals geprüft und verbessert sowie aus persönlichen Sicherheitsgründen auch die Büroadresse gewechselt.

Auch auf den entsprechenden Hacker-Foren auf Reddit wurde (vom selben Nutzer) vor der Studie gewarnt; hierbei war vor allem ein Satz kennzeichnend für die Felderfahrungen im Umgang mit Hackern insgesamt:

But the worst mistake you can make? Assuming it's harmless.



Rule #1 in the Darknet: Paranoia Keeps You Free.

If you see this account (or others like it), **do not engage**. Spread the word instead.

Abbildung 40. Screenshot Reddit Hacking-Forum: OpSec-Paranoia

Quelle: Reddit (2025), Subreddit DarkWireSys

Cyberangriffe konnten nicht festgestellt werden, es gab aber einen Versuch, den Fragebogen zu hacken über eine Eingabe von Schadcode im Freitextfeld.

Für künftige Studien ist zu bedenken, dass empirische Forschung in Hacker-Foren und dem Darknet zwar möglich ist, aber mit hohen Sicherheitsvorkehrungen einhergehen muss: Zum Schutz der Anonymität der Teilnehmer, aber auch zum Eigenschutz.

Forschungsethisch ist es nötig, auf der Einwilligungsseite Informationen über den Zweck und Forschende als Klarnamen bereitzustellen; es muss aber auch klar sein, dass jede E-Mail-Adresse, physische Adresse und Telefonnummer im Darknet gegen die eigene Zustimmung publiziert werden kann und auch dauerhaft nicht löscherbar ist.

Hackerethik: Robin-Hood-Mentalität

Wissen Black Hats, dass sie Black Hats sind? Es wurde angenommen, dass Black Hat Hacker und vor allem die, die aus finanziellen Motiven hacken, wissen, dass sie Black Hat Hacker sind und es auch keinen Weg gibt, das zu verschleiern. Doch die Grenzen sind nicht ganz so trennscharf. In einem Darknet-Fraud-Forum reflektiert ein Hacker über moralische Fragen im Zusammenhang mit Betrug und gibt selbst zu, dass es paradox sei, Verhalten wie kriminelles Hacking überhaupt ethisch einzuordnen. Aber auch unter Black Hat Hackern gibt es informelle moralische Regeln und Grenzen. Innerhalb der Cyberkriminalität gibt es eine Moral im Unmoralischen. Unter dem Titel ‚Steal From Corporations, Not Individuals‘ hat ein Hacker eine Art moralisches Essay verfasst (siehe Abb. 41).

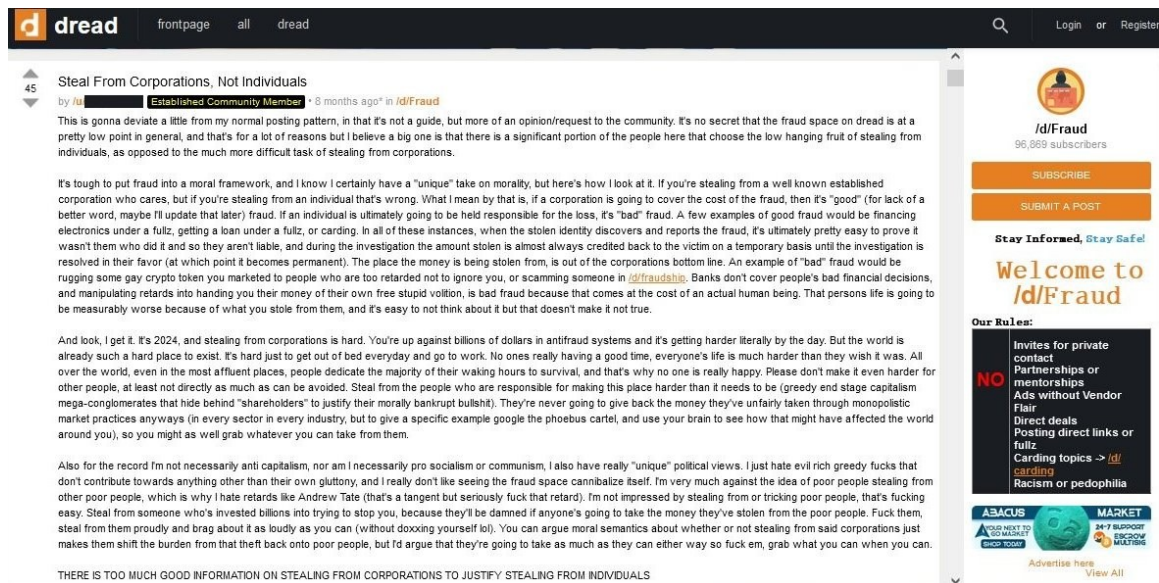


Abbildung 41. Screenshot Dread (Darknet): Subforum *d/fraud*

Quelle: Dread (2025d) (Darknet-Unterforum *d/fraud*)

Die Grundregel lautet hier, von Unternehmen zu stehlen. Es wird kritisiert, dass viele Hacker den einfacheren Weg gehen und von Einzelpersonen stehlen. Es wird zwischen ‚good fraud‘ und ‚bad fraud‘ (gutem vs. schlechtem Betrug) unterschieden. Viele Hacker halten sich für moralisch überlegen, weil sie ‚nur‘ Unternehmen angreifen, aber niemals Einzelpersonen angreifen würden. In manchen Darknet-Foren schlägt dies in einen regelrechten Hass gegenüber ‚Third World scammers‘ um. So schrieb einer der anonymen Moderatoren des Dread-Hacker-Forums *d/SocialEngineering* den Kommentar: „Seing all you third world scammers posting ‚help me with my phishing‘ ‚help me with my e-mail spamming‘ makes me sick“ (Dread, 2025a).

Analysiert man die Texte zur Ethik, werden drei Gründe vorgebracht, warum das Hacken von Unternehmen moralisch besser sei als das von Einzelpersonen. Das erste Argument fällt in die Kategorie, dass Unternehmen derartige Verluste gar nicht spüren würden. Das ist falsch, da Cyberangriffe auf Unternehmen oft zu Entlassungen, Reputationsverlusten oder sogar Insolvenz führen und somit Anteilseigner und Belegschaft direkt treffen. Das zweite Argument ist, dass man ja eher Reichen als Armen schadet. Es ist kein Verbrechen, erfolgreich zu sein, und auch dieses Argument wird hier zurückgewiesen. Das dritte Argument ist die technische

Herausforderung. Einzelpersonen anzugreifen, wird metaphorisch als das Abgreifen der ‚low hanging fruits‘ beschrieben. Viele Black Hat Hacker verachten den einfachen Kreditkartenbetrug und bewundern technisch versierte Angriffe. Doch der Schwierigkeitsgrad eines Angriffs macht diesen nicht moralisch besser. Das zentrale Argument folgt einer Robin-Hood-Mentalität: Man nehme es nur von den Reichen (z.B. von Großkonzernen) und verachte gleichzeitig ‚Third World Scammer‘. Doch das ist inkonsequent: Gerade Hacker aus Ländern mit extremer Armut könnten behaupten, es ja ebenfalls nur von wohlhabenden Personen aus dem Westen zu nehmen. Ein Teilnehmer der Befragung (männlich, Black Hat und nach eigenen Angaben aus Brasilien) schrieb bei der Frage nach den Motiven für das Hacking in das Freitextfeld „Revenge against poverty“ - also Rache für Armut.

Das Freitextfeld des Fragebogens nutzten einige Teilnehmer für recht ausführliche Ergänzungen und Erklärungen, z.B.:

„It's funnt [sic] because for many things on the quiz I think 'oh, I would never do that' but then think about it and realized [sic] I've already done it. Also, it's not mentioned here but all the times I hacked something in a situation that could be conceived as illegal, I always gifted what I obtained. Either clothes for my sister or having dinner with my friends.“

Ob Geld zu stehlen, um danach mit Freunden essen zu gehen, dies zu einem Akt der Wohltätigkeit macht, lässt sich stark anzweifeln, dies ist jedoch die Innenperspektive der Täter.

Es bleibt festzuhalten, dass Black Hats auf allen Ebenen ausgeprägte Rechtfertigungsstrategien haben, um zu rechtfertigen, warum ihr Verhalten ja gar nicht so schlimm sei.

Reproduktion des eigenen Klischees

In Hollywood-Produktionen und Netflix-Serien werden Hacker gerne maskiert, düster und mit schwarzen Kapuzenpullovern dargestellt. Viele Hacker reproduzieren aktiv dieses Klischee:

In Telegram-Gruppen inszenieren sie sich mit düsteren Designs, schwarzen Hoodies und typischen Hollywood-Bildern. Das Hacker-Stereotyp wird zum Teil nicht kritisiert, sondern eher zelebriert. Dies lässt sich so deuten, dass das düstere Image, inklusive Gruselfaktor und Illegalität, Teil der Faszination und des Reizes ist. Das Darknet ist mit wenigen Ausnahmen recht dunkel gestaltet. Technisch gibt es keinen Grund, warum Darknet-Foren und Marktplätze nicht genauso nutzerfreundlich designet sein können wie Websites im Clearnet. Es gibt einige Ausnahmen, dennoch ist das dunkle Thema ein wiederkehrendes Element. Dieses Phänomen ließe sich als eine Art ‚Freude am Bösen‘ bzw. *Joy to be evil* beschreiben.

5.11.2 Zusammenfassung und Bewertung der zentralen Befunde

Die Hauptforschungsfrage war, inwiefern sich Black Hat Hacker und White Hat Hacker unterscheiden. Hierbei geht es primär um die Kriminalätiologie: Warum nutzen die einen Hacker ihre Fähigkeiten zur Cyberabwehr und die anderen für eine kriminelle Karriere?

Hierzu konnten 1.185 Hacker anonym befragt werden, 851 White Hats und 334 Black Hats, durch eine Rekrutierung u.a. in Darknet-Hackerforen.

Ergebnis 1: Black Hat Hacker sind im Durchschnitt junge, intelligente, gut qualifizierte, computeraffine Männer. Hacking ist nicht nur durch Geld motiviert, sondern durch Motivbündel von 4-5 Motiven. Die bedeutsamsten Motive sind Herausforderung, Thrill und Spaß (,Trolling‘).

Demografisch zeigte sich in der selbstselektierten Stichprobe ein erstaunlich homogenes Bild. Es handelt sich bei Hackern (Black Hats und White Hats) mehrheitlich um junge, gut qualifizierte Männer. Relevant für Zwecke der Prävention sind besonders die Profile und Motive der kriminellen Black Hat Hacker: Die Stichprobe war zu rund 90 % männlich, 92 % Akademiker oder auf dem Weg dahin und 70 % unter 28 Jahre alt. Die erhobenen Daten decken sich mit Ergebnissen der ersten Studie und anderen empirischen Studien und Meta-Analysen (BKA, 2015b). Black Hat Hacker nannten im Durchschnitt 4.46 Motive pro Person. Damit wird deutlich, dass Cyberkriminalität nicht monokausal ist. Die Frage nach *dem* Motiv

der Hacker greift zu kurz, es ist eher von Motivbündeln auszugehen mit 4-5 Motiven pro Person, die *gleichzeitig* vorliegen.

Es ergaben sich jedoch auch teilweise Widersprüche zur diskutierten Literatur (Kapitel 3). Die Aussage von Wernert (2021, S. 39) „[d]er überwiegende Teil der Cyberkriminellen handelt aus finanzieller Motivation“ kann so nicht bestätigt werden. Finanzieller Gewinn wurde nur von 48.8 % der Black Hats als ein Motiv genannt und rangierte nur auf dem fünften Platz der genannten Motive, deutlich hinter Herausforderung (76.3 %), Thrill (59.3 %), Spaß (55.7 %) und Macht (50.9 %). Andersherum formuliert, haben über 50 % (also die Mehrheit) der Black Hat Hacker finanziellen Gewinn gar nicht als Motivkategorie angegeben. Natürlich kann hier auch auf Seiten der Täter eine idealisierende Selbsttäuschung vorliegen, da es durchaus edler wirken könnte, zu behaupten, intrinsisch motiviert zu sein. Es bleibt jedoch festzuhalten, dass Black Hats im Durchschnitt jung und gut qualifiziert sind; sie könnten demzufolge auch auf legalem Wege ein gutes Einkommen erzielen. Viele Black Hat Hacker hätten berufliche Alternativen und sind als akademische Fachkräfte im IT-Bereich keineswegs perspektivlos. Wer legal ähnlich viel verdienen könnte und sich *trotzdem* für Kriminalität entscheidet, kann somit nicht allein durch Geld motiviert sein.

Etwa ein Drittel der befragten Black Hat Hacker führte auch Rebellion und das Ablehnen von Autorität als motivationalen Faktor an. Dies spiegelt sich auch in dem Verhalten wider, dass Hacker anonyme, dezentrale Technologien bevorzugen wie Linux, Bitcoin und den Tor-Browser. Ebenfalls rund 30 % berichteten von Suchtgefühlen im Zusammenhang mit dem Hacking. Die Tatsache, dass cyberkriminelles Verhalten, wie z.B. Online-Glücksspiel, ein Suchtverhalten darstellen kann, wurde bislang empirisch kaum beachtet und erfordert weitere Forschung.

Die Motivkategorie ‚Status‘ wählten lediglich 28,1 % der Black Hats als Motiv, was jedoch zu dem Befund passt, dass auch die Narzissmus-Scores der Black Hat Hacker deutlich moderater als erwartet ausfielen. Die beiden Motivkategorien ‚Frust/Rache‘ und ‚Aktivismus‘ wurden am seltensten ausgewählt, wobei Letzteres auf die Stichprobenstruktur

zurückzuführen sein dürfte. Ideologisch, politisch oder aktivistisch motivierte Hacker werden als Gray Hat Hacker definiert, wobei die Studie auf White- und Black Hats abzielte.

Zusammenfassend lässt sich aus den erhobenen Daten ein abgrenzbares Hackerprofil bilden: Junge, intelligente, computeraffine Männer auf der Suche nach Herausforderung, Thrill und Unterhaltung. Dieses Profil kann zum Zwecke *selektiver Prävention* (Bürger & Kaess, 2024) genutzt werden, um entsprechende Risikogruppen zu erreichen und ggf. frühzeitig zu intervenieren. Neugierde und auch die Suche nach Spaß und Herausforderung sind an sich positive Attribute, welche durchaus in legale Bahnen gelenkt werden können. Problematisch wird die Suche nach Herausforderung und Nervenkitzel (*Thrill Seeking*) erst in Kombination mit ausgeprägten psychopathischen oder machiavellistischen Persönlichkeitsdispositionen.

Ergebnis 2: Verglichen mit der Allgemeinbevölkerung zeigen Black Hats und White Hats signifikant höhere Ausprägungen bei allen Merkmalen der Dunklen Triade. Black Hat Hacker sind deutlich machiavellistischer und psychopathischer als White Hat Hacker. Bei isolierter Betrachtung ist Narzissmus leicht mit White Hat Hacking assoziiert.

Die Leithypothese der Arbeit war - im Sinne der Persönlichkeitspsychologie und im Kontext der kriminologischen Individualtheorien -, dass besonders Psychopathie und Machiavellismus bei Black Hat Hackern stark ausgeprägt sind und sie deutlich psychopathischer und machiavellistischer sind als die Allgemeinbevölkerung und als White Hat Hacker.

Wie in Kapitel 3 aufgeführt wurde, existieren kaum Studien, die die Dunkle Triade bei Hackern direkt untersuchen. Am relevantesten und der Fragestellung der Arbeit am nächsten kommt die Studie von Gaia und Kollegen (2021) mit dem Titel *Dark Traits and Hacking Potential*. Untersucht wurden darin jedoch nicht ‚echte‘ Black Hat Hacker in Darknet-Foren, sondern Management- und Computer Science Studenten, die einen Fragebogen zu selbstberichteter

Cyberdelinquenz ausfüllten. Die Ergebnisse von Gaia et al. (2021) zur Dunklen Triade fassen die Autoren im Abstract wie folgt zusammen:

„The results suggest that white hat, grey hat, and black hat hackers score high on the Machiavellian and psychopathy scales. We also found evidence that grey hatters oppose authority, black hatters score high in the thrill-seeking dimension, and white hatters, the good guys, tend to be narcissists.” (Gaia et al., 2021, S. 23)

Die Ergebnisse konnten an Hackern in Clear- und Darknetforen bestätigt werden. Auf der Skala der Short Dark Triad (SD3) von Jones & Paulhus (2014) zeigen Black Hat Hacker im Vergleich zur Allgemeinbevölkerung erheblich höhere Werte in Machiavellismus ($d = 1.56$) und subklinischer Psychopathie ($d = 1.28$), aber auch White Hat Hacker unterscheiden sich überraschenderweise von den Normwerten ($d = 0.68$ bei Psychopathie und $d = 0.88$ für Machiavellismus).

Beim Gruppenvergleich der Hackergruppen miteinander zeigte sich jedoch hypothesenkonform, dass Black Hats signifikant machiavellistischer ($d = 0.61$) und psychopathischer ($d = 0.71$) sind als die Gruppe der White Hats. Lediglich im Narzissmus unterscheiden sich die Gruppen kaum ($d = 0.15$). Neben den gruppenvergleichenden t -Tests für unabhängige Stichproben wurde ebenfalls eine binäre logistische Regression durchgeführt. Die Triademerkmale zeigen mittlere bis starke Korrelationen untereinander (Paulhus & Williams, 2002), das heißt, höhere Werte in Narzissmus gehen auch mit wahrscheinlich höheren Werten in Psychopathie und Machiavellismus einher. Betrachtet man Psychopathie, Machiavellismus und Narzissmus einzeln (isolierte Betrachtung durch eine binäre logistische Regression), zeigte sich, dass Psychopathie und Machiavellismus die Chance erhöhen, Black Hat Hacker zu sein. Narzissmus erhöhte aber leicht die Chance, White Hat Hacker zu sein. Wer Anerkennung sucht, scheint diese eher als White Hat zu finden als im Verborgenen. Mit dem Befund der binär-logistischen Regression konnte also auch die Vermutung von Gaia et al. (2021) „the good guys, tend to be narcissists” (S. 23) gestützt werden. Zumindest bei isolierter Betrachtung wurde Evidenz dafür gefunden, dass

Narzissmus leicht mit dem White Hat Hacking verbunden sein könnte, während Psychopathie und Machiavellismus eher mit dem Black Hat Hacking verbunden sind.

Vorherige empirische Untersuchungen (siehe aktueller Forschungsstand, Kapitel 3) konnten zeigen, dass insbesondere Psychopathie und Machiavellismus mit destruktiven Verhaltensweisen korrelieren; diese Zusammenhänge scheinen auch bei *Cyberkriminalität im engeren Sinne* (Hacking) zu gelten.

Es liegt jedoch in der Natur der statistischen Tests, dass keine Aussage über Kausalität getroffen werden kann. Es wurde angenommen, dass Black Hat Hacker machiavellistischer und psychopathischer sind und *deswegen* kriminell (Persönlichkeit = Ursache, Kriminalität = Wirkung). Dass Kriminalität ein häufiges Korrelat von Psychopathie ist, ist empirisch gut belegt, während zahlreiche Autoren Kriminalität deshalb sogar als definitorischen Bestandteil des Psychopathiekonstruktes sehen (z.B. Hare, 2005). Aber auch der umgekehrte Wirkzusammenhang ist nicht ausgeschlossen. Personen könnten höhere Machiavellismus oder Psychopathie-Scores zeigen, *weil* sie Black Hat Hacker sind und viel Zeit im Darknet und der entsprechenden Subkultur verbringen.

Während der Feldphase und mehrerer Monate in Hacker-Foren und Darknet, verbunden mit der intensiven Auseinandersetzung mit der dort anzutreffenden Ethik, blieb auch die eigene Haltung nicht unbeeinflusst und führte zeitweise zu einer temporären, aber spürbaren Verschiebung hin zu einem zynischeren Menschenbild. Dass Black Hats nach Jahren oder Jahrzehnten in bestimmten Betrugsforen machiavellistischer oder psychopathischer denken und Aussagen zustimmen wie „I am not concerned about the losers“ (Levenson et al., 1995, S. 153), ist auch nicht gänzlich ausgeschlossen.

Grundsätzlich ist aber eher davon auszugehen, dass die Persönlichkeit (Dunkle Triade) das Verhalten beeinflusst (Kriminalität) und nicht andersherum.

Neben dem klaren Bild der Black Hats ist ebenfalls der Befund bemerkenswert, dass auch White Hats (verglichen mit der Norm) auffällig in Bezug auf Machiavellismus und

Psychopathie sind. Bei Machiavellismus ist festzustellen, dass White Hat Hacker ihren ‚kriminellen Kollegen‘ näher sind als der Allgemeinbevölkerung.

Für die auffälligen Scores der White Hats könnte es zwei mögliche Erklärungen geben:

- (1) Angreifer und Verteidiger sind sich tatsächlich ähnlicher als zunächst erwartet. Cyberangriffe und Cyberabwehr erfordern sehr ähnliche Fähigkeiten: Wer weiß, wie man ein System absichert, weiß auch, wie man es angreifen könnte und umgekehrt. Dass Angreifer und Verteidiger ähnliche Fähigkeiten benötigen, ist in anderen Deliktsfeldern nicht der Fall: Einen Mord zu begehen und Mordermittlungen durchzuführen, hat wenig miteinander zu tun. Cyberangriffe und Cyberabwehr liegen hier deutlich näher beieinander und möglicherweise auch die Persönlichkeitsprofile der Angreifer und Verteidiger.
- (2) Die Grenzen zwischen Black Hats und White Hats sind weniger trennscharf als angenommen. Einige Black Hats könnten sich in bewusster Täuschungsabsicht oder tatsächlicher Eigenwahrnehmung der Gruppe der White Hats zugeordnet haben, obwohl sie von außen betrachtet klar in die Gruppe der Black Hats fallen würden. Während der Feldphase und der Rekrutierung von Probanden in Darknet-Foren wurden teilweise die dort geltenden Verhaltensregeln gelesen. Dass ein Fraud-Forum (also wörtlich ein Betrugsforum) überhaupt ethische Regeln formuliert, ist zynisch, aber auch innerhalb der Cyberkriminalität gelten bestimmte moralische Regeln. Viele Black Hats sehen sich dabei moralisch überlegen. Sie würden ‚nur Unternehmen‘ angreifen, niemals Einzelpersonen. Viele Black Hats haben ausgeprägte Rechtfertigungsstrategien und sehen sich eventuell gar nicht als kriminell (vgl. erwähnte *Robin-Hood-Mentalität*, Kapitel 5.11.1).

Auch bei White Hats ist anzunehmen, dass zumindest einige in der Jugend Erfahrungen mit moralischen Grenzüberschreitungen gemacht haben oder in der Jugend Black Hats waren. Immerhin gaben 56 % der White Hats an, ihre Fähigkeiten u.a. auch im Darknet erworben zu haben. Es bedarf jedoch weiterer Forschung, um die Eigenwahrnehmung und Identifikation

von Hackern genauer zu verstehen, da einiges darauf hindeutet, dass die Grenzen zwischen Black Hats und White Hats deutlich fließender sind, als die gängige Schwarz-Weiß-Klassifizierung vermuten lässt. Studie 3 (Validierungsstudie) sollte Aspekte der Selbstidentifikation aufgreifen.

Ergebnis 3: Black Hat Hacker sind machiavellistische, strategisch-planende ‚primäre Psychopathen‘. Sie entsprechen damit eher dem Profil der *Successful Psychopaths*.

Noch deutlicher wird das Bild der Black Hat Hacker als ‚machiavellistische Psychopathen‘ bei einer differenzierten Betrachtung der Faktoren primärer & sekundärer Psychopathie. Primäre Psychopathie ist bei Black Hats signifikant stärker ausgeprägt als sekundäre Psychopathie. Auch bei den Vergleichen mit der Allgemeinbevölkerung und White Hats wurde die besondere Rolle der Furchtlosigkeit bzw. primären Psychopathie bei Black Hats deutlich. Verglichen mit White Hats, unterschieden sich Black Hats stark in primärer Psychopathie, wobei sich bei sekundärer Psychopathie nur halb so große Unterschiede zeigten. Dasselbe Phänomen konnte auch beim Vergleich mit den Normwerten der Bevölkerung gezeigt werden. Die Unterschiede der Black Hats in primärer Psychopathie waren doppelt so groß wie die Unterschiede bei sekundärer Psychopathie. Abbildung 42 zeigt die jeweiligen Mittelwerte und Gruppenunterschiede von White Hats, Black Hats und Normwerten für die beiden Psychopathie-Subskalen der LSRP.

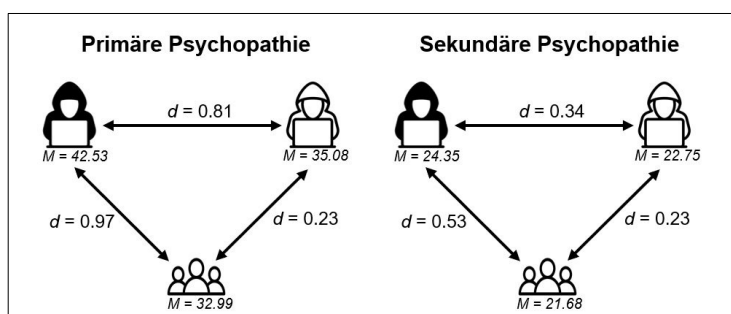


Abbildung 42. Ergebnisse der Mittelwertvergleiche durch *t*-Tests (LSRP)

Anmerkung. Quelle: Eigene Darstellung, Piktogramme: Vector Stall (Flaticon.com). Effektgrößen nach Cohen (1988), Signifikanzniveau bei allen Tests $p < .001$ (zweiseitig). Die Piktogramme symbolisieren Black Hats und White Hats (oben) sowie Referenzwerte der Allgemeinbevölkerung (unten).

Primäre Psychopathie ist vor allem gekennzeichnet durch Empathie- und Furchtlosigkeit und strategisch-planvolles Verhalten (Lykken, 1995, S. 133-155). Im Gegensatz dazu beschreibt sekundäre Psychopathie eher impulsives Verhalten, emotionale Instabilität und geringe Selbstkontrolle (Hicks & Drislane, 2019, S. 299-300; Lykken, 1995, S. 37).

Black Hat Hacker entsprechen dem Profil ‚machiavellistischer primärer Psychopathen‘ (furchtlos, planvoll-strategisch) bei gleichzeitig gemäßigter sekundärer Psychopathie und gemäßigtem Narzissmus. Das Psychopathieprofil der Black Hat Hacker in Bezug auf das Verhältnis primärer und sekundärer Psychopathie entspricht damit eher den sogenannten *Successful Psychopaths* als gewaltkriminellen Psychopathen. Interessanterweise ähnelt das psychologische Gesamtprofil der Black Hat Hacker stark dem eines idealtypischen Cyberkriminellen, dem es langfristig gelingt, sich dem Strafvollzug zu entziehen. Würde man ‚auf dem Papier‘ das ideale Täterprofil eines solchen Hackers entwerfen, sähe es vermutlich folgendermaßen aus:

Hohe Intelligenz, hohe primäre Psychopathie, ausgeprägter Machiavellismus, aber gemäßigte sekundäre Psychopathie (Impulsivität) und gemäßigter Narzissmus (Darstellungsdrang).

Sowohl sekundäre Psychopathie als auch ein stark ausgeprägter Narzissmus könnten die Entdeckungswahrscheinlichkeit deutlich erhöhen. Impulsive, emotionale oder unüberlegte Handlungen würden die eigene OpSec der Hacker gefährden. Ebenso kann die narzisstische Statuserhöhung und Suche nach Anerkennung z.B. mit teuren Uhren, Autos oder Luxusurlauben schnell zu Fragen, Neid oder steuerlichen Ermittlungen führen, insbesondere dann, wenn der zur Schau gestellte Lebensstil nicht mit den offiziell angegebenen Einkommensquellen übereinstimmt.

Gerade die Hacker, die trotz langjähriger Aktivität *nicht* entdeckt wurden und in dieser Studie untersucht werden konnten, zeigen ein auffälliges Profil: Sie kombinieren strategisches, manipulatives Denken (Machiavellismus) mit emotionaler Kälte (primäre Psychopathie).

Ergebnis 4: Es gibt einen Online Disinhibition Effect. Die enthemmende Wirkung des Cyberraums zeigt sich bei Black Hats und White Hats in ähnlicher Stärke.

Um den Online Disinhibition Effect nach Suler (2004) empirisch zu überprüfen, wurden die *Online-Skrupellosigkeit* und *Offline-Skrupellosigkeit* je Hackergruppe verglichen.

Sowohl Black Hat Hacker ($n = 321$) als auch White Hat Hacker ($n = 834$) zeigen signifikant höhere Bereitschaft zu kriminellm Verhalten im digitalen Raum als offline. Der Unterschied zwischen Online-Skrupellosigkeit und Offline-Skrupellosigkeit beträgt im Mittel rund einen Skalenpunkt auf einer 5-stufigen Likert-Skala, bei jeweils starker Effektstärke. Dies ist ein empirischer Beleg für den Online-Enthemmungseffekt, er tritt jedoch bei beiden Gruppen nahezu gleich stark auf.

Im Sinne der Kriminalätiologie erklärt der Effekt somit nicht, warum manche Hacker ihre technischen Fähigkeiten für Angriffe (Black Hats) und andere für Cybersicherheit (White Hats) einsetzen. Er wirkt eher verstärkend, nicht ursächlich. Laut Lewins Feldtheorie (1951) ist Verhalten immer eine Funktion aus Person und Situation, in diesem Fall scheint die Online-Situation (z.B. durch Anonymität) die Schwelle für skrupelloses Verhalten zu senken, besonders bei Personen, die ohnehin eine Disposition zu dunklen Persönlichkeitsmerkmalen haben. White Hats und Black Hats unterscheiden sich signifikant, aber nur schwach in der wahrgenommenen Entdeckungswahrscheinlichkeit, der Geringschätzung der Kompetenz der Polizei im digitalen Raum und in der Neigung zur Schuldumkehr.

Ergebnis 5: Black Hat Hacker lernen ihre Hackingfähigkeiten etwas öfter im Darknet als White Hats, aber auch die Mehrheit (56 %) der White Hats gibt Hacker-Foren und u.a. das Darknet als Lernquelle an. White Hat Hacker lernen ihre Fähigkeiten öfter im formellen Rahmen (z.B. Universitätsstudium).

White Hats gaben deutlich häufiger als Black Hats an, ihre Hackingfähigkeiten u.a. durch formelle Bildung erworben zu haben (41.6 % vs. 23.4 %), was teilweise durch das jüngere

Alter erklärbar ist und dadurch, dass White Hats schon weiter auf dem akademischen Weg sind als Black Hats. Noch relevanter - im Sinne der Lerntheorien - ist jedoch, dass beide Gruppen ihre Fähigkeiten u.a. im Darknet und Hacker-Foren erwarben: 69,1 % der Black Hats, aber auch 56 % (die Mehrheit) der White Hats. Es besteht zwar eine Prozentsatzdifferenz von rund 13, diese ist jedoch deutlich geringer als erwartet. Wenn Lerntheorien die monokausale Erklärung für Cybercrime wären, dann müssten alle Hacker, die ihre Fertigkeiten u.a. im Darknet lernen, zwangsläufig Black Hat Hacker werden. Dem ist jedoch nicht so: Der hohe Darknetanteil in *beiden* Gruppen spricht dafür, dass beide Hackergruppen (im jungen Alter) ihre Fähigkeiten im legalen Graubereich lernen. Ausschlaggebend bleibt die individuelle Disposition (Persönlichkeitsmerkmale), die darüber entscheidet, ob der Lebensweg im Laufe des Heranwachsens in eine legale oder illegale Hackerkarriere mündet. Immerhin lernt die Mehrheit der White Hats ihre Fähigkeiten in denselben Foren wie die Black Hats, und trotzdem entscheiden sie sich letztlich für eine legale Karriere.

Ergebnis 6: Cyberprofiling ist im Grundsatz möglich, da es bedeutsame Korrelationen gibt zwischen Persönlichkeitsmerkmalen (Dunkle Triade) einerseits und den Motiven und dem Modus Operandi andererseits.

Profiling basiert immer auf der Grundannahme, „das Verhalten von Tätern [...] als Informationsquelle zur Unterstützung der Verbrechensaufklärung zu nutzen“ (Musolff, 2002, S. 3). Nur wenn es empirisch belegbare Korrelationen zwischen Verhalten und Persönlichkeit gibt, lässt sich im Umkehrschluss aus Verhalten eine Wahrscheinlichkeitsaussage über ein Profil ableiten: „The aim of the profile ist to prove that significant correlations exist between the criminal behavior and the personality traits of the perpetrator“ (Chiesa et al., 2009, S. 8).

Aus diesem Grund wurde geprüft, ob es Korrelationen zwischen der bevorzugten Angriffsart (Technische Hacks vs. Social Engineering) und der Persönlichkeit (Dunkle Triade) gibt.

Psychopathie (besonders primäre Psychopathie) und Machiavellismus korrelieren leicht positiv mit der Vorliebe für Social Engineering. Das Ergebnis von Jones et al. (2021) kann damit nur teilweise bestätigt werden. In ihrer Studie war Machiavellismus ebenfalls mit einer Vorliebe für Täuschung und langfristiger Planung verbunden, aber Narzissmus und Psychopathie waren eher typisch für schnelle, technisch-basierte brachiale Angriffe.

Ein eindeutigeres Bild der Zusammenhänge zeigte sich bei den Merkmalen der Dunklen Triade mit den Motiven von Black Hat Hackern.

Bei Visualisierung der jeweils drei stärksten, signifikanten Korrelationen zwischen Triademerkmale und Motiven zeigt sich ein dichtes Netz der Zusammenhänge zwischen Psychopathie, Machiavellismus, Narzissmus und primärer Psychopathie mit den vier Motiven Macht, Thrill, Geld und Rache (siehe Abb. 39).

Insbesondere Psychopathie, primäre Psychopathie, Machiavellismus und Narzissmus korrelierten am stärksten mit den Motiven Macht, Thrill, Geld und Rache. Das ist mit dem inhaltlichen Kern der Konstrukte vereinbar: Personen mit hohen Ausprägungen in Psychopathie oder Machiavellismus streben typischerweise nach Dominanz, materiellen Vorteilen und intensiver Stimulation und zeigen auch häufig eine Neigung zu Rachemotiven (z.B. Giammarco & Vernon, 2014). Überraschend ist hingegen, dass Narzissmus nicht signifikant mit dem Motiv ‚Status‘ korrelierte, obwohl dieses Motiv inhaltlich zum Bedürfnis nach Bewunderung passen würde.

Sekundäre Psychopathie korrelierte ebenfalls schwach positiv mit dem Machtmotiv und als einzige Subskala schwach positiv mit dem Motiv Sucht (Feelings of Addiction) und schwach negativ mit dem Motiv Aktivismus. Dies reiht sich ein in die Befunde der Literaturanalyse von Jauk und Dieterich (2019, S. 662) zu Suchtverhalten und der Dunklen Triade; demnach zeige besonders Psychopathie Zusammenhänge mit Substanzmissbrauch, aber auch anderem Suchtverhalten, wie Glücksspiel und Computer- bzw. Internetnutzung.

Insgesamt handelt es sich zwar um schwache Korrelationen, aber einen Indikator, dass es grundsätzlich bedeutsame Zusammenhänge zwischen Motiven, Angriffsarten und Persönlichkeitsdispositionen der Hacker geben könnte, sodass Cyberprofiling grundsätzlich möglich ist.

Hier ist weitere empirische Forschung nötig, inwiefern Merkmale der Tat (Motive, Modus Operandi) etwas über Merkmale der Täter verraten können.

Ergebnis 7: Rund 42 % der Black Hats und White Hats haben bereits KI für Hacking-Aktivitäten genutzt. Aktuell bevorzugen kriminelle Hacker ChatGPT und Deepseek, aber auch eigene ‚dunkle Modelle‘ wie WormGPT werden genutzt für die Recherche und die Entwicklung von Malware und Phishing-Mails.

Wie Hacker künstliche Intelligenz nutzen, ist eine der wichtigsten Fragestellungen für die Zukunft der Cybersicherheit. Künstliche Intelligenz verändert dabei zum einen die Angriffe: „Auch viele kriminelle Akteure ergänzen bereits ihr bisheriges Repertoire durch Generative KI. Im Bereich Cybercrime sind davon vorwiegend die Phänomene Phishing und Malwareentwicklung betroffen“ (BKA, 2025a, S. 33). Zum anderen kann Generative künstliche Intelligenz langfristig nicht nur die Angriffe, sondern auch Profile der Angreifer verändern, da die intellektuelle Einstiegshürde beim Hacking sinkt (BKA, 2024, S. 24).

42 % der Black Hats und 41.5 % der White Hats haben (Stand 2025) bereits künstliche Intelligenz zum Hacking benutzt; die Unterschiede sind so minimal, dass die Seite der Angreifer hier keinen erkennbaren Innovationsvorsprung hat.

Die Daten zeigen, dass Black Hat Hacker eine bemerkenswerte Bandbreite an KI-Modellen für unterschiedliche Zwecke instrumentalisieren. Insgesamt wurden 21 verschiedene Modelle von Black Hat Hackern genannt. Der Einsatz der Generativen KI reicht von technischer Unterstützung (z.B. Erstellung von Skripten oder Exploit-Entwicklung) bis hin zu strategischer Informationsgewinnung für das *Social Engineering*. Besonders auffällig ist, dass nicht nur spezialisierte Underground-Modelle, wie WormGPT (quasi ChatGPT von Hackern für

Hacker), sondern vor allem Mainstream-KIs wie ChatGPT und Deepseek am häufigsten verwendet werden. Es zeigt, dass KI aus dem legalen und frei zugänglichen Bereich für kriminelle Zwecke zweckentfremdet wird.

Bereits im Jahr 2025 nutzten 42 % der Black Hat Hacker KI für Hacking-Aktivitäten. Es ist anzunehmen, dass dies erst der Beginn einer grundlegenden Verschiebung ist. KI wird zunehmend als Werkzeug für Cyberangriffe genutzt werden, um einzelne Phasen der Killchain¹³ zu automatisieren bis hin zu dem Szenario, dass KI-Agenten Cyberangriffe weitestgehend autonom ausführen können.

5.11.3 Methodische Reflexion

Die zentrale Leistung dieser Studie bestand darin, eine schwer zugängliche Zielgruppe außerhalb von Gefängniskontexten zu rekrutieren: Aktive Hacker aus Clearnet- und Darknet-Foren. Damit wurde ein empirischer Zugang zu einer Population ermöglicht, die bisher weitestgehend im Verborgenen agiert und in der empirischen Forschung bisher kaum direkt untersucht wurde. Die Fallzahl von $N = 1.185$ Hacker ist recht hoch für diese schwierig zu erreichende Gruppe. Da die Erhebung strikt anonym erfolgen musste, es um die Erhebung innerer Einstellungen und Motive ging und Hacker weltweit verteilt leben, war die Wahl des Formates der Online-Befragung alternativlos.

Taddicken (2013, S. 212) nennt *Stichprobenfehler* und *Messfehler* als zwei potentielle Kategorien von Verzerrungen bei Online-Befragungen. Im Rahmen der Studie wurden Hacker-Foren und Personen bestimmter Berufsbezeichnungen durch Posts und Anzeigen erreicht. Wer nicht in entsprechenden Foren Mitglied ist, konnte nicht erreicht werden. Innerhalb der Foren fand eine Selbstselektion statt. Ein zentrales Problem jeder Selbstselektion ist der Selektionsbias. Nicht alle Mitglieder der Grundgesamtheit ziehen mit gleicher Wahrscheinlichkeit eine Teilnahme in Erwägung. Personen mit starkem Mitteilungsbedürfnis oder einem gesteigerten Selbstdarstellungsdrang nehmen tendenziell

¹³ *Killchain* ist ein Begriff, der die Kette der chronologischen Ereignisse und Vorgehensweisen eines Cyberangriffs von Planung bis Nachbereitung beschreibt.

eher teil, während besonders sicherheitsbewusste Hacker mit hohen Ansprüchen an Anonymität (OpSec) sich möglicherweise bewusst gegen eine Teilnahme entscheiden. Ebenfalls hat die Mehrzahl der Teilnehmer keine Angaben zur Nationalität gemacht, da diese Angabe optional war. Die externe Validität ist daher eingeschränkt, insbesondere hinsichtlich der Frage, ob die Ergebnisse auf spezifische Hackergruppen einzelner Länder übertragbar sind.

Da keine Liste der Grundgesamtheit der Black Hat Hacker (außerhalb des Strafvollzugssystems) vorliegt, konnte nur probiert werden, durch eine breite Streuung unterschiedlicher Kanäle und Hacker-Foren ein möglichst valides Abbild der Grundgesamtheit zu erreichen.

Die zweite Fehlerkategorie der *Messfehler* betrifft zum Beispiel Verzerrungseffekte durch falsche Antworten, beispielsweise durch den Effekt der *sozialen Erwünschtheit* (Taddicken, 2013, S. 214).

Um diesem Effekt vorzubeugen, wurde das Erhebungsinstrument als ‚Persönlichkeitstest‘ gestaltet und das Motiv der Selbsterkenntnis angesprochen („Ich möchte meine Dark Traits testen“). Wenn das Teilnahmemotiv die Selbsterkenntnis ist, ergäben Falschangaben keinen Sinn.

Die Validität der erhobenen Daten lässt sich nur im Sinne eines Plausibilitätschecks mit dem bestehenden Forschungsstand beurteilen. In der Erhebung waren 91,6 % der befragten Hacker ($N = 1.185$) männlich, was sich exakt mit den bekannten Informationen zu Hackern aus anderen Meta-Analysen deckt (BKA, 2015b). White Hats sind berufstätig im Bereich Cybersicherheit und waren etwas älter und auch etwas weiter auf dem akademischen Weg, auch das ist in sich schlüssig (siehe Kapitel 5.9). Die hohen Werte bei subklinischer Psychopathie und Machiavellismus (in beiden Gruppen) zeigen, dass soziale Erwünschtheit eher kein Problem darstellte.

Zur Sicherung von Reliabilität und Konstruktvalidität wurde auf etablierte, international validierte Standardinstrumente zurückgegriffen. Die eingesetzten Skalen zur Erhebung der Dunklen Triade weisen in dieser Studie vergleichbare Cronbachs Alpha-Werte auf wie in früheren Studien, was auf eine stabile interne Konsistenz hinweist.

Jones & Paulhus (2014, S. 34) berichten für die Subskalen Alpha-Reliabilitäten von .72 bis .73 für Psychopathie (in der durchgeführten Studie lag die Reliabilität bei .73). Für Narzissmus fanden die Autoren in zwei Studien Werte von .68 bis .78 (S. 34). In der durchgeführten Studie lag die Reliabilität der Narzissmus-Subskala ebenfalls im selben Bereich (bei .65), und für Machiavellismus berichten Jones & Paulhus (2014, S. 34) Koeffizienten von .74 bis .76, wobei die Reliabilität in der hier durchgeführten Studie bei .78 lag.

Da Standardskalen verwendet wurden und ähnliche Reliabilitätswerte wie bei Studien der Allgemeinbevölkerung erzielt werden konnten, deuten die Ergebnisse darauf hin, dass es valide und reliabel gelungen ist, die Merkmale der Dunklen Triade bei Hackern zu erheben.

Deutliche Unterschiede zeigten sich zwischen White Hats und Black Hats bei den Merkmalen der Dunklen Triade: Black Hat Hacker sind signifikant psychopathischer und machiavellistischer als White Hat Hacker.

Auch wenn auf Basis der erhobenen Daten keine kausalen Aussagen möglich sind, bietet dieses Persönlichkeitsprofil wichtige Erklärungsansätze für Cyberkriminalität. Das Profil ‚machiavellistischer, primärer Psychopathen‘ bei gleichzeitig gemäßigter Impulsivität und Narzissmus könnte Teil der Erklärung sein, wie es diesen Tätern gelingt, langfristig den strafrechtlichen Konsequenzen zu entgehen.

Eine Schwäche der quantitativen Befragung besteht darin, dass Hacker nicht selbst zu Wort kommen und komplexe Realitäten auf fünfstufige Likert-Skalen reduziert werden müssen.

Die dritte Studie setzt genau hier an, indem sie dieselben Fragen offen stellt, also ohne vorgegebene Antwortoptionen in Verbindung mit einer anschließenden qualitativen Auswertung.

6 Studie 3: Qualitative Interviews mit Hackern

6.1 Zielsetzung und Gütekriterien

Das Ziel der dritten Teilstudie besteht darin, die quantitativen Daten der zweiten Studie zu validieren und zu vertiefen. Das Vorgehen entspricht dem Prinzip von *Mixed-Methods-Designs* nach Creswell & Plano Clark (2018) bzw. präziser dem „explanatory sequential design“ (Creswell & Plano Clark, 2018, S. 77), bei dem quantitative Ergebnisse im Anschluss qualitativ vertieft werden, um so ein ganzheitliches Verständnis des Forschungsgegenstands zu gewinnen. Es geht darum, durch Leitfadeninterviews mit Black Hat Hackern an die Innenperspektive zu gelangen, wie aktive Cyberkriminelle selbst ihre Motive, Persönlichkeit und moralische Perspektive beschreiben. Besonders aufschlussreich sind Zitate von aktiven, kriminellen Hackern außerhalb des Strafvollzugssystems, da sie seltene Einblicke in eine schwer zugängliche Szene in Hacker-Foren und im Darknet ermöglichen. Gerade im geschützten Rahmen wissenschaftlicher Forschung und unter strikter Wahrung ihrer Anonymität äußern sich Black Hats potentiell offener, als sie es gegenüber Strafverfolgungsbehörden oder in Gerichtsprozessen tun würden. Die Aussagen von identifizierten Hackern im Rahmen von Gerichtsverhandlungen sind in der Regel anwaltlich abgestimmt und daher nicht uneingeschränkt valide, da das Freiheitsinteresse und das Ziel der Strafmilderung überwiegen und die Antworten somit strategisch, aber nicht unbedingt wahr sind. Wenn z.B. forensische Gutachter Straftäter in Justizvollzugsanstalten interviewen, ist das keine neutrale Erhebungssituation, sondern ein Bewerbungsgespräch um die Freiheit.

Die quantitative Befragung von $N = 1.185$ Hackern lieferte signifikante Ergebnisse auf Basis etablierter Skalen mit nachgewiesener Validität und Reliabilität. Der Nachteil dieses strikt quantitativen Vorgehens ist jedoch, dass die Realität notwendigerweise auf numerische Skalenwerte reduziert werden muss. Lamnek & Krell (2016) sprechen in diesem Zusammenhang von „Messfetischismus“ (S. 25) und kritisieren, dass bei der Reduktion auf standardisierte Skalen wichtige qualitative Aspekte verloren gingen. Komplexe Persönlichkeitsmerkmale, wie primäre Psychopathie und Machiavellismus, lassen sich nicht

allein durch einen Zahlenwert vollumfänglich abbilden. Es wurde bereits quantitativ beschrieben, dass Black Hat Hacker hohe Ausprägungen auf etablierten Skalen für primäre Psychopathie und Machiavellismus zeigen. Doch was bedeutet es, strategisch-empathielos und machiavellistisch zu sein und entsprechend zu agieren? Wie beschreiben insbesondere Black Hat Hacker die Innenperspektive?

Zur Beantwortung dieser Fragen und Validierung der quantitativen Ergebnisse wurden strukturierte, problemzentrierte Leitfadeninterviews als geeignete Erfassungsmethode gewählt (Mayring, 2023, S. 61-62).

Das thematische Codieren nach Flick (2025) dient als Auswertungsmethode der qualitativen Interviewdaten. Thematisches Codieren eignet sich ideal für die vorliegende Zielsetzung, denn die Auswertungsmethode qualitativer Daten wurde „für vergleichende Studien entwickelt, die mit aus der Fragestellung abgeleiteten, vorab festgelegten Gruppen arbeiten“ (Flick, 2025, S. 402). In diesem Fall sind die vorab definierten Gruppen ‚White Hats‘ und ‚Black Hats‘ und es geht darum, sie hinsichtlich verschiedener thematischer Kategorien (Motive, Online-Enthemmung, Persönlichkeitsdispositionen, etc.) miteinander zu vergleichen. Das thematische Codieren nach Flick (2025) ist verglichen mit der Inhaltsanalyse nach Mayring weniger populär, aber dem Untersuchungsgegenstand angemessen.

Die quantitativen Ergebnisse der zweiten Studie sollen also durch offene Fragen und thematisches Codieren (Flick, 2025) validiert, ergänzt und erklärt werden, indem Hacker selbst zu Wort kommen. Creswell & Plano Clark (2018) nennen dieses Vorgehen explizit als ein Beispiel für *Mixed Method Designs*: “A researcher collects data using quantitative survey procedures and follows up with interviews of a few individuals who completed the survey to help explain the reasons behind and meaning of the quantitative survey results.” (S. 5). Die Autoren bezeichnen diese Reihenfolge des Vorgehens als „explanatory sequential design“ (Creswell & Plano Clark, 2018, S. 77). Es geht also in der qualitativen Forschung nicht darum, Hypothesen zu prüfen (z.B. Breuer, 2010, S. 40), sondern die bereits ermittelten quantitativen Ergebnisse vertiefend zu validieren. Die üblichen Gütekriterien der quantitativen Forschung

(Objektivität, Validität, Reliabilität) sind für qualitative Methoden nur bedingt anwendbar (Flick, 2010, S. 396). Mayring (2023, S. 123-124) schlägt daher für qualitative Forschung die Gütekriterien der „Verfahrensdokumentation“, „Argumentative[n] Interpretationsabsicherung“, „Regelgeleitetheit“ und „Nähe zum Gegenstand“ vor. Außerdem könne man qualitative Ergebnisse durch erneute Rücksprache mit Probanden und Methodentriangulation absichern (Mayring, 2023, S. 124-125).

Das Forschungsvorhaben sollte also insgesamt Hackern angemessen sein und alle Schritte regelbasiert durchgeführt und „intersubjektiv nachvollziehbar“ (Mayring, 2010, S. 606) dokumentiert werden. Insbesondere soll zu jedem Zeitpunkt beim thematischen Codieren explizit deutlich gemacht werden, welche Interpretation oder Generalisierung über Hacker auf Basis welcher Zitate erfolgt ist.

6.2 Interviewleitfaden

Ziel des „Explanatory Sequential Design[s]“ (Creswell & Plano Clark, 2018, S. 77) ist es, quantitative Ergebnisse zu erklären und zu validieren. Daher orientierte sich der Interviewleitfaden sehr eng an der Struktur des quantitativen Fragebogens der zweiten Studie.

Hierbei sollen die signifikanten Ergebnisse vertieft werden, auch die nicht-hypothesenkonformen Ergebnisse, z.B., dass Black Hats viel weniger narzisstisch sind als erwartet. Insgesamt umfasst der Interviewleitfaden 17 Fragen entlang von 9 übergeordneten Themenblöcken:

Block 1: Informed Consent: Einwilligung und Informationen zur Studie und Datenverarbeitung. Verständlichkeit, Kürze und Klarheit als oberstes Prinzip, damit die Informationen auch für Nicht-Muttersprachler (der englischen Sprache) verständlich sind.

Block 2: Hacker-Kategorien und Aktivitäten: Black Hat, White Hat etc. (Q1-Q2)

Block 3: Motivationale Faktoren (Q3)

Block 4: Online-Enthemmung, Schuldumkehr, Entdeckungswahrscheinlichkeit, Kompetenz der Polizei (Q4-8)

Block 5: Quelle der Fähigkeiten im Kontext von Lerntheorien (Q9-10)

Block 6: Rolle von KI im Hacking (Q11)

Block 7: Rolle von Psychologie und Social Engineering bei Cyberangriffen (Q12)

Block 8: Dunkle Triade: Psychopathie, Narzissmus, Machiavellismus (Q13-15)

Block 9: Abschluss, grobe demografische Angaben zur Person und Bitte, die Short-Dark Triad (SD3) zusätzlich auszufüllen (Q16-17)

Die Einwilligungserklärung und der Leitfaden wurden je nachdem, ob das Interview auf Deutsch oder Englisch, schriftlich oder per Videocall erfolgte, sprachlich angepasst. Bei Aufzeichnungen wurde zusätzlich die Einwilligung zur Aufzeichnung eingeholt. Der vollständige Leitfaden und die dazugehörige Einwilligungserklärung sind in Anhang 6 aufgeführt.

Die meisten Fragen wurden inhaltlich identisch aus dem SoSci-Survey-Fragebogen (Studie 2) übernommen, verändert wurde aber das Antwortformat und die Auswertungsmethode: Statt standardisierter Likert-Skalen wurden offene Antworten erfragt, z.B.:

Q4: Would you agree with the following statement? "If people have weak passwords and poor security, it's their own fault if they get hacked." Why or why not?

Während die zweite Studie Zustimmungswerte auf Likert-Skalen erfasste, mit dem Ziel, diese statistisch auszuwerten, erfasst die dritte Studie offene Antworten und die Frage nach dem *Warum*, um diese mittels der Methode des thematischen Codierens (Flick, 2025) qualitativ auszuwerten. Im Sinne der qualitativen Logik wird sich an bestehenden Kategorien orientiert, Befragte „sollen aber offen, ohne Antwortvorgaben, darauf reagieren“ (Mayring, 2023, S. 62). Ziel der problemzentrierten Leitfadeninterviews ist die Gewinnung „subjektiver Bedeutungen, vom Subjekt selbst formuliert“ (Mayring, 2023, S. 62).

Es wurden nicht alle Fragen der zweiten Studie identisch übernommen, sondern auch Erfahrungen und Kritik der Teilnehmer der zweiten Studie bei der Leitfadenkonzeption berücksichtigt.

Ein Ergebnis der zweiten Studie war, dass die Grenzen zwischen White Hats und Black Hats möglicherweise fließender sind als erwartet. Dies war auch im Freitextfeld eine Kritik einiger Hacker, dass die Schwarz-Weiß-Klassifizierung in Black Hats und White Hats unzureichend sei. Außerdem haben Black Hats umfassende Rechtfertigungsstrategien, sodass sie sich selbst möglicherweise gar nicht als ‚richtige Black Hats‘ sehen. Ob jemand Black Hat Hacker ist (im Sinne der hier verwendeten Definition: strafbares Hacking innerhalb der letzten 12 Monate) und sich selbst als Black Hat Hacker identifiziert, sind im Zweifel zwei verschiedene Fragestellungen. Daher enthält der Interviewleitfaden eine Frage zur Selbstidentifikation und eine Frage zu den tatsächlichen Hacking-Aktivitäten, um reale Handlungen und Selbstsicht unterscheiden zu können.

Im quantitativen Design wurde außerdem die Zeitperspektive nicht berücksichtigt. Es wurde nur erhoben, ob Personen *aktuell* Black Hat oder White Hat Hacker sind. Die zweite Studie hat ergeben, dass auch 56 % der White Hat Hacker angeben, ihre Fähigkeiten in Hacker-Foren und im Darknet gelernt zu haben. Dabei ist es durchaus wahrscheinlich, dass einige White Hat Hacker sich in ihrer Jugendzeit im rechtlichen Graubereich bewegten und erst später auf die ‚helle Seite‘ gewechselt sind. Die Frage nach den Hacking-Aktivitäten und Motiven wurde daher um den Zusatz „Has this changed over time?“ ergänzt. Gerade die Fälle, die von der Illegalität in die Legalität (oder andersherum) gewechselt haben, sind für Zwecke der Prävention besonders interessant.

Schwierig war die Problemstellung, inwiefern sich Psychopathie, Machiavellismus und Narzissmus durch offene Fragen qualitativ validieren lassen, da die meisten psychologischen Laien nur eine vage oder meistens falsche Vorstellung haben, was die Begriffe Psychopathie, Machiavellismus oder Narzissmus inhaltlich bedeuten. Daher stellte sich die Frage nach der Sinnhaftigkeit, Personen offen zu fragen, ob sie bei sich selbst z.B. narzisstische Persönlichkeitsanteile erkennen.

Erfahrungen und bisherige Forschung deuten darauf hin, dass die Persönlichkeitsmerkmale der Dunklen Triade aus der Innenperspektive durchaus erkannt und reflektiert werden

können. Konrath, Meier und Bushman (2014) entwickelten eine Skala, die Narzissmus mit nur einem Item erhebt: „To what extent do you agree with this statement: 'I am a narcissist.' (Note: The word 'narcissist' means egotistical, self-focused, and vain)“ (S. 3). Die so genannte *Single Item Narcissism Scale (SINS)* korreliert signifikant mit längeren Messinstrumenten, wie der NPI ($p < .001$, $r = .40$) (Konrath et al., 2014, S. 3).

Die Ergebnisse deuten darauf hin, dass zumindest Narzissten weder Leidensdruck haben noch ein Problem darin sehen, Narzissten zu sein. Bisherige Felderfahrungen und Kommunikation mit Hackern deuten darauf hin, dass sie (ähnlich wie Narzissten) ihre strategische, machiavellistische Manipulationsneigung durchaus reflektieren und nicht als Schwäche, sondern eher als Stärke oder Talent sehen. Orientiert an dem Vorgehen von Konrath et al. (2014), wurde je Konstrukt erst eine Kurzdefinition genannt in Verbindung mit der Frage, ob oder inwiefern Personen diese Eigenschaften bei sich erkennen.

Es wurde sich jedoch nicht ausschließlich auf die Selbstreflektion verlassen. In der Auswertung bzw. Codierung sollen alle Antworten (z.B. bisherige Taten, Motive und Sichtweisen auf Opfer) auf machiavellistische, narzisstische oder psychopathische Tendenzen überprüft werden.

Alle Teilnehmer wurden zusätzlich gebeten, die *Short Dark Triad (SD3)* auszufüllen (Frage 17). Mindestens ein Teilnehmer hatte bereits bei Studie 2 teilgenommen, doch durch die Anonymität war eine Zuordnung zum Datensatz nicht mehr möglich. Um dennoch eine inhaltliche Verbindung zwischen den qualitativen Antworten und Mittelwerten der Dunklen Triade herzustellen, wurden *alle* Probanden gebeten, die SD3 zu beantworten, wobei der Bitte nur rund die Hälfte der Probanden nachgekommen ist. Das Ziel bestand darin, individuelle Machiavellismus-, Psychopathie- und Narzissmus-Werte pro Fall zu berechnen und diese im Rahmen der qualitativen Analyse zu berücksichtigen.

6.3 Probandengewinnung

Creswell & Plano Clark (2018, S. 5) schlagen vor, einige Teilnehmer der quantitativen Untersuchung danach qualitativ zu befragen (also dieselben Probanden). Da die Online-Befragung (Studie 2) vollständig anonym erfolgte und keine Kontaktdaten erfasst wurden, bestand keine Möglichkeit, zu Teilnehmern der zweiten Studie Kontakt aufzunehmen, um sie erneut zu befragen.

Für die qualitative Studie wurden daher erneut Hacker über dieselben Rekrutierungswege angesprochen.

Der Fokus der Probandengewinnung lag in der schwierigen Aufgabe, Black Hat Hacker in Hacker-Foren, primär im Darknet, zu finden und bei Wahrung ihrer Anonymität zu einer Teilnahme zu überzeugen. Black Hat Hacker in Darknet-Foren oder Darknet-Chats zu überzeugen, den Kommunikationskanal zu wechseln (z.B. E-Mail oder Telegram), ist bereits eine große Herausforderung. In manchen Fällen dauerte der Kommunikationsprozess z.B. vom 19. Mai bis zum 3. August, also fast drei Monate, bis ein Interview abgeschlossen werden konnte.

Es konnten 14 Black Hat Hacker (englischsprachig) und 4 White Hat Hacker (deutschsprachig) qualitativ befragt werden. Der Fokus und das Interesse lag auf der Innenperspektive der Black Hats.

White Hat Hacker konnten im eigenen Cybersicherheits-Netzwerk und über LinkedIn rekrutiert werden.

8 Black Hat Hacker wurden über Darknet-Hackerforen rekrutiert, 2 Black Hat Hacker wurden über Clearnet-Hacker-Foren rekrutiert. Ein Auftragshacker, der seine Dienste im Darknet anbietet, konnte gewonnen werden und 3 weitere Black Hat Hacker über das Schneeballsystem, indem Black Hats nach weiteren Kontakten zu anderen Black Hats gefragt wurden. Eingeladen wurden primär Black Hats, die eine hohe Reputation in Darknet-Foren haben, in Form von renommierten, lange bestehenden Accounts (Kriterium: Relevanz).

Teilweise wurden offene Aufrufe in Darknet-Foren gestartet (siehe Abb. 43), woraufhin Personen selbst Kontakt aufgenommen haben (Selbstselektion).

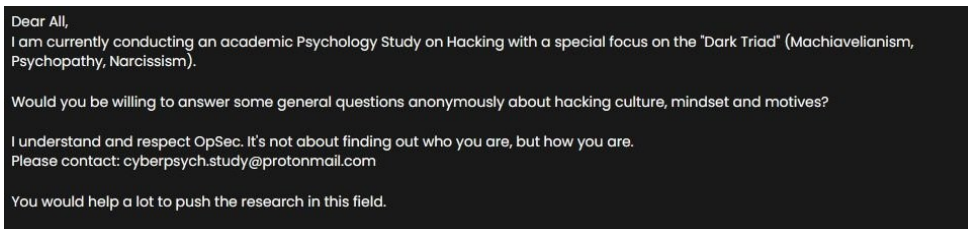


Abbildung 43. Screenshot: Probandengesuch Hacker-Forum Breachform (2025) (Darknet)

Es handelt sich also beim Samplingverfahren um eine bewusste Auswahl und teilweise Selbstselektion. Es wurden grundsätzlich dieselben Darknet- und Clearnet-Hacker-Foren wie in Studie 2 verwendet. Aufgrund der kleinen Fallzahl der qualitativen Studie werden die exakten .onion-Links und Zuordnungen, welche Einzelfälle aus welcher Quelle rekrutiert wurden, nicht publiziert, um strikte Anonymität zu gewährleisten und die zugesagte OpSec der Täter kompromisslos zu respektieren. Kommunikation fand entweder direkt im Darknet oder verschlüsselt statt, die wahre Identität der Black Hat Hacker war dem Forschenden zu keinem Zeitpunkt bekannt.

6.4 Durchführung der Interviews und Transkription

Insbesondere bei Black Hat Hackern muss sich das methodische Vorgehen daran orientieren, was in der Praxis möglich ist. Die Felderfahrungen und Ergebnisse haben gezeigt, dass Black Hat Hacker geografisch aus aller Welt kommen und extrem vorsichtig bis paranoid in Bezug auf ihre *Operational Security* (OpSec) sind. Persönliche, qualitative Leitfadeninterviews wären zwar ideal, sind aber geografisch und praktisch nicht umsetzbar, zumindest nicht mit aktiven Black Hats außerhalb des Strafvollzugsystems.

Black Hat Hacker in Darknet-Foren waren schwierig zu überzeugen, da es in diesem Fall nicht nur um eine anonyme Online-Befragung ging, sondern eine direkte Kontaktaufnahme

und Kommunikation stattfand. Dass Black Hats vorsichtig sind, wäre eine Untertreibung dessen, wie exzessiv tatsächlich auf den Schutz der Identität geachtet wird.

Die Leitfadeninterviews konnten bei Black Hat Hackern überwiegend nur schriftlich, englischsprachig durchgeführt werden (über kryptografisch PGP-verschlüsselte E-Mailkommunikation oder anonyme Apps). Black Hat Hacker kommunizierten unter Pseudonymen oder temporären ‚Wegwerf-E-Mailadressen‘, die zum Teil nur wenige Tage oder Stunden bestehen. Dem Forschenden wurden zu keinem Zeitpunkt echte Identitäten, E-Mailadressen oder Telefonnummern bekannt. Eine der Schwierigkeiten bestand darin, Black Hat Hacker aus dem Darknet ‚herauszubekommen‘, also sie zu überzeugen, die Kommunikation auf einem anderen anonymen Kommunikationskanal per Telegram oder Protonmail fortzusetzen. Bei zwei der Black Hats wurde die Befragung direkt in einem Darknetchat durchgeführt, da sie nicht bereit waren, andere Kontaktmöglichkeiten bereitzustellen. Die anderen Black Hats wurden mit entsprechender Verschlüsselung der Kommunikation per E-Mail (9 Fälle), per Telegram-App (2 Fälle) oder durch Audioanrufe in einer weiteren App für verschlüsselte Telefonie befragt (1 Fall) und anschließend wörtlich transkribiert. Aus Gründen des Datenschutzes wurde die Transkription der Audioaufnahme selbst und ohne Softwareunterstützung durchgeführt.

Die E-Mail-Kommunikation fand meist kryptografisch verschlüsselt statt (PGP-Methode). Das bedeutet, die Antworten, die Hacker tatsächlich übermittelt haben, hatten nachfolgendes Format:

-----BEGIN PGP PUBLIC KEY BLOCK-----

xjMEZ/6aPxYJKwYBBAHaRw8BAQdAeaLo1kVhtTxuKnb11UfnlwDNlsRFYnzW

5MEapzJAE5XNQWN5YmVycHN5Y2guc3R1ZHIAcHJvdG9ubWFpbC5jb20gPGN5

YmVycHN5Y2guc3R1ZHIAcHJvdGubWFpbC5jb20+wsARBBMWCgCDBYJn/po/

AwsJBwmQ1U23h7KWWcZFFAAAAAAAHAAgc2FsdEBub3Rh dGlvbnMub3BlbnBn [...]

Diese verschlüsselten Informationen wurden dann durch einen so genannten *Private Key* mit der Software *Kleopatra* auf dem lokalen Endgerät wieder entschlüsselt. Das bedeutet, selbst wenn ein Nachrichtendienst die Kommunikation abfangen würde, ist diese derartig kryptografisch verschlüsselt, dass die Daten ohne Kenntnis des privaten Schlüssels nicht zu decodieren sind.

Black Hat Hacker wurden ausführlich darüber informiert und haben eingewilligt, dass die Antworten ausgewertet und publiziert werden dürfen. Dass sie darauf bestanden, dass die Kommunikation dennoch auf einem hohen Niveau der Verschlüsselung und Anonymität erfolgt, hat damit zu tun, dass sie eine Verknüpfung zwischen ihrer Identität und den Antworten vermeiden wollen.

Per E-Mail wurde in allen Fällen der vollständige Leitfaden übermittelt, Nachfragen waren hier also nur asynchron möglich. In Chats wurden die Fragen eine nach der anderen übermittelt, sodass Nachfragen direkt möglich waren. Chats hatten dafür den Nachteil, dass dieses Kommunikationsformat durch sehr kurze Nachrichten gekennzeichnet ist. Teilnehmer haben Fragen teils mit Ja/Nein oder 1-2 Worten beantwortet und waren nur schwer zu motivieren, mehr Details oder längere Antworten zu geben. Bei Black Hats orientierte sich das methodische Vorgehen weniger daran, was im Sinne der Erkenntnis ideal wäre, sondern daran, was praktisch umsetzbar ist.

Zwei White Hat Hacker wurden ebenfalls schriftlich interviewt und zwei per Videocall (deutschsprachig), die Aufnahmen wurden im Anschluss wörtlich transkribiert.

Sowohl bei den schriftlichen Interviews als auch bei Transkripten der Audiointerviews wurden Tipp- und Rechtschreibfehler sowie individueller Ideolekt korrigiert. Insbesondere bei Black Hats war es notwendig, jegliche Rückschlüsse auf eine Identität nicht nur jetzt, sondern auch in Zukunft unmöglich zu machen: Im Bereich der forensischen Linguistik und des soziolinguistischen Profilings existiert beispielsweise das Konzept eines ‚Idiolektes‘, was die Summe individueller Sprachmuster bezeichnet, die wie ein sprachlicher Fingerabdruck für eine Person individuell sind (aktuelle Forschung z.B. Shymko, 2025). Dies kann Elemente

wie Satzlänge, Wortschatz oder falsch geschriebene Worte beinhalten. Bei der derzeitigen Entwicklungsgeschwindigkeit künstlicher Intelligenz ist antizipierbar, dass es in Zukunft durch ‚Sprachprofiling‘ möglich sein könnte, Personen anhand vollständig anonymer Texte zu identifizieren. Aus diesem Grund wurden individuelle, sprachliche Auffälligkeiten oder Slang entfernt. Ein Teilnehmer nutzte z.B. stets „Yah“ statt „Yes“ oder „cause“ statt „because“, was entsprechend redigiert wurde, ohne damit den Inhalt einer Aussage zu verändern. Auch geografische Sprachnuancen wurden redigiert. Zum Beispiel ist die übliche Schreibweise für ‚Gray Hat Hacker‘ in Großbritannien und Europa eher ‚Grey‘, während die Schreibweise in den USA ‚Gray‘ ist. Alle Antworten wurden an die US-Schreibweise („gray“) angepasst, sodass auch in Zukunft kein sprachliches Profiling in Bezug auf geografische Nuancen möglich ist.

Endergebnis der Erhebungs- und Aufbereitungsphase waren 14 Interviewtranskripte von Black Hat Hackern und 4 Interviewtranskripte von White Hat Hackern in einer einheitlichen Form mit durchgehender Zeilennummerierung. Hierin sind alle Antworten sowie die Einwilligung zur Datenverarbeitung (und Aufnahme, falls zutreffend) dokumentiert.

Die vollständigen, anonymen Interviewtranskripte wurden den Betreuern auf einem USB-Datenträger ausgehändigt, werden jedoch zum Schutz der Identität und in Übereinstimmung üblicher Vorgehensweisen beim Umgang mit Interviewdaten nicht publiziert.

Alle Kernaussagen von Black Hats und White Hats wurden jedoch im Codebogen erfasst, codiert und sind nach Themenblöcken sortiert in Anhang 8 (Codebogen Black Hats) und Anhang 9 (Codebogen White Hats) aufgeführt.

6.5 Auswertungsmethode

Das thematische Codieren nach Flick (2025) ist gut geeignet, um die beiden Hackergruppen in Bezug auf verschiedene Themenbereiche miteinander zu vergleichen. Durch die qualitative Methode des thematischen Codierens soll die Forschungsfrage beantwortet werden, „wie sich soziale Gruppen in ihren Perspektiven auf bestimmte Gegenstände oder

Prozesse unterscheiden“ (S. 408). Es geht also um „die Herausarbeitung von Gemeinsamkeiten und Unterschieden zwischen den vorab festgelegten Gruppen“ (S. 408). Diese Auswertungsmethode besteht dabei aus zwei wesentlichen Phasen: Der Einzelfallanalyse und dem fallübergreifenden Gruppenvergleich (Flick, 2025, S. 407-408).

Zu jedem Fall wurde entsprechend der Methodik nach Flick (2025) eine Kurzbeschreibung erstellt; diese „enthält eine für das Interview typische Aussage (das Motto des Falls), eine knappe Darstellung der Person im Hinblick auf die Fragestellung [...] und die zentralen Themen, die sie im Interview hinsichtlich des Untersuchungsgegenstandes angesprochen hat“ (Flick, 2025, S. 403). Die knappen Einzelfallbeschreibungen mit jeweils typischer Aussage („Motto“) sind in Kapitel 6.6.1 dargestellt. Da die Analyse explizit nicht auf ein Profiling des einzelnen Falls abzielt, sondern auf übergeordnete Gruppenvergleiche, wurde bewusst auf tiefergehende Einzelfallanalysen verzichtet.

In der zweiten Phase wurde ein fallübergreifender Gruppenvergleich je Themenkategorie durchgeführt.

Hierfür wurde zuerst das Kategoriensystem definiert (Anhang 7). Mayring (2010) unterscheidet die „induktive Kategorienentwicklung“ (S. 603), bei der die thematischen Kategorien am Material entwickelt werden, und die „deduktive Kategorienanwendung“ (S. 603), bei der die Themenblöcke „durch die vorab festgelegte Definition der Kategorien“ (S. 603) festgelegt sind. Das Kategoriensystem, bzw. die Struktur der Themen, war in diesem Fall bereits durch die Fragen und Themenblöcke des Leitfadens festgelegt. Da das Ziel der Analyse im fallübergreifenden Vergleich von Black Hats und White Hats liegt und nicht in einer Einzelfallanalyse, wurde je Hackergruppe ein Codebogen erstellt, gegliedert nach den Themenblöcken des Kategoriensystems.

Im nächsten Schritt wurde jedes einzelne Leitfadeninterview Satz für Satz durchgegangen und jeder inhaltlich bedeutsame Satz der passenden Kategorie zugeordnet und interpretiert in Form eines Codes. Codes sind dabei knappe, zusammenfassende Paraphrasierungen der zentralen Bedeutung der Aussage. Durch die direkte Aufführung der Aussagen und

Interpretationen ist intersubjektiv nachvollziehbar, welche Schlussfolgerungen auf Basis welcher Zitate gezogen wurden. Manche Aussagen wurden mehreren Kategorien zugeordnet und jeweils im Kontext des Themas interpretiert.

Tabelle 14 zeigt einen Ausschnitt des Codebogens der Black Hats in der Kategorie ‚Motive‘.

Tabelle 14: Ausschnitt Codebogen Black Hats, Kategorie ‚Motive‘

ID	Textstelle Interview	Code/ Interpretation
BH01	„But life turned into despair, and to survive I had to become something else, I had to create a persona that would help me get my life back.” (Z. 39-40)	Finanzielle Notwendigkeit als Motiv
BH01	“I don't even know where to start, it's more than 20 years of work. Yes, motivation changes over time, for the simple fact that we grow as people and our necessity changes [...]” (Z. 63-65)	Motive haben sich verändert im Zeitverlauf

Auf diesem Wege wurde das Kategoriensystem der Black Hats und White Hats mit Aussagen befüllt, die thematisch sortiert und inhaltlich interpretiert wurden.

Die strikte thematisch gegliederte Strukturierung des Materials je Hackergruppe bildete die Basis, um Black Hats und White Hats je Themenbereich vergleichen zu können. Das bedeutet, im Codebogen für die Gruppe der Black Hat Hacker und im Codebogen der Gruppe der White Hat Hacker finden sich in der Kategorie ‚Psychopathie‘ alle Aussagen, die direkt oder indirekt thematisch mit Psychopathie im Zusammenhang stehen, sowie die entsprechenden Interpretationen.

Nach der vollständigen Codierung des Materials bestand der letzte Schritt darin, je Hackergruppe und Themenkategorie Häufigkeiten auszuzählen, aus allen Codes einen kleinsten gemeinsamen Nenner oder eine übergeordnete Sinnstruktur herauszuarbeiten.

Hierbei ging es darum, übergeordnete Muster zu erkennen und Codes, die sich ähneln, zu allgemeinen Kategorien zusammenfassen. Die Ergebnisse der fallübergreifenden Gruppenvergleiche sind in Kapitel 6.6.2 dargestellt, sortiert nach Themenbereichen.

6.6 Ergebnisse

6.6.1 Einzelfallbeschreibungen

Black Hat Hacker BH01

„I'm not a thief. I'm just someone who went to hell and came back.”

Der Befragte bietet Hacking als Dienstleistung im Darknet an und bestreitet durch kriminelles Hacking seinen Lebensunterhalt. Er beschreibt sich jedoch nicht als Black Hat, sondern als ‚Survivor‘. Sein Einstieg in das Hacking begann als Teenager vor über 20 Jahren aus Neugier, entwickelte sich jedoch mit der Zeit zu einer Einkommensquelle. Er betont auch Excitement, Rebellion und Rache als wiederkehrende Motive. Grundsätzlich betont er Unterschiede zwischen dem Verhalten online und offline und sei u.a. im analogen Leben sozial engagiert. Disziplin und Vorsicht gegenüber Strafverfolgung sind für ihn zentral. Er erkennt manipulative Strategien als notwendiges Werkzeug seiner Arbeit an.

[Demografie: männlich, 30-40 SD3-Scores: /]

Black Hat Hacker BH02

„I'm open with my friends and family about everything, except my online presence.”

Der Interviewte begann mit 14 Jahren mit dem Hacken von Minecraft-Accounts (ein Computerspiel) und Datenbanken, später entwickelte er Skripte, Bots und Captcha-Bypasses. Er studierte Cybersecurity, lernte das Hacking aber vor allem durch andere Hacker in Hacker-Foren. Er sieht sich als ‚Gray Hat‘ und hält es für legitim, Unternehmen illegal zu hacken, lehnt aber Hacking aus finanziellen Motiven ab. Er betont die Bedeutung von Social Engineering. Er erkennt eine Diskrepanz zwischen seiner Offenheit und Kommunikationsfreude offline und der Verslossenheit und seinen Taten im Cyberspace. Subskalenwerte der Dunklen Triade liegen deutlich über den Normwerten der Allgemeinbevölkerung (siehe: Jones & Paulhus, 2014).

[Demografie: männlich, > 18 Jahre, SD3-Scores: PSYCH: 3.44, NARC: 3.56, MACH: 3.67]

Black Hat Hacker BH03

„My ethics are situational.”

Der Befragte begann das Hacking ebenfalls im Alter von 13 Jahren durch ‚Modding‘ und ‚Cheating‘ in Computerspielen und hat seitdem nie aufgehört, weiter zu lernen. Er beherrscht mittlerweile 7 Programmiersprachen. 90% der Fähigkeiten stammen aus dem Selbststudium und auch das Lernen von anderen Hackern auf Discord und in Darknet-Foren spielten eine Rolle. Die Hacking-Karriere begann aus Neugierde, wobei es heute um Herausforderung, Lernen und ‚Brot zu verdienen‘ geht. Er sieht sich trotz Illegalität als Gray Hat mit situationsabhängiger Ethik, wobei der Cyberraum sich für ihn abstrakt anfühlt. Anerkennung im narzisstischen Sinne spielt keine große Rolle, er ist aber in der Lage, sich emotional von seinen Angriffszielen zu entkoppeln und strategisch, manipulativ und geduldig zu agieren.

[Demografie: männlich, 20-25, USA, SD3-Scores: PSYCH: 2.33, NARC: 3.56, MACH: 3.67]

Black Hat Hacker BH04

„As a Black Hat Hacker I hack things illegally for fun, enjoyment, entertainment, training, experience, experiment and being bored and as a Gray Hat Hacker I hack stuff for good.”

Der Befragte beschreibt sich selbst als Hybrid: Einerseits hackt er illegal, u.a. aus Spaß, Langeweile und um Erfahrungen zu sammeln, andererseits sieht er sich als Gray Hat, wenn er andere Kriminelle, wie Scammer, Kinderschänder oder Menschenhändler, digital angreift und enttarnt. Seine Aktivitäten reichen von Phishing, Social Engineering und OSINT bis zu Malware-Entwicklung und Botnetzen. Motive sind vielfältig, im Zentrum stehen jedoch Herausforderung, Anerkennung von Gleichgesinnten und die Verehrung des Vorbildes Kevin Mitnick¹⁴.

¹⁴ Kevin Mitnick († 2023) war ein früherer Black Hat Hacker und späterer White Hat, bekannt durch zahlreiche Bücher und Vorträge (Kirwan & Power, 2013, S. 51).

Er ist überzeugt, dass schwache Passwörter Eigenverschulden sind, und unterscheidet klar zwischen digitalem und physischem Diebstahl. Online und offline zeigt er dasselbe Selbstbild, auch Freunde kennen ihn als Hacker. Die Polizei hält er für inkompetent. Selbststudium über das Darknet, Hacker-Foren und Kurse waren seine Lernmethoden. Er agiert kühl und strategisch, Anerkennung spielt keine Rolle.

[Demografie: männlich, >18 Jahre, SD3-Scores: /]

Black Hat Hacker BH05

- „My motivation is money and status. Just like a trophy cabinet, that shows how far I've gone in the game.”

Der Befragte sieht sich klar als Black Hat Hacker, agiert bewusst illegal und verfolgt vor allem finanzielle Motive und Statusziele. Seine Tätigkeiten umfassen vor allem Phishing und Bank-Scams, also Opfern möglichst hohe Beträge zu stehlen. Er begann seine Hackingfähigkeiten im Alter von ca. 18 Jahren in Foren zu lernen und hat sich überwiegend autodidaktisch weiterentwickelt. Online beschreibt er ein ‚Masken-Verhalten‘, das ihn enthemmt und emotionalen Abstand erzeugt, offline bleibt er verletzlich. OpSec und die regelgeleitete Einhaltung eigener Abläufe sind ihm wichtig. Er leugnet psychopathische und narzisstische Züge, aber berichtet ausgeprägte machiavellistische Strategieorientierung, die sich auch in den SD3-Scores spiegelt.

[Demografie: männlich, 30-35, Nigeria, SD3-Scores: PSYCH: 3.11, NARC: 3.0, MACH: 4.44]

Black Hat Hacker BH06

„I love the thrill, it's fun watching systems collapse and I like to see things burn. It's not always about the money.”

Der Interviewte bezeichnet sich als Black Hat, motiviert durch Nervenkitzel, Unterhaltung und gelegentlich finanziellen Gewinn. Seine Aktivitäten umfassen Account-Übernahmen, Botnet-

Kontrollen und Doxxing. Er unterscheidet klar zwischen digitaler und physischer Welt, wobei er offline keine Risiken eingeht. Hackingfähigkeiten entwickelte er autodidaktisch über Foren, Darknet-Tutorials und KI-gestützte Tools. Social Engineering ist für ihn zentral, Psychopathie, Narzissmus und Machiavellismus sind stark ausgeprägt. Er liebt das Überlegenheitsgefühl gegenüber Opfern, fühlt keine Schuld und agiert opportunistisch. Die Polizei beurteilt er als ineffektiv und er betont strategisches Vorgehen und Anpassungsfähigkeit als Schlüssel zum Erfolg.

[Demografie: männlich, 20-25, Lateinamerika, SD3-Scores: PSYCH: 3.78, NARC: 4.56, MACH: 4.00]

Black Hat Hacker BH07

„There is no one thing that motivates me, you cannot ask why a biker loves to ride. It is simple, because it is fun.”

Der Befragte nimmt Aufträge für illegales Hacking an und ist moralisch flexibel. Er ist spezialisiert auf Malware, Telefon-Hacking und RATs, greift aber auch Scammer an und sieht sich daher als Gray Hat. Motive sind Spaß, Herausforderung und die Verbesserung der eigenen Fähigkeiten. Je herausfordernder etwas ist, desto motivierter ist er. Für ihn ist Hacking intrinsisch motiviert und vergleichbar mit dem Fahren eines Motorrads, die Handlung selbst macht Freude. Damit distanziert er sich auch von Scammern; denen gehe es nicht um Spaß und Geld, sondern nur um Geld, und sie seien technisch weniger fortgeschritten. Er beschreibt sich als ganz gewöhnlich in der Realität, wobei Opfer selbst schuld seien, wenn sie schwache Passwörter nutzen. KI-Systeme hält er für Recherchezwecke für nützlich, aber noch zu fehleranfällig, um sie zur Codegenerierung oder Suche von Schwachstellen zu nutzen.

[Demografie: >18 Jahre, SD3-Scores: /]

Black Hat Hacker BH08

„I won't rob someone on the streets. Too many people watching, robbing online is fair game.“

Der Befragte ist ein Black Hat Hacker, der sich auf Cyberangriffe auf Bankkonten und Unternehmen konzentriert. Seine Motivation ist finanzieller Gewinn, Status und die intellektuelle Herausforderung, große Ziele anzugreifen. Er unterscheidet strikt zwischen Online-Operationen und realer Welt, wobei er Risiken in der analogen Welt vermeidet. Hackingfähigkeiten erlernte er autodidaktisch ab dem Alter von 14 Jahren über Darknet-Foren, Selbststudium und Lernen von erfahrenen Hackern. Erste Angriffsziele waren das WiFi der Nachbarn, die eigene Schule und Hacking und Modding in Computerspielen. Social Engineering und psychologisches Verständnis sind für ihn die zentralen Werkzeuge und machen 85% des ‚Spiels‘ aus. Er ist sehr machiavellistisch, auch Anerkennung spielt eine Rolle. OpSec wird strikt eingehalten und Polizeiarbeit als eher ineffektiv und unterlegen eingeschätzt.

[Demografie: männlich, 25-30, Europa, SD3-Scores: PSYCH: 2.78, NARC: 4.11, MACH: 4.44]

Black Hat Hacker BH09

„I started hacking in video games when I was 12, probably 13. It very quickly escalated to hacking others' online accounts [...]“

Der Befragte ist Black Hat Hacker mit Fokus auf Exploit-Entwicklung, u.a. aus finanzieller Motivation, betrachtet sich aber trotzdem als Gray Hat Hacker und sagt, er sei früher in mehr Black Hat-Aktivitäten involviert gewesen. Er begann im Alter von 12-13 Jahren ebenfalls mit dem Hacking in Videospielen und anschließendem Selbststudium. Anfängliche Motive waren Herausforderung und die eigenen Fähigkeiten zu testen. Durch den Kontakt mit anderen Hackern wandelten sich die Motive zu Anerkennung in der peer-group, Sucht und Spaß. Im Laufe des Älterwerdens, mit zunehmender Reife und auch finanziellen Verpflichtungen, wurden finanzielle Motive zum Hauptmotiv, wobei er betont, dass die anderen Motive, wie

Herausforderung, nach wie vor eine Rolle spielen. Opfer haben seiner Ansicht nach primär selbst die Verantwortung; er sieht das Hacking als „low risk, high reward“ und hält die Polizei im Cyberraum für unfähig. Er betont die Rolle menschlicher Fehler und sieht bei sich stark machiavellistische- und moderat narzisstische Tendenzen. Psychopathie sei im Zeitverlauf abgemildert, da er heute das Leid der Opfer besser verstehen könne, was früher nicht der Fall war, und er heute weniger impulsiv agiere.

[Demografie: männlich, 20-30, SD3-Scores: /]

Black Hat Hacker BH10

„Empathy is conditional for me, and I don't feel guilt. I understand emotion much more than I feel it. I analyze people the same way I analyze systems“

Der Befragte ist Black Hat Hacker und handelt sehr machiavellistisch und opportunistisch und primär aus finanziellen Motiven. Auch er begann im Alter von 11 Jahren über Computerspiele und YouTube-Tutorials mit Betrug und Carding, entwickelte sich weiter zu gezielten Ransomware-Angriffen, Social Engineering und der Datenhehlerei. Anerkennung spielt für ihn keine Rolle, im Gegenteil verachtet er Hacker, die nach Anerkennung streben. Sein Fokus liegt auf effizientem Profitstreben. Bevorzugte Ziele sind Banken und große Unternehmen, was mit einer antikapitalistischen Einstellung einhergeht. Er würde auch offline stehlen und sieht - abgesehen von einer höheren Entdeckungswahrscheinlichkeit - keinen Unterschied. Er hackt und stiehlt online nach eigenen Angaben von allem und jedem, was er kann, arbeitet aber im wirklichen Leben nebenbei in einem eher eintönigen und schlecht bezahlten Job als Tarnung.

[Demografie: männlich, 20-30, Osteuropa, SD3-Scores: /]

Black Hat Hacker BH11

„Humans are predictable if you understand their emotional triggers.“

Der Befragte beschreibt sich als Black Hat, der vor allem Datenhehlerei und Wirtschaftsspionage betreibt und sich auf Cyberangriffe gegen Unternehmen fokussiert. Motive sind dabei finanzieller Gewinn und die Herausforderung, Systeme zu hacken. Er agiert nur online risikoreich und kriminell, würde es aber in der analogen Welt nicht tun. Hackingfähigkeiten lernte er autodidaktisch, beginnend mit Beobachtung von Robotik und Systemen ab dem Alter von 16 Jahren. Social Engineering und Psychologie nutzt er gezielt für seine Angriffe. Narzissmus wird als gering eingeschätzt, das Verhalten ist jedoch sehr opportunistisch und strategisch, wobei Moral nach eigenen Angaben keine Rolle spielt.

[Demografie: männlich, 30-35, SD3-Scores: /]

Black Hat Hacker BH12

„The only inspiration for me was: If everything is unfair, then why should I be fair and suffer a lot?“

Der Befragte sieht sich als Black- und Gray Hat Hacker und ist neben dem Phishing, Social Engineering und Malware vor allem auf das Hacken von Instagram-Accounts spezialisiert. Das Hauptmotiv ist Geld bzw. finanzielle Stabilität, aber er beschreibt es auch als Sucht: Er kann nicht aufhören, sitzt Stunden an einer Stelle und vergisst die Zeit dabei, ohne zu wissen, ob es Tag oder Nacht ist. Während des Hackings stoppen alle negativen Gedanken und das ‚Overthinking‘. Der Befragte war früher sehr religiös und denkt grundsätzlich viel über Moral, Religion und Philosophie nach und ist heute zu einer sehr nihilistischen Einstellung gelangt: Wenn die ganze Welt unfair sei, warum solle er sich dann fair verhalten und leiden? YouTube und Hacker-Foren waren wichtige Lernquellen für das Hacking. Eine gewisse Gleichgültigkeit gegenüber dem Leid der Opfer und machiavellistische Tendenzen wurden sehr deutlich.

[Demografie: > 18 Jahre, SD3-Scores: PSYCH: 2.78, NARC: 3.33, MACH: 4.44]

Black Hat Hacker BH13

„To me it's just a game sometimes you win, sometimes you lose.”

Der Befragte ist ein Black Hat und ist auf Exploits und Social Engineering spezialisiert. Er begann aus Neugier, heute geht es vor allem um Herausforderung und Reputation, wobei das Geld eher Mittel zum Zweck ist, aber nicht das Hauptmotiv. Er sieht Cyberkriminalität grundsätzlich als ein Spiel und das Verhalten im Cyberraum fühle sich weniger real an, wie Theater. Er würde physisch nicht stehlen, da das reale Konsequenzen hat, aber Unternehmen oder Banken digital angreifen. Er hält die Gefahr, erwischt zu werden, für real, die Kompetenz der Polizei für länderabhängig. Der Einstieg in das Hacking erfolgte im Teenageralter über Videospiele, Modding und Neugierde. Narzissmus (Suche nach Anerkennung) und Machiavellismus (Zweck heiligt die Mittel) sind stark ausgeprägt. Psychopathie etwas gemäßigter, wobei Empathie nur offline besteht, nicht im Cyberraum.

[Demografie: männlich, 30-35, Europa, PSYCH: 3.33, NARC: 4.22, MACH: 4,22]

Black Hat Hacker BH14

„Social Engineering is like 80%, let me say 70 to 80% for any hacker. It's important, because you have to think like a victim.”

Machiavellistischer Auftragshacker und Scammer, der seine Dienste über eine eigene Seite im Darknet bereitstellt und von Mund-zu-Mund-Propaganda lebt. Zum Teil wählt er auch eigene Angriffsziele, motiviert durch Geld und Weiterentwicklung der eigenen Fähigkeiten. Interpol hat seine Seite bereits mehrfach abschalten können, was ihn motivierte, die Seite in besserer und sichererer Version wieder online zu stellen. Er startete in Jugendjahren mit White Hat Hacking-Aktivitäten und legalem Interesse an Technologie. Ein Spielfilm über eine Hackergruppe und das Darknet faszinierte ihn und war der Funke oder Auslöser, die Seiten zu wechseln. Bestätigung von außen spielt eine untergeordnete Rolle, während psychopathische und machiavellistische Aspekte durchweg deutlich hervorstehen. Als

Antwort auf die Definition zu Machiavellismus und ob er sich darin wiederfinde, antwortete der Befragte: „That’s exactly me!“.

[Demografie: männlich, 30-35, SD3: PSYCH: 3.33, NARC: 4.22, MACH: 4.22]

White Hat Hacker WH01

„In meiner Kindheit/Jugend war ich definitiv Black Hat, jetzt arbeite ich aber professionell und legal.“

Vor über 15 Jahren eine Black Hat-Vergangenheit u.a. mit Carding (Kreditkartenbetrug). Heute im IT-Bereich legal tätig und nutzt Hackingfähigkeiten auch privat legal, um Dinge zu optimieren oder zu tüfteln. Hacking versteht er dabei im Sinne der früheren, ursprünglichen Definition als technisch-kreatives Problemlösen. In Kindheit und Jugend standen Anerkennung und finanzielle Motive im Vordergrund, während es heute „eine nicht zu bändigende Faszination für technische Herausforderungen“ ist. Der Einstieg in das Hacking geschah auch hier in früher Jugend über Computerspiele und Modding. Er ist ein Befürworter digitaler Souveränität, wobei Merkmale der Dunklen Triade nicht im außergewöhnlichen Maße auffallen.

[Demografie: männlich, 30-35, Deutschland, SD3: PSYCH: 2.56, NARC: 2.22, MACH: 2.44]

White Hat Hacker WH02

„Also, ich würde mittlerweile tatsächlich eher zu White Hat tendieren. Aber ich hab schon eine graue, oder sagen wir mal, dunkle Vergangenheit.“

Hat ebenfalls vor ca. 30 Jahren im rechtlichen Graubereich begonnen. Heute im IT-Bereich im Konzern tätig mit Tätigkeiten im Bereich der Prävention, Beratung und Hilfestellungen, wobei es darum geht, IT in Prozesslandschaften abzubilden; er ist außerdem sozial engagiert. Erste Hackerfahrungen bereits mit 11-13 Jahren (C64/Amiga), geprägt durch den älteren Bruder. In den 80er/90er Jahren aktive Grauzone: Zutrittskontrollen überwunden,

BTX-Experimente etc. Er ist und war nie durch Profit motiviert, sondern durch Neugier, technische Herausforderung und den Wunsch, Schwachstellen aufzuzeigen. Später folgte ein Informatikstudium und beruflicher Wechsel in die IT-Security. Er sieht Social Engineering als zentrales Risiko. Hält mangelhafte Sicherheitsvorkehrungen aber teils für Eigenverschulden der Verantwortlichen. KI wird als Chance und Risiko zugleich eingeschätzt. Auffällige Merkmale der Dunklen Triade sind nicht erkennbar, also gering ausgeprägt.

[Demografie: männlich, 50-55, Deutschland, SD3: PSYCH: 2,44, NARC: 2,33, MACH: 2,67]

White Hat Hacker WH03

„Empathie ist nicht meine Stärke. Häufig sind Menschen selber schuld.“

Der Befragte ist SOC-Analyst/ White Hat und ist im Alter von ca. 10 Jahren ebenfalls über Videospiele und YouTube-Videos auf das Hacking gestoßen. Er hat ebenfalls als Black Hat begonnen: Hat in Kindheits- bzw. Teenagerjahren selbst Hacks und DDoS-Angriffe ausgeführt, aber früh auf die legale Seite gewechselt. Er sieht Opfer bei schlechten Schutzmaßnahmen teils als ‚selbst schuld‘ und unterscheidet moralisch zwischen Angriffen auf Unternehmen oder Einzelpersonen. Er hat nach eigenen Angaben eine Angststörung und Empathie ist nicht seine Stärke. Er agiert sehr opportunistisch und machiavellistisch in Bezug auf die eigenen Ziele und unterscheidet stark in Freund und Feind. Er betont die Rolle von KI und Social Engineering in der Branche und schätzt die Kompetenz der Strafverfolgungsbehörden als sehr gering ein.

[Demografie: männlich, 25-30, Deutschland, SD3: PSYCH: 3.22, NARC: 3.89, MACH 3.78]

White Hat Hacker WH04

„Also gemäß der Definition, die du genannt hast, wäre ich sehr schlecht in meinem Job, wenn ich nicht ein vielleicht sogar etwas höheres Maß an sozialer Kompetenz und Empathie hätte.“

Ethischer Social Engineering Pentester mit militärisch-nachrichtendienstlichem Hintergrund. Er arbeitet ausschließlich im Auftrag von Kunden, fokussiert sich auf den ‚Faktor Mensch‘ und lehnt unautorisiertes Hacking oder das Bloßstellen von Menschen strikt ab. Die Motivation ist altruistisch. Zur Zeit beim Militär war es das Motiv, dem Land zu dienen, heute geht es darum, den Kunden zu dienen im Sinne der Cybersicherheit. Er sieht den ‚Faktor Mensch‘ als bedeutsamen Teil der Sicherheitsarchitektur und künstliche Intelligenz als Multiplikator für Cyberangriffe. Überdurchschnittliche Merkmale der Dunklen Triade sind nicht erkennbar, außer gewissen machiavellistischen Gewohnheiten: Der Befragte gibt an, aus seiner Zeit beim Nachrichtendienst die Gewohnheit übernommen zu haben, stets im Hinterkopf zu haben, ob jemand eine potentiell nützliche Quelle sein könnte. Dieses Denkmuster der Beurteilung des zukünftigen Nutzens sei zum Teil auch Jahre später schwer abzulegen, auch wenn er Menschen nicht ausnutzt oder manipuliert.

[Demografie: männlich, 45-50, Deutschland, SD3: /]

6.6.2 Fallübergreifende Gruppenvergleiche

Selbstidentifikation: Black Hat, White Hat, Gray Hat

In der Literatur und Theorie verlaufen die moralischen Grenzen klar und abgrenzbar: Black Hats hacken kriminell und eigennützig, White Hats hacken autorisiert und legal im Sinne der Cybersicherheit und Gray Hats hacken unautorisiert, aber aus sozialen oder ideologischen Motiven (z.B. Kirwan & Power, 2013, S. 54). Im Interview mit 14 kriminellen Hackern und 4 White Hats wurde deutlich, dass die Realität komplexer ist.

Zum einen können Personen parallel legale IT-Security-Projekte ausführen (White Hat Aktivitäten) und auch Straftaten begehen. Neben der Gleichzeitigkeit ist auch ein Seitenwechsel möglich und sogar üblich: Drei von vier befragten White Hats waren im Kindheits- und Jugendalter Black Hats oder Gray Hats. Und selbst Personen, die eindeutig und ohne Zweifel der Kategorie der Black Hats zuzuordnen sind (z.B. indem sie Cybererpressungen begehen oder Privatpersonen die Bankkonten leeren), haben aus der

Innenperspektive erstaunliche Rechtfertigungsmechanismen entwickelt und sehen sich zum Teil eher als ‚Gray Hats‘.

Diese Diskrepanzen zwischen realen Taten und Selbstbild wurden so eindeutig, da getrennt nach der Selbstidentifikation gefragt wurde und den realen Hacking-Aktivitäten.

Bei 7 von 14 Black Hat Hackern (also der Hälfte der befragten Black Hats) wurde der Code vergeben: „Realistisches Selbstbild: Taten im Einklang mit Selbstidentifikation“. Die Befragten geben direkt und unmissverständlich zu verstehen, dass ihnen klar ist, was sie tun:

„I'm a Black Hat Hacker and I operate outside the law and I'm fully aware of it. I'm not here to help co-operations. I exploit them based on needs.“ (Interview BH05, Z. 39-40)

Hacker BH05 weist einen Machiavellismus-Score von 4.44 und einen Psychopathie-Score von 3.11 auf dem Instrument der SD3 (5-stufige Likert-Skala) auf. Darin könnte der Grund liegen, warum Moral und Empathie für den Befragten keine bedeutsamen Kategorien zu sein scheinen:

„I do phishing and bank scams. Well, I'm involved in any job that is financially motivated.“ (BH05, Z. 44-45)

Auch Hacker BH06 hat sowohl einen hohen Psychopathie-Score (3.78) als auch Machiavellismus-Score (4.00) und begeht Taten in den Bereichen Botnets, Doxxing und Account-Übernahmen, ohne den Drang, das beschönigt auszudrücken:

„I'm a Black Hat Hacker and I do it because I can.“ (BH06, Z. 39)

Im Gegensatz dazu zeigte die andere Hälfte der befragten Black Hat Hacker (7 von 14) umfassende, kreative Wege der moralischen Rechtfertigung. Einige Hacker differenzieren verschiedene Hacking-Aktivitäten, gestehen jedoch ein, dass Teile ihrer Tätigkeit nicht als Aktivismus auszulegen sind, sondern eindeutig dem Black Hat Hacking zuzuordnen sind:

„I actually consider myself as both Black Hat and Gray Hat, because as a Black Hat Hacker I hack things illegally for fun, enjoyment, entertainment, training, experience, experiment and being bored. As a Gray Hat Hacker I hack stuff for good things, such

as hacking scammers, Doxxers, Pedos, drug dealers, weapon dealers and human traffickers, later exposing them.“ (BH04, Z. 39-42)

BH01 sieht sich wiederum wertneutral als Ingenieur oder Überlebender:

„Before everything else, I'm an engineer. But life turned into despair, and to survive I had to become something else, I had to create a persona that would help me get my life back.“ (BH01, Z. 39-40)

„I don't put any label on myself, it's just me. But if I had to, then I would say that I'm a survivor.“ (BH01, Z. 40-41)

In diesem Fall sind die schwierigen Lebensumstände der Rechtfertigungsfaktor, mit dem Kriminalität zur nötigen Überlebenshandlung umgedeutet wird. Jeder Mensch muss zum Überleben einen Lebensunterhalt bestreiten, und gerade junge, intelligente IT-Talente hätten andere Möglichkeiten, ihr ‚Überleben‘ legal zu sichern.

Viele Black Hat Hacker ziehen eine deutliche moralische Grenze zwischen Angriffen gegen Unternehmen und Angriffen gegen Individuen. Auch Hacker BH02 hackt Unternehmen illegal („dumping databases by finding SQL vulnerabilities“ Z. 43-44), betrachtet sich aber selbst als Gray Hat, da Geld nicht das primäre Motiv sei. Zumindest die Hälfte der befragten Black Hat Hacker scheinen alle illegalen Hacking-Aktivitäten, die nicht durch finanziellen Gewinn motiviert sind, als ‚Aktivismus‘ bzw. Gray Hat Hacking zu betrachten:

„I'd say Gray Hat. I don't do harm for fun or profit, but I definitely don't ask for permission before poking around.“ (BH03, Z. 39-40)

Wer illegal Datenbanken von Unternehmen hackt und die Daten im Darknet veröffentlicht, ist jedoch nicht automatisch Aktivist. Auch Hacker BH09 entwickelt Exploits, betrachtet sich jedoch als Gray Hat. Hacker BH07 agiert als Auftragshacker und eindeutig illegal:

„I take tasks for helping others, it can even be hacking someone's phone or device, or finding info about someone, analyzing the requests or network packets, or even more: malware, RATs, and many things“ (BH07, Z. 50-52)

Er hat basierend darauf eine interessante Rechtfertigungsstrategie entwickelt. Er habe gute Intentionen, denn das Hacking sei zwar zum Nachteil für die Opfer, aber seinen Auftraggebern tue er ja etwas Gutes:

„[...] of course, all are illegal. I help with good intentions too, though it all depends on perspective: for law, I am evil, for them, I am their brother.” (BH07, Z. 42-46)

Mit derselben Argumentation könnte ein Auftragsmörder argumentieren, er tue ja für seine Auftraggeber etwas Gutes. Auch Auftragshacker BH07 kommt somit zu der Schlussfolgerung „I am Gray Hat.” (BH07, Z. 41). Zahlreiche Rechtfertigungsstrategien erinnern direkt an die acht Mechanismen der Rechtfertigung und Schuldexternalisierung nach Banduras (1999) *Moral Disengagement Theorie*.

Hacker BH10 beschrieb im Interview eindeutige Black Hat Aktivitäten gegen Unternehmen und auch Einzelpersonen:

„Yes, I would, and do, hack and steal from the bank accounts of individuals.” (BH10, Z. 85)

„Most of my time is spent on the acquisition and sale of private data. This is mostly done through ransomware and extortion.” (BH10, Z. 46-50)

Erpressungen und Ransomware sind das, was Wernert (2021) als „Massenphänomen im Bereich Cybercrime“ (S. 164) bezeichnet. Hacker BH10 begeht genau diese Delikte, aber auch er sieht sich im Graubereich:

„In terms of ‘Black/White/etc.’ I would consider myself to be in somewhat of a gray area, as I do not necessarily act based on morals or the law, for that matter, but rather financial gain.” (Z. 39-41)

Wenn finanziell motivierte Cyber-Erpressungen gegen Individuen und Unternehmen nicht als Black Hat Hacking zu definieren sind, stellt sich die Frage, was dann überhaupt Black Hat Hacking wäre. Während also die Hälfte der Black Hats sich selbst als Black Hats betrachtet, hat die andere Hälfte der Black Hats umfassende Rechtfertigungsstrategien entwickelt, wobei alle 8 Aspekte von Banduras (1999) *Moral Disengagement Theorie* in Aussagen von Black Hat Hackern zu erkennen waren.

Tabelle 15: Acht Prinzipien des *Moral Disengagements* nach Bandura (1999) bei Black Hat Hackern

Rechtfertigungs-Prinzip nach Bandura (1999)	Beispielhafte Zitate von Black Hat Hackern
<i>Moral Justification</i>	Cyberkriminalität wird gerechtfertigt, indem es als notwendig dargestellt wird: „Of course, there is financial interests (I find ‘financial needs’ more appropriate)” (BH01, Z. 70) „The road never been easy btw.” (BH01, Z. 68-69)
<i>Euphemistic Labeling</i>	Statt ‚Kriminalität‘ oder ‚Cyberangriff‘ nutzen viele Black Hats beschönigende Begriffe: „I definitely don’t ask for permission before poking around” (BH03, Z. 39-40) Poking around = ‚Herumstöbern‘ als verharmlosende Beschreibung für das kriminelle Eindringen in Systeme (§ 202a StGB: Ausspähen von Daten).
<i>Advantageous Comparison</i>	Vorteilhafte Vergleiche, indem betont wird, dass man selbst ja moralische Grenzen habe und andere noch viel schlimmer seien: „I rarely hack individuals, but focus mainly on companies.” (BH11, Z. 73)
<i>Displacement of Responsibility</i>	Bandura (1999) meint eigentlich die Argumentation, ‚Man habe ja nur Befehle (von anderen) befolgt‘. Hacker BH07 ist Auftragshacker und argumentiert, er tue ja seinen Kunden etwas Gutes, indem er ihre Aufträge ausführt: „[...] of course, all are illegal. I help with good intentions too, though it all depends on perspective: for law, I am evil, for them, I am their brother.” (BH07, Z. 42-46)
<i>Diffusion of Responsibility</i>	Keine Verantwortungsdiffusion im Sinne einer Gruppenaktivität, aber Argumentation, alles sei sowieso unfair, jeder nehme sich ohnehin, was er/sie will: „The only inspiration for me was: if everything is unfair, then why should I be fair and suffer a lot? No, I shouldn’t.” (BH12, Z. 137-138)
<i>Distortion of Consequences</i>	„I do believe there is a low chance of being caught. If you know what you are doing, take basic precautions, and do not allow greed or ego to cloud your OpSec, the chances of actual legal consequences are slim to none” (BH10, Z. 124-126)
<i>Dehumanization</i>	„I can detach emotionally from my targets.” (BH03, Z. 130)
<i>Attribution of Blame</i>	„If you have a bad door in a bad neighborhood, you should expect a visit.” (BH05, Z. 70)

Rechtfertigungs-Prinzip nach Bandura (1999)	Beispielhafte Zitate von Black Hat Hackern
	„If manipulation gives me benefit, then of course I will. People suffer because of the system and their fault, not because of mine.” (BH12, Z. 192-193)

Bandura (1999) beschreibt in seiner *Moral Disengagement Theorie* diese acht Mechanismen, mit denen Menschen moralische Bedenken ‚ausschalten‘ können, um unmoralisches oder illegales Verhalten vor sich selbst zu rechtfertigen und Schuld zu externalisieren. Diese umfassenden Rechtfertigungsmechanismen sind wichtig in Bezug auf die Rolle der Dunklen Triade, da sie eine mögliche Alternativerklärung darstellen. Je reflektierter Black Hat Hacker erkennen, moralisch falsch und eindeutig kriminell zu handeln, desto mehr müssen sie definitionsgemäß skrupellos oder empathielos sein. Je mehr Hacker sich selbst jedoch einreden, dass Unternehmen das ja ohnehin gar nicht spürten oder es andere Hacker gibt, die noch viel Schlimmeres tun, ist es ggf. möglich, diese Cyberstraftaten trotz intakter Empathiefähigkeit auszuführen. Rechtfertigungsstrategien und dunkle Persönlichkeitsmerkmale schließen sich jedoch nicht aus. Die quantitativen Ergebnisse zeigten bei Black Hats hohe Scores bei Psychopathie und Machiavellismus und gleichzeitig auch hohe Zustimmungswerte, dass Opfer ‚selbst schuld‘ seien ($M = 4$, 5-er Skala).

Die qualitativen Daten stützen das Zusammenspiel aus skrupellosen Persönlichkeitsmerkmalen und ausgeprägten Rechtfertigungsstrategien entlang aller acht Mechanismen nach Bandura (1999).

Einige Black Hat Hacker betonten, dass die Grenzen zwischen Black Hats und White Hats teilweise fließend seien und man Black Hat Hacker gewesen sein müsse, um ein guter White Hat Hacker sein zu können:

„[...] but to become a good hacker you must break things, in order to put them back together, to test them, to reverse engineering them and exploit them, for knowledge, for passion of doing things and trying things.” (BH01, Z. 98-101)

„In a way, no one is Black Hat or White Hat entirely.” (BH07, Z. 40)

„Many private-sector White Hats were once Black/Gray Hats.” (BH09, Z. 88)

Damit konnten die Ergebnisse der zweiten Studie validiert werden, denn auch die quantitativen Daten zeigten, dass 56 % der White Hats ihre Hackingfähigkeiten u.a. in Hacking-Foren und im Darknet erlernen. Dort lernt man - und dies lässt sich nach langer Zeit der Recherche und Probandengewinnung im Darknet sicher festhalten - eher das kriminelle Hacking, bei dem nicht um Erlaubnis gebeten wird. Black Hat Hacker BH09 formulierte es am pointiertesten:

„You have to consider, where did these professionals get the knowledge? Let me tell you: they don't teach you these things in schools LOL.” (BH09, Z. 92-93)

Diese Feststellung deckt sich mit den Interviewdaten der White Hat Hacker. Drei von vier der befragten White Hats waren in der Kindheit und Jugend Black Hats, die später die Seiten gewechselt haben:

„Gray Hat vermutlich. In meiner Kindheit/Jugend war ich definitiv Black Hat, jetzt arbeite ich aber professionell und legal.“ (WH01, Z. 36-37)

„Also, ich würde mittlerweile tatsächlich eher zu White Hat tendieren. Aber ich hab schon eine graue, oder sagen wir mal, dunkle Vergangenheit. Die ist aber schon 30 oder über 30 Jahre her. Das waren ja noch die Anfänge des Internets, wo man sich rumprobiert hat, BTX-Geschichten gemacht hat und so weiter, also so richtig Oldschool-Geschichten. Da wäre ich wahrscheinlich eher der ‚böse‘ gewesen. Aber heute ist das halt nicht mehr so.“ (WH02, Z. 33-37)

„Mit 10 ist mein Interesse gewachsen. Viel Videospiele, viel YouTube, erste Linux Server (für TeamSpeak etc.) ... wollte immer mehr wissen. 4chan. Angriffe auf Mastercard und Visa, selbst als Teen viel geddoSt. [Anmerkung: DDoS-Angriffe durchgeführt]“ (WH03, Z. 95-97)

Noch deutlicher wird im Abschnitt zur Quelle der Hackingfähigkeiten, wie ähnlich oder fast identisch die Anfänge der Hackerkarrieren verlaufen, egal ob Black Hats oder White Hats.

Drei der vier befragten White Hats haben auf der dunklen Seite begonnen und im Laufe des Heranwachsens und Nachlassens des jugendlichen Leichtsinns die Seiten gewechselt. Ein umgekehrter Wechsel von der legalen auf die illegale Seite scheint weniger verbreitet, kam jedoch ebenfalls bei einem der Befragten vor. Nur Black Hat Hacker BH14 beschrieb, dass

er sich ursprünglich für das ethische Hacking interessierte, aber ein Film über das Hacking und Darknet inspirierte ihn, diese Seite zu erkunden:

„Yes, I was into ethical hacking then and I watched the movie and I got like the rush to get, into the business, like know more about hacking and I started to write my own malware and exploits and software and mixing machines for money laundering and a lot of things.” (BH14, Z. 82-85)

Insgesamt zeigte sich, dass eine Schwarz-Weiß-Klassifizierung von Hackern nicht möglich ist aufgrund von Gleichzeitigkeit, Seitenwechseln, moralischer Subjektivität und umfassenden Rechtfertigungsstrategien, die alle acht moralischen Rechtfertigungsmechanismen nach Bandura (1999) beinhalten.

Motive von Black Hat Hackern

Bei 14 von 14 befragten Black Hat Hackern war mehr als ein Motiv erkennbar. Damit konnte validiert werden, was sowohl das BKA (2015b) als auch die zweite Studie deutlich zeigte. Ergebnis der zweiten Studie war, dass Black Hat Hacker im Durchschnitt 4-5 Motive angeben und finanzieller Gewinn nur auf dem fünften Rang der am häufigsten genannte Motive rangierte, hinter den Motiven Herausforderung, Thrill, Trolling/Spaß und Macht. Black Hat Hacker gaben eine große Spannweite unterschiedlicher Motive an, die sich teilweise im Zeitverlauf gewandelt haben:

„I did what I did for many different reasons.” (BH01, Z. 72)

Zur Liste der 10 Motivkategorien und der Frage, welche davon zuträfen, antwortete Hacker BH04:

„Can I say all of them? Because I feel like that’s all of the reasons that motivate and discipline me each time I go on this path?” (BH04, Z. 65-66)

Auch bei den Hackern, die sich selbst finanziell bereichern, zeigte sich in allen 14 Fällen, dass Geld nicht das einzige Motiv ist, manchmal nicht mal das primäre Motiv. Es traten Motivkombinationen auf, wie ‚Geld + Sucht‘, ‚Geld + Herausforderung‘ oder ‚Geld + Status‘:

„My motivation is money and status. Just like a trophy cabinet, that shows how far I've gone in the game.” (BH05, Z. 65-66)

„We wish for fun, money, and other things too.” (BH07, Z. 101-102)

„Do not get me wrong, even if it's mainly for financial interest, I always enjoy a challenge, and developing my skills and being respected by my peers is a side effect of the skills that come with that.” (BH09, Z. 65-67)

„My motivation behind my actions always has been, and always will be, money. Sure, there are other reasons which I suppose would add fuel to the fire, so to speak, but money is by far my biggest priority. I would also say that there is some degree of addiction involved in such actions, as I, along with most people I know, feel a thrill of some kind from pulling off said actions.” (BH10, Z. 66-70)

Grundsätzlich gibt es bei Geld häufig ein dahinterstehendes Motiv, da es lediglich ein Tauschmittel ist, um damit wiederum andere Dinge zu erreichen. Häufig ist auch der Weg das Ziel:

„I enjoy the process more than the output. Money is just a tool to access more.” (BH13, Z. 163)

Keiner der befragten Black Hat Hacker hat nur Geld als Motiv angegeben. Im Gegenteil lag der Fokus der Interviews, in Übereinstimmung mit den Ergebnissen der zweiten Studie, gar nicht auf finanziellem Gewinn, sondern einer beachtlichen Breite ganz unterschiedlicher Motive für das Black Hat Hacking. Das am häufigsten genannte Motiv der Black Hats der Studie 2 war Herausforderung (Challenge) mit 76,3 %. Das ließ sich auch in den qualitativen Daten erkennen:

„For me personally, I enjoy breaking into systems and researching to increase skills more. Nothing motivates me, the more challenge I see, the more I want to grow stronger and break it.” (BH07, Z. 70-72)

Hacking wird teilweise wie ein Wettkampf oder ein Puzzle betrachtet:

„I also love puzzles built by arrogant engineers.” (BH11, Z. 61)

Am explizitesten, aber auch vulgärsten, formulierte es Hacker BH01. Die Worte werden hier trotz ihrer Vulgarität wörtlich zitiert, da nicht nur der Inhalt, sondern auch die Ausdrucksweise

ein Abbild der Realität ist und qualitative Forschung u.a. den Zweck hat, diese Realitäten aus der Innenperspektive zu beschreiben:

„Maybe it's more like a statement: 'Don't fuck with me, I never give up, you can be smarter, you can have resources, but I'm persistent, you are just training, no matter what it costs me, in the end I will always find a way to win.'” (BH01, Z. 78-81)

Herausforderung weckt in Hackern eine starke Motivation, hierin unterscheiden sich Black Hats und White Hats kaum:

„Heute ist es eine nicht zu bändigende Faszination für technische Herausforderungen („Das ist nicht möglich“ ist mein Triggerwort) und anschließend das großartige Gefühl, diese Herausforderung gemeistert zu haben.“ (WH01, Z. 72-75)

Auch antiautoritäre Einstellungen, Systemkritik und antikapitalistische Einstellungen waren Teil der Motivstruktur mancher Black Hat Hacker:

„Rebellion? Yes, since forever, it's part of my nature.” (BH01, Z. 74)

„I never had respect for the system, for its people, politicians or else” (BH01, Z. 75)

„I hope my actions help spark a flame of distrust for banks, as I personally hate them.” (BH10, Z. 88-89)

„Yes, I would, and do, hack companies online for both my own financial gain as well as the financial loss of the targeted business. I typically go for bigger corporations as I despise capitalism and believe those in the 'best' positions deserve the worst. I will not bore you with the details.” (BH10, Z. 95-98)

In der zweiten Studie hatten 30,8 % der Black Hat Hacker „Feelings of Addiction“ (Suchtgefühle) als Motivkategorie ausgewählt. Zwei der 14 befragten Black Hats haben aus der Innenperspektive dieses Phänomen von Cyberkriminalität als Suchtverhalten beschrieben:

„I would also say that there is some degree of addiction involved in such actions, as I, along with most people I know, feel a thrill of some kind from pulling off said actions.” (BH10, Z. 68-70)

Hacker BH12 beschreibt trotz Sprachbarriere (kein englischsprachiger Native-Speaker) eindrucksvoll, dass er beim Hacking in einen Flowzustand kommt, der ihm erlaubt, das Gedankenkarussell und negative Emotionen währenddessen auszublenden:

„I enjoy it. It is like I can't leave it, like I am addicted to it. I pass hours and hours sitting in one place. While working, I forget all the things which make me scared, as well as it stops my overthinking, that's also a reason.” (BH12, Z. 67-70)

„It's just that I sometimes lose track of whether it's day or night while I'm working, it doesn't matter to me.” (BH12, Z. 48-49)

Während ein Flowzustand und das Vergessen der Zeit positiv erlebt werden können, beschreibt Hacker BH12 es selbst wörtlich als Sucht und stellt Hacking in einer Reihe mit Substanzsüchten:

„But seriously, I don't drink, nor use any drugs, or have any other addiction, except hacking.” (BH12, Z. 78)

Die quantitativen Daten der Online-Befragung zeigten, dass ‚Status‘ nur von rund 28 % der befragten Black Hat Hacker als Motivkategorie genannt wurde und damit auf Platz 8 von 10 der am häufigsten genannten Motive liegt. In Übereinstimmung mit dem Ergebnis, dass auch Narzissmus bei Black Hat Hackern weniger bedeutsam ist, zeigte sich auch bei der Auswertung der qualitativen Daten ein zwiespältiges Verhältnis zum Statusmotiv. Einige Black Hats betonten nicht nur, dass Status sie nicht antreibe, sondern sie das Motiv regelrecht verachten:

„One thing that I do not care for is recognition or notoriety, and I do not have a permanent online identity for such reasons. Those who do focus on achieving such things are, in my eyes, pathetic.” (BH10, Z. 70-72)

Anderen ist Status wichtiger, aber auch in diesen Fällen gilt es zu differenzieren, wem oder was gegenüber eine Statuserhöhung erreicht werden soll. Keiner der befragten kriminellen Hacker kann auf Instagram, LinkedIn oder im analogen Leben mit den eigenen Taten offen prahlen. Manchmal geht es eher um einen Status sich selbst gegenüber, im Sinne einer Steigerung des Gefühls der Selbstwirksamkeit:

„My motivation is money and status. Just like a trophy cabinet, that shows how far I've gone in the game.” (BH05, Z. 65-66)

Es geht nicht darum, diese Trophäensammlung digitaler Verbrechen anderen zu zeigen, sondern eher um Stolz auf die eigenen bisherigen beruflichen Erfolge, da aus Sicht der Täter auch eine illegale Karriere eine Karriere ist.

Bei der Befragung von Hacker BH13 wurde aktiv nachgefragt, vor wem oder was gegenüber er ‚Status‘ erreichen möchte, wenn dieser Ruhm doch nie mit einer realen Identität verknüpft werden kann. Wer soll davon beeindruckt werden?

„To those who know.” (BH13, Z. 154)

Trotz der offenen Fragen konnten fast alle Motive von Black Hat Hackern den 10 Motivkategorien zugeordnet werden, die im quantitativen Fragebogen verwendet wurden. Das zeigt, dass die 10 Motivkategorien eine recht erschöpfende Liste von Motiven darstellen. Zwei genannte Motive konnten keiner der Kategorien zugeordnet werden. Hacker BH06 gab neben finanziellem Gewinn eine reine Zerstörungswut im Sinne einer digitalen Brandstiftung als Motiv an:

„I love the thrill, it's fun watching systems collapse and I like to see things burn, it's not always about the money.” (BH06, Z. 60-61)

Bereits in der Schulzeit begann die Hacking-Karriere mit dieser Motivation:

„Found a leaked keylogger on a hacking forum, sent it to classmates and watched chaos unfold LOL.” (BH06, Z. 89-90)

Auch Hacker BH12 gab eine Motivkategorie an, die bisher und auch in der Literatur nicht vorkommt. Das Motiv lässt sich als eine Art der nihilistischen Resignation beschreiben, bei der hinterfragt wird, wieso man sich moralisch korrekt verhalten solle, wenn die ganze Welt doch ohnehin unfair und sinnlos sei:

„The only inspiration for me was: if everything is unfair, then why should I be fair and suffer a lot? No, I shouldn't. I should do what I like, what I want, no matter what happens.” (BH12, Z. 137-138)

„I don't believe in God and I am also influenced by nihilism and Charvak philosophy.” (Z. 75)

„[...] but life is not fair, nature is not fair, even in my country they are unfair” (Z. 83-84)

Zusammenfassend konnten die Ergebnisse zu Motiven der zweiten Studie validiert werden. Bei Black Hat Hackern ist von mehreren Motiven auszugehen, die gleichzeitig vorliegen, wobei die Suche nach Herausforderung eine zentrale Rolle einnimmt.

Es ist zudem anzumerken, dass Motive nicht statisch sind, sondern sich im Verlauf des Lebens ändern können:

„I don't even know where to start, it's more than 20 years of work. Yes, motivation changes over time, for the simple fact that we grow as people and our necessity changes [...]” (BH01, Z. 63-65)

„At first, it was curiosity and wanting to outsmart systems. Now it's more about the challenge, learning, and sometimes making bread.“ (BH03, Z. 62-63)

Manche Hacker sind derart intrinsisch motiviert, dass sie kein einzelnes Motiv nennen können, das sie antreibt. Hacker BH07 verglich das Hacking daher mit dem Motorradfahren:

„There is no one thing that motivates me; you cannot ask why a biker loves to ride. It is simple: because it is fun.“ (BH07, Z. 78-79)

Schuldexternalisierung

Ein wichtiges Prinzip von Banduras *Moral Disengagement Theorie* (1999) ist die “Attribution of Blame” (S. 203). Die Schuld für die Tat wird anderen gegeben, häufig den Opfern selbst. Die quantitativen Daten zeigten, dass Black Hats, aber auch White Hats, der Aussagen zustimmen, Opfer seien selbst schuld, gehackt zu werden, wenn sie schwache Passwörter nutzen.

Auch dieser Befund konnte validiert werden. Alle 14 der befragten Black Hats und 4 White Hats schreiben Opfern *mindestens* eine Teilschuld zu, wobei die Sichtweise der Black Hats deutlich zynischer und weniger differenziert ausfällt. Black Hat Hacker wählten eine Vielzahl kreativer Metaphern, um auszudrücken, dass Opfer selbst schuld seien:

„Totally agree, I think it's important to care for your digital assets, like you do for your physical assets. If you wouldn't use a weak lock for your gold, why would you for your accounts?” (BH02, Z. 72-73)

„If you have a bad door in a bad neighborhood, you should expect a visit.” (BH05, Z. 70)

„Hell yeah, because we are in a jungle, don't act like a prey.” (BH06, Z. 65)

„It's like walking into the wrong side of town, known for robberies and danger, flaunting cash and not having any form of protection, and being surprised when you get robbed.“ (BH09, Z. 74-75)

Eine besondere Zynik hat der Kommentar des Hackers BH10, der hofft, dass Opfer daraus etwas lernen, damit es Leuten wie ihm in Zukunft nicht noch mal gelingt, sie zu bestehlen:

„In a sense, I hope that people learn from their mistakes and do not allow people like myself to take advantage of them in the future. However, weak security is no different from an open door.” (BH10, Z. 76-78)

Eine Kreativität zeigte sich nicht nur bei der Wahl der zahlreichen Metaphern der Schuldumkehr, sondern auch bei der Verteilung der Teilschuld auf andere Entitäten. Neben den Opfern treffe nämlich auch die Banken, die Techkonzerne und das System eine Teilschuld:

„Blame should fall more on tech companies, that don't design secure defaults.” (BH03, Z. 67-68)

„Partially true, but the system is also to blame, because they don't enforce better security.” (BH11, Z. 65)

Auch Banken sollten keine Gelder anvertraut werden, wenn diese nicht in der Lage seien, diese zu schützen:

„Although I just mentioned that individuals are responsible for their own security, I believe that the banks hold the majority of that responsibility when they are trusted by the aforementioned individual. If they cannot reasonably secure funds, they should not be in possession of them.” (BH10, Z. 85-88)

Die Aussagen zur Schuldumkehr unterschieden sich weniger in der Zielrichtung, sondern eher in der Formulierung und Drastik der Bemerkungen. Einige Black Hats gingen noch weiter, als Opfern nur eine Teilschuld zu geben, und sagten, dass Menschen getäuscht werden wollen oder dankbar sein sollten, dass sie überhaupt noch online sind:

„[...] people want to be fools.” (BH12, Z. 88)

„The dummies on the internet should be happy that we, who keep everything running, let them online in the first place. If they don't want to put in the work of keeping themselves safe, it's on them for getting hacked.” (BH09, Z. 71-73)

Zu sagen, dass Opfer sich hätten besser schützen können, ist als außenstehender Dritter weniger drastisch, als dies als Täter zu sagen. Auch White Hats sehen Opfer in der Verantwortung, formulieren das jedoch deutlich differenzierter:

„Gleichzeitig muss ein souveräner digitaler Bürger die Eigenverantwortung mitbringen, sich sicher im Internet bewegen zu können. Eine Teilschuld ist vielleicht also gegeben, was in keinem Fall die Schuld des Täters mindert. Passend wäre hier die Analogie eines Autofahrers, der bei einem nicht selbst verursachten Auffahrunfall verletzt wird, aber nicht angeschnallt war.” (WH01, Z. 91-95)

Diese Teilverantwortung trage auch die Geschäftsführung bei Cyberangriffen:

„Wenn die Firma halt schlecht vorbereitet ist oder schlecht aufgestellt ist, darf man sich nicht wundern. Und dann ist das auch fahrlässig.“ (WH02, Z. 146-147)

White Hat WH04, mit einem militärischen Nachrichtendiensthintergrund, differenziert, ob Opfer es nicht besser wussten oder trotz besseren Wissens schwache Passwörter aus Bequemlichkeit nutzen:

„Ne, das wäre zu einfach. Also ich stimme dem so nicht zu. Ich würde das nach, wenn ich das darf, nach Bundeswehrmanier mal bewerten wollen. Ich würde jetzt unterscheiden wollen, haben wir es hier mit einem Ausbildungsmangel zu tun oder mit einem erzieherischen Mangel.“ (WH04, Z. 149-152)

Online Disinhibition Effect

Es zeigte sich quantitativ, dass der Cyberraum eine enthemmende Wirkung hat (siehe Kapitel 5.10.9) und Black Hat Hacker online skrupelloser agieren als offline ($M = 3.65$ vs. $M = 2.65$). Auch dieser Befund konnte in den Leitfadeninterviews validiert werden. Die Mehrzahl (12 von 14) der Black Hat Hacker würde zwar digital stehlen oder angreifen, aber nicht analog. Es zeigt sich also eine deutliche Diskrepanz in der Enthemmung und Kriminalitätsbereitschaft online- und offline:

„This doesn't mean I'm willing to physically steal from someone on the street, that's a very different kind of criminal.” (BH01, Z. 102-103)

Bei einigen Black Hats liegen die Skrupellosigkeit und die moralischen Überzeugungen online und offline derartig weit auseinander, dass sie in der analogen Welt (eigenen Angaben zufolge) nicht einmal fluchen oder ein Kaugummi stehlen wurden:

„No, I have never stolen anything in real life, not even candy from an aisle.” (BH02, Z. 83)

„Like I never use any bad words because I haven't felt the need to use them (Never means never). I become, how I am, in the Cyber World.” (BH12, Z. 113-114)

„Offline, I'm open with my friends and family about everything, except my online presence, I'm an open book and love socializing. But online, I stay anonymous on some aliases, while not on some other.” (BH02, Z. 88-90)

Einige Hacker reflektieren diese Diskrepanz der Moral und betrachten sich daher zum Teil wie ‚zwei Persönlichkeiten‘:

„I can't be just one person.” (BH01, Z. 110)

„Hack and steal from everyone and everything I can when I am online. I work a rather mundane and low-paying job in real life. I actively despise capitalism and attempt to ruin companies that benefit from the evils of it when I am online. I actively contribute to a capitalist society in real life. My online and offline identities are essentially polar opposites. The reason for the difference is mostly for my privacy and for some level of plausible deniability if, for some reason, my two identities are ever connected.” (BH10, Z.115-120)

In manchen Beschreibungen wurde deutlich, dass Black Hats zum Teil ein Doppelleben führen, wobei sie online ganz anders agieren als im realen Leben. Hacker BH14, dessen Hackerkarriere bereits durch einen Film inspiriert wurde, führt ein weiteres Filmzitat an, um seinem Gefühl im Cyberraum Ausdruck zu verleihen:

„I'll say one thing for sure. I'm a movie guy. If you watched Batman Last Knight, someone said something: “Nobody cares about me or who I am, until I put on the mask.”¹⁵ (BH14, Z. 163-164)

¹⁵ Das Filmzitat, auf das hier Bezug genommen wird, stammt aus dem Film Batman *The Dark Knight Rises* (2012) und stammt vom Protagonisten Bane, gespielt von Tom Hardy und lautet korrekt: „No one cared who i was, until i put on the mask“.

Das Bild einer ‚Maske‘ ist dabei eine treffende Repräsentation eines Gefühls der Anonymität und Enthemmung, das einige Black Hat Hacker in unterschiedlicher Form ausdrückten (Hervorhebung durch den Autor):

„I feel **invisible** online, plus the thrill to stay behind the keyboard.” (BH08, Z. 77)

„Online feels more **anonymous and theatrical**; offline has real, immediate consequences.” (BH13, Z. 78)

„To me **it's just a game** sometimes you win, sometimes you lose. That's the mindset I have for them.” (BH13, Z. 159-160)

„I'm emotional with physical victims, **but online, it's a mask.**” (BH05, Z. 81)

Einer der Gründe der Enthemmung liegt also in dem Gefühl, dass sich Straftaten im Digitalen weniger real anfühlen, sondern unsichtbar, wie ein Spiel, Theater oder eine Maske. In den Daten konnten zwei weitere Gründe für die Enthemmung identifiziert werden: Zum einen die Entdeckungswahrscheinlichkeit, bzw. das Kosten-Nutzen-Verhältnis aus Sicht der Täter und zum anderen die Fähigkeiten, da Diebstahl in der Realität ein ganz anderes Set an Fähigkeiten erfordert:

„I'm only skilled in digital stealing, that's why I don't interfere physically, because I'm not physically strong.” (BH04, Z. 84-85)

„I won't rob someone on the streets. Too many people watching, robbing online is fair game.“ (BH08, Z. 74)

„[...] petty theft IRL¹⁶ is high risk, low reward, when you can do it online for low risk, high reward.“ (BH09, Z. 83-84)

Somit konnte auch qualitativ validiert werden, dass ein gewisser Enthemmungseffekt im Cyberraum vorliegt. Einige Black Hat Hacker betonen profane, alltägliche oder sogar soziale Momente im realen Leben, um auszudrücken, dass sie in ihrem analogen Leben ‚gewöhnlich‘ sind:

„Also, I do charity work, so I guess that I don't lack empathy.” (BH01, Z. 150-151)

„In the real world I'm just a dude.” (BH06, Z. 77)

¹⁶ IRL = in real Life (im realen Leben)

„In real, I would just love to have a coffee.” (BH07, Z. 98)

„[...] or sometimes I volunteer IRL to help homeless people.” (BH09, Z. 143)

Ob diese Einlassungen der Realität entsprechen oder eine konstruierte, kompensierende Rechtfertigung darstellen, konnte nicht überprüft werden. Doch auch wenn dies aufgrund kognitiver Dissonanz schwer zu akzeptieren ist, dass dieselben Personen, die Konten von Menschen online leeren, teilweise auch freundlich oder sozial engagiert sein können, ist nicht ausgeschlossen. Zumindest die Cyberkriminellen, mit denen direkt kommuniziert wurde, waren im Forschungsprozess höflich, unterstützend, haben Zusagen eingehalten, viel Erfolg für die Dissertation gewünscht und gefragt, ob sie ansonsten noch irgendwie behilflich sein können. Während 12 der 14 Befragten auf die ein oder andere Art und Weise einen Enthemmungseffekt beschrieben, verdeutlichte Hacker BH10, dass für ihn außer der Entdeckungswahrscheinlichkeit emotional keinerlei Unterschied bestehe:

„Yes, I would, and at one point in my life greatly considered, stealing from people in real life, as I see that as no different from my online activity. There is an added risk of being caught and confronted, but that is all.” (BH10, Z. 91-93)

Wahrgenommene Entdeckungswahrscheinlichkeit und OpSec

Sowohl Black Hats (14 von 14) als auch White Hats (4 von 4) stimmen mit weitestgehend ähnlichen Worten darin überein, dass bei guter OpSec und Sicherheitsvorkehrungen - aber auch nur dann - die Entdeckungswahrscheinlichkeit sehr gering ist:

„If you know what you’re doing and keep your OpSec tight, the odds are low.” (BH03, Z. 88)

„Yes, because I’ve been doing this same thing for 5 years, and neither me, my friends, nor my dealers got caught, and the reason is because I stayed true to myself without breaking any of my own rules or protocols” (BH04, Z. 94-96)

„If you are good, it’s very low. Most people get caught working with idiots.” (BH06, Z. 81)

Dass Black Hat Hacker die Entdeckungswahrscheinlichkeit gering einschätzen, heißt keineswegs, dass sie leichtsinnig agieren. Im Gegenteil halten sie die Wahrscheinlichkeit nur

deshalb für so gering, *weil* sie eigene Sicherheitsregeln (Operational Security) strikt und teilweise fast in paranoider Art und Weise einhalten:

„I act as though I am already under surveillance from them as a habit.” (BH10, 135-136)

„Well, and I'll say in the hacking space, there's no guarantee you don't get caught. Your OpSec matters” (BH14, Z. 113-114)

„I do believe there is a low chance of being caught. If you know what you are doing, take basic precautions, and do not allow greed or ego to cloud your OpSec, the chances of actual legal consequences are slim to none” (BH10, Z. 124-126)

Wahrgenommene Kompetenz der Polizei im Cyberspace

Nur drei der 14 befragten Black Hat Hacker schreiben der Polizei eine hohe Kompetenz im digitalen Raum zu, die Mehrzahl schätzt die Strafverfolgungsbehörden in unterschiedlich drastischen Worten als inkompetent ein:

„The police are incompetent in cyberspace, the only ones who get caught are skids¹⁷ and dummies. The police need private-sector partnerships to even do that.” (BH09, Z. 88-89)

„I don't think they have the skill set to deal with people like me or my team.” (BH08, Z. 85)

„Truthfully, my knowledge of the police is limited. However, from what I have heard, I believe it is fair to say that they are not only incompetent but a joke. Their approach is reactive, not proactive, and they rely on third parties and private-sector actors to do the real work.” (BH10, Z. 131-133)

Drei Black Hats differenzierten das Kompetenzniveau jedoch geografisch und halten insbesondere die NSA und US-Bundesbehörden (die sogenannte *Three Letter Agencies*, FBI, CIA, etc.) für sehr kompetent:

„Yes, unless they are in the top-5 jurisdictions globally, they rely on external intelligence or on leaks.” (BH11, Z. 84-85)

They are incompetent, at the least where I live, they are.” (BH02, Z. 100)

¹⁷ „skids“ = Script Kiddies. Despektierliche Bezeichnung für unerfahrene, oft junge Neulinge der Hackerszene, ohne fortgeschrittene technische Fähigkeiten.

„That said, three-letter agencies are a different story. They are not incompetent. They are extremely patient, extremely quiet, and, unfortunately, extremely effective.” (BH10, Z. 133-135)

Hierin stimmen auch White Hats überein:

„Inkompetent finde ich ist nicht das richtige Wort. Ich glaube, sie sind einfach noch ein bisschen hinter der Zeit.“ (WH02, Z. 181)

„Ja, die normale Polizei auf jeden Fall. Es gibt spezialisierte SOKOs, die schon etwas leisten können, meistens aber nur in Verbindung mit ausländischen Kollegen.“ (WH01, Z. 134-135)

Es sei jedoch darauf hingewiesen, dass dies die *wahrgenommene* Kompetenz der Polizei repräsentiert, nicht unbedingt die tatsächliche Kompetenz, da gerade dem BKA in den vergangenen Jahren bedeutsame Schläge gegen Cyberkriminalität gelungen sind, wie auch die Abschaltung zentraler Darknet-Foren.

Quelle der Hackingfähigkeiten

Die größte Relevanz vor dem Hintergrund der Prävention von Cyberkriminalität hat die Frage des Beginns der jeweiligen Hacker-Karrieren. Was bringt Hacker dazu, Cyberstraftaten zu beginnen? Wo lernen sie ihre Fähigkeiten? In welchem Alter?

Sowohl die Black Hat Hacker als auch die White Hat Hacker berichteten fast identische Entstehungsgeschichten, in denen Videospiele und jugendliche Neugier eine zentrale Rolle einnehmen. Black Hats (14 von 14) und White Hats (3 von 4) fanden den Einstieg in das Hacking im Kindheits- oder Jugendalter meist zwischen 10-17 Jahren.

Rund die Hälfte der interviewten Black Hat Hacker (6 von 14) und auch 3 von 4 White Hat Hackern haben ihre Hackerkarriere über ‚Modding‘ oder ‚Cheats‘ innerhalb von Computerspielen begonnen. Das Bundesamt für Cybersicherheit der Schweiz (BACS) definiert Cheats als „Methoden [...], mit denen man sich unfaire Vorteile verschafft, indem man die normalen Regeln und Herausforderungen des Spiels umgeht“ (BACS, 2024) und ‚Mods‘ werden definiert als: „Abkürzung für Modifikationen, sind Programme, die dazu dienen,

dem Spiel neue Funktionen hinzuzufügen oder Aktionen zu ermöglichen, die ursprünglich nicht vorgesehen waren“ (BACS, 2024). Erste Inspiration, die zum Teil den Verlauf des restlichen Lebensweges bestimmt, ist ‚Modding‘ bzw. ‚Cheating‘ innerhalb von Computerspielen:

„As you will find, if you ask enough hackers, it is often video games, and this applies to me as well. I started hacking in video games when I was 12, probably 13. It very quickly escalated to hacking others' online accounts to continue playing in the game after they were caught. Then I began developing my own cheat software, which I used to infect other game cheaters who didn't know much about computer security.“ (BH09, Z. 104-108)

„Started with basic exploits in games, then moved into web-app vulnerabilities and OSINT. Lately more into Social Engineering, with mastery of 7 program languages.“ (BH03, Z. 44-45)

„Early teenager years. Video games, modding and curiosity.“ (BH13, Z. 89)

„Around 14 years, there used to be a popular YouTube channel on Minecraft¹⁸ hacking, which inspired me to cheat, which inspired me to crack Minecraft accounts. Website security used to be very low those days, they didn't even hash passwords! I think the power I felt made me continue for all these years.“ (BH02, Z. 104-107)

Insbesondere der letzte Satz offenbart, dass dieses Machtgefühl beim Hacking den ‚Funken‘ darstellte, diesen Weg weiter zu verfolgen. Auch Hacker BH10 fand den Einstieg als Kind im Alter von nur 11 Jahren über Computerspiele und auch hier eskalierte es von Cheating in Videospielen zu einer späteren cyberkriminellen Karriere:

„When I was around 11, I used to play a LOT of mobile games. I came across the online modded APK/IPA scene and fell in love. The whole idea of changing something to work in the way which I want, completely took me by storm and is what kick-started my entire life. From there, I began learning to code, creating my own cheats for random games, and then it turned less legal.“ (BH10, Z. 139-144)

Cheating in Computerspielen scheint eine mögliche ‚Einstiegsdroge‘ für Cyberkriminalität zu sein, wobei die Psychologie des Cheatings bereits dem Gedanken des Hackings sehr nahekommt: Durch technische Tricks wird etwas manipuliert oder verändert, um sich dadurch

¹⁸ Minecraft ist ein beliebtes Computerspiel.

Vorteile zu verschaffen. Interessanterweise berichteten die befragten White Hat Hacker einen identischen Einstieg. White Hat WH04 ist kein technischer Hacker, sondern Ex-Soldat (Nachrichtendienst), der heute Firmen in Bezug auf Social Engineering berät. Die drei anderen White Hats haben als Kinder oder Jugendliche eher als Black Hats oder im Graubereich begonnen.

Hacker WH01 fand den Einstieg über Computerspiele:

„Ich fand Videospiele super und hatte durch ‚Modding‘ den Einstieg gefunden.“
(WH01, Z. 140)

Hacker WH02 und WH03 haben im Graubereich oder als Black Hat begonnen und den Einstieg ebenfalls über Computerspiele gefunden:

„[...] und dann natürlich mit Spielen da so Cheats-Geschichten zu machen oder im Kaufhaus mal alle Computer sperren. Damals konnte man ja am Computer noch rumspielen in den Kaufhäusern und solche Geschichten. Und dadurch ist das tatsächlich entstanden, weil das natürlich mega cool war. Ja, ich war da irgendwie 11, 12, 13... und da war das natürlich total mega cool, weil du auch so ein Freak warst irgendwie, ne. Und ja, so ist es auch dann historisch gewachsen, sozusagen.“ (WH02, Z. 200-205)

„Mit 10 ist mein Interesse gewachsen. Viel Videospiele, viel YouTube, erste Linux Server (für TeamSpeak etc.)... wollte immer mehr wissen. 4chan. Angriffe auf Mastercard und Visa, selbst als Teen viel geddoSt.“ [Anmerkung: DDoS-Angriffe durchgeführt] (WH03Z. 95-97)

Computerspiele und jugendliche Neugier sind die erste Inspiration. Allerdings ist ‚Modding‘ oder ‚Cheating‘ noch kein Hacking. In der zweiten Phase lernen Hacker weitere Fähigkeiten. Alle Hacker betonten, dass hier primär Selbststudium eine Rolle spielte und übereinstimmend wurde die Bedeutung von Foren und auch YouTube-Videos hervorgehoben:

„Everything I know today is self-taught. I picked it up from old hackers in the game.“
(BH08, Z. 94)

„90% self-study. Books, forums, CTFs, exploit DBs, reverse-engineering old malware. Occasionally, I learned from older hackers on Discord and Darknet forums.“ (BH03, Z. 102-103)

„I learnt most of what I know by myself and long hours of work.“ (BH11, Z. 93)

„I started around 16. Hacking forums, coding, hardware to test. It's been more than 2 decades ago, that was the game back then. I have always studied and practiced by myself.” (BH01, Z. 126-127)

„There used to be a couple forums I frequented named Nulled & Cracked. I had high reputation profiles there, I learnt from there (Skidding), moved on, and developed my own tools and shared there.” (BH02, Z. 111-113)

„I began messing with mods and scripts when I was a teenager and taught myself to code by following YouTube tutorials and reading books (unfortunately, I cannot remember what those were). From there, I fell down a rabbit hole [...]” (BH10, Z. 148-150)

Die engen Verknüpfungen zwischen ‚Modding‘ in Computerspielen und Hacking konnten verifiziert werden. Beim Anklicken einer beliebigen Video-Anleitung zum Cheating auf der Plattform YouTube schlägt der Algorithmus ähnliche Videos vor, nach dem Prinzip: „Nutzer die sich das angesehen haben, interessieren sich auch hierfür“. Durch diese Vorschläge ist es mit wenigen Klicks möglich, von harmlosen Cheating-Inhalten auf umfangreiche Hacking-Tutorials zu stoßen, ohne aktiv danach gesucht zu haben.

Mit diesen Fähigkeiten haben sowohl Black Hats als auch White Hats dann erste unautorisierte bis kriminelle Hacks ausgeführt wie z.B. Kreditkartenbetrug, DDoS-Angriffe, Computer in Kaufhäusern zu sperren, das WLAN der Nachbarn zu hacken oder die eigene Schule:

„I was like 14, stumbled on information from the Darkweb, from forums and sites, then started testing stuff on neighbors and school networks.” (BH08, Z. 89-90)

„When I was starting out, I focused more on fraud and was active in the carding scene for a number of years. Yes, my actions have changed over time” (BH10, Z. 47-49)

Die qualitativen Ergebnisse deuten darauf hin, dass Computerspiele eine bedeutsame ‚Einstiegsdroge‘ darstellen und sowohl White Hats als auch Black Hats den Einstieg auf der dunklen Seite oder im Graubereich finden. Echtes Hacking wird eher durch Selbststudium gelernt und weniger im formellen Rahmen:

„You have to consider, where did these professionals get the knowledge? Let me tell you: they don't teach you these things in schools LOL.” (BH09, Z. 92-93)

Das ist eine wichtige Kernerkenntnis, da es die Grundforschungsfrage umdreht: Die Frage ist gar nicht, warum Personen Black Hat Hacker werden. Die meisten Hacker beginnen aus jugendlicher Neugier als Black- oder Gray Hats; die Frage ist eher, warum einige damit aufhören. Im Laufe des Heranwachsens lenken viele Hacker ihre Interessen in legale Bahnen und werden White Hat Hacker. WH01 hat einen recht niedrigen SD3-Psychopathie-Score von 2.22 und sagt:

„Ich lebe legal, um nachts ruhig schlafen zu können.“ (WH01, Z. 105-106)

Wenn jedoch Angst vor Strafe und Empathie mit Opfern keine Rolle spielen, gibt es auch keinen Grund, diesen eingeschlagenen Pfad der Illegalität zu verlassen:

„If something can be exploited, it should be. Why should I not do something that benefits me if doing so is both easy and has no consequences for myself?“ (BH10, Z. 79-81)

Auch die quantitativen Daten der zweiten Studie zeigen, dass die Mehrheit der Black Hat Hacker (69 %) und die Mehrheit der White Hat Hacker (56 %) ihre Fähigkeiten auf der ‚dunklen Seite‘ (z.B. Darknet-Foren) lernen. Es besteht zwar ein Unterschied, dieser ist aber nicht sehr groß. In beiden Hackergruppen sind es mehr als 50 % der Befragten (die Mehrheit), die angeben, u.a. im Darknet ihre Fähigkeiten zu lernen, und dort lernt man nicht primär das ethische Hacking. Es zeigte sich zudem, dass die Gruppe der Black Hats deutlich machiavellistischer ($d = 0.61$) und psychopathischer ($d = 0.71$) ist.

Validiert durch die qualitativen Interviews, deuten die Daten darauf hin, dass der Einstieg in das Hacking häufig über Computerspiele und aus jugendlicher Neugier passiert. Hacker lernen dann ihre Skills im Selbststudium im Darknet oder legalen Graubereich. White Hats lenken ihre Talente dann mit zunehmender Reife und beginnender Strafmündigkeit in legale Bahnen, während Black Hats dabeibleiben und skrupelloser werden.

Die Dunkle Triade entscheidet demnach nicht unbedingt darüber, wer Black Hat Hacker *wird*, sondern wer Black Hat Hacker *bleibt*.

Rolle von Social Engineering

Eine große Homogenität der Einstellungen zeigte sich bei den 14 befragten Black Hats auch bei der Frage nach der Rolle von Social Engineering. Es ging also um die Einschätzung der Bedeutung der Psychologie und des ‚Angriffsvektors Mensch‘ beim kriminellen Hacking. Alle Black Hats (14 von 14) hoben die Bedeutung des Social Engineerings hervor:

„Studying human behavior and mind, and actions, is how we learn how to exploit them.” (BH01, Z. 140)

„You can bypass the best firewalls, if you understand how people think. Manipulation, persuasion, timing - more effective than code in many cases.“ (BH03, Z. 112-113)

„Social Engineering is the base, especially for phishing.” (BH05, Z. 112)

„I use Social Engineering to trick people into opening the door, instead of smashing through the wall.” (BH06, Z. 102-103)

„Psychology is by far more important than code. The ability to predict and steer someone's behavior is one for which I am most grateful to have learned. I've done more with a convincing email than I've ever done with any brute force. Humans are, and always will be, the weakest link, and are so easily manipulated.” (BH10, Z. 167-170)

„Hacking is not just exploiting the device, but people themselves.” (BH07, Z. 144)

„Based on psychology, humans are predictable, if you understand their emotional triggers.” (BH11, Z. 102)

Hacker BH08 beziffert die Bedeutung von Social Engineering mit 85 %:

„Social Engineering is 85 percent of the game. You can buy zero days but you can't patch stupidity. People are weak“ (BH08, Z. 103-104)

Zudem merkte Hacker BH09 an, dass im Grunde alle Cyberangriffe auf menschliche Fehler zurückzuführen seien. Denn selbst technische Sicherheitslücken seien letztlich ein menschliches Versagen:

„Human error is all there is to hacking. If it's not due to Social Engineering, it's due to a bug in the code, a mistake made by a human.” (BH09, Z. 131-132)

Auch drei der vier White Hat Hacker betonten die bedeutsame Rolle von Social Engineering:

„Ist das Hauptthema. Kaum ein Angriff klappt ohne Social Engineering. Wer weiß Menschen zu manipulieren, bekommt alles was er will.“ (WH03, Z. 112-113)

Nur ein White Hat Hacker hatte eine gegenteilige Meinung und sieht Social Engineering als Instrument für Hacker, die keine fortgeschrittenen technischen Fähigkeiten besäßen:

„‘Social Engineering‘ wird in der Szene gerne von Narzissten hervorgehoben, die auf technischer Ebene keine Skills haben, aber gut labern können und unbedingt Anerkennung brauchen.“ (WH01, Z. 164-166)

Dem ist jedoch entgegenzuhalten, dass die Anerkennung, Status und Narzissmus gerade bei Black Hat Hackern wenig bedeutsam sind.

Rolle der KI beim Hacking

White Hats betonten die Chancen und Risiken der KI. Mit umgekehrten Vorzeichen sahen auch Black Hat Hacker Chancen und Risiken für sich. In Bezug auf KI-Modelle sind weder Black Hats noch White Hats derzeit in Euphorie oder Angst, sondern betonen Chancen und Risiken:

„Für die Bösen sind es Chancen, aber für die Guten natürlich auch [...]“ (WH02, Z. 226-227)

„AI is a double-edged sword. Great for automating tasks like recon or phishing templates. I've used it to generate fake personas and emails, but not for exploits. Yet.“ (BH03, Z. 107-108)

„AI is a game changer. You could literally spin up phishing scams and scripts, and it cuts down time.“ (BH08, Z. 98-99)

Hacker BH10 spezifiziert derzeitige Anwendungsszenarien für Cyberangriffe von perfekt geschriebenen Phishing-Mails bis hin zu Deepfake-Anrufen (z.B. Enkeltrick oder CEO-Fraud), bei denen mit KI die echte Stimme einer Person digital geklont werden kann:

„AI is genuinely changing everything. I've used it for automated phishing kits, voice cloning, fake documents, and bypassing certain filters. It is insane for Social Engineering. I've barely even scratched the surface of what's possible“ (BH10, Z. 160-162)

Manche Black Hat Hacker schränken die Bedeutung der KI ein, da KI-Modelle (noch) nicht fortgeschritten genug sind, Fehler produzieren und viele Restriktionen haben, sofern man die Modelle kriminell nutzen möchte:

„For advanced hacking, AI has no way yet. It has many restrictions and flaws; what it gives is unrealistic, not the truth [...]“ (BH07, Z. 134-137)

Hacker BH09 bedauerte, dass künstliche Intelligenz die Hackerszene kaputt mache, da plötzlich auch Anfänger Schadcode ohne Programmierkenntnisse erstellen können und somit die intellektuelle Einstiegshürde sinkt:

„It's currently shitting on the scene, all these skids come in with AI-coded malware. It's really sad to see. I have not used it much myself, but I have seen it used for fraud, bypassing KYC, and such things to sign up under fake IDs on websites like crypto exchanges and banks.“ (BH09, Z. 118-120)

Die Dunkle Triade

In Bezug auf die Triademerkmale zeigten die Daten der Studie 2 (quantitativ) ein eindeutiges Black Hat Profil: Hohe Ausprägungen für Machiavellismus und primäre Psychopathie (also skrupellos, manipulativ, kalt, strategisch), aber gleichzeitig moderatere Ausprägungen bei Narzissmus und sekundärer Psychopathie (Impulsivität). Die qualitativen Daten stützen diesen Befund. Bei 13 von 14 Black Hats waren anhand der SD3-Scores oder Antworten in den Leitfadeninterviews machiavellistische oder psychopathische Persönlichkeitsdispositionen erkennbar. Zahlreiche Aussagen von Black Hat Hackern wirken wie Lehrbuchbeispiele für primäre Psychopathie oder Machiavellismus:

„I plan and I execute with method, any risk I take is calculated.“ (BH01, Z. 158)

„I don't care if people suffer or not.“ (BH12, Z. 185)

„Yes. I can be strategic, manipulative, and patient when I need to be, especially in long-term Operations or Social Engineering.“ (BH03, Z. 138-139)

„Yes, I think long term, I act based on utility, not morality.“ (Z. 126)

Immer wieder wurde eine ausgesprochene Skrupellosigkeit deutlich, aber nicht auf eine leichtsinnig-impulsive Art, sondern strategisch und langfristig. Manche Hacker füllten

zusätzlich die SD3-Skala aus, sodass ein direkter Bezug zwischen Skalenwert und Innenperspektive möglich war. Black Hat Hacker BH03 zeigte mit 2.33 einen eher niedrigen Psychopathie-Score und gibt an, Schuld zu fühlen, diese aber ausblenden zu können:

„I can detach emotionally from my targets. But I do feel guilt and have lines I don't cross.“ (BH03, Z. 130)

Hacker BH08 hat gemäß der SD3-Subskala einen höheren Psychopathie-Score von 2.78 und gibt an, dass Schuld keine Rolle spiele, da es lediglich um eine logische Risikoabwägung gehe:

„Guilt rarely factors in my work, I weigh risk logically not emotionally.“ (BH08, Z. 123)

Bei Black Hat Hacker BH06 ist der Psychopathie-Score bereits derartig hoch, dass so etwas wie „Schuld“ gar nicht gefühlt wird:

„I don't feel bad that much.“ (BH06, Z. 119)

„I love the thrill, it's fun watching systems collapse and I like to see things burn [...]“ (BH06, Z. 60-61)

Es zeigten sich in Summe stimmige Zusammenhänge zwischen den SD3-Scores und inhaltlichen Antworten, was ein Indiz für die Validität des verwendeten Instrumentes ist. Auch in Bezug auf Machiavellismus zeigten z.B. Hacker BH06, BH12 einen sehr hohen Subskalen-Mittelwert > 4 (auf der 5-stufigen Likert-Skala), was auch in ihren Äußerungen deutlich wurde:

„Completely, I adapt, manipulate and move on. It's a game.“ (BH06, Z. 127), MACH-Score: 4.00

„If manipulation gives me benefit, then of course I will.“ (Z. 192), MACH-Score: 4.44

Auch Hacker BH13 mit einem Machiavellismus-Score von 4.22 bezeichnete sich als „strategic and pragmatic“ (Z. 126) und Hacker BH14 (NARC-Score: 4.00) antwortete auf die Definition von Machiavellismus:

„That is exactly me!“ (BH14, Z. 171)

Am eindrucksvollsten wurde das Profil eines Machiavellisten mit hoher primärer Psychopathie anhand des Hackers BH10 deutlich. Die Leitfrage dieser Arbeit zielt darauf ab,

herauszufinden, warum Black Hat Hacker kriminell handeln. Doch der Befragte BH10 drehte die Logik der Frage herum: Warum sollte er nicht kriminell sein?

„If something can be exploited, it should be. Why should I not do something that benefits me if doing so is both easy and has no consequences for myself?“ (BH10, Z. 79-81)

Tatsächlich sind die meisten Gegenargumente, warum man *nicht* kriminell agieren sollte, emotionaler Natur: Empathie, Moral, Gewissen und Angst vor Strafe. Wenn all diese Aspekte jedoch im Persönlichkeitsprofil absolut keine Rolle spielen, gibt es aus der Innenperspektive auch keinen Grund, es nicht zu tun. Die Konsequenz im Verhalten ist die Nutzenmaximierung durch Cyberkriminalität ohne Rücksicht auf Opfer:

„I Hack and steal from everyone and everything I can when I am online.“ (BH10, Z. 115)

Hacker BH10 gab dabei eine umfassende Beschreibung der eigenen Gefühlslage beim Hacking:

„I do feel some varying levels of guilt (not actual guilt, but the closest thing to it), depending on who I steal from. Individuals could potentially be in a tough financial spot and could suffer greatly from my actions, and for that, I do genuinely apologize, but I do not care enough to refrain from stealing from them. Companies do not deserve that same mindset. Quite frankly, there is nothing I would not do that results in a loss of any kind for any company, especially a larger corporation.“ (BH10, Z. 107-112)

Bereits die Beschreibung des Schuldgefühls als „nicht echte Schuld, aber das, was ihr am nächsten kommt“ macht deutlich, dass es sich hierbei eher um kognitive Empathie handelt, also ein Verständnis der Folgen für die Opfer, statt eines echten Mitgefühls:

„Empathy is conditional for me, and I don't feel guilt. I understand emotion much more than I feel it. I analyze people the same way I analyze systems by ways of vulnerabilities, triggers, behavioral loops, etc. I don't necessarily seek chaos, but if it's profitable, I wouldn't flinch either. Emotionally, I am cold. This is not a trait I hide or am ashamed of.“ (BH10, Z. 189-193)

Auch die Formulierung, er verstehe Emotionen eher, als sie zu fühlen, deutet auf kognitive anstelle affektiver Empathie hin (zur Unterscheidung der Formen der Empathie siehe z.B.:

Kerem, Fishman & Josselson, 2001). Diese Kälte und Empathielosigkeit wird aus der Innenperspektive auch keineswegs als Problem oder Schwäche betrachtet, wie der letzte Satz unmissverständlich deutlich macht („This is not a trait I hide or am ashamed of“).

Es wurde vermutet, dass dieses Profil hoher primärer Psychopathie (furchtlos, kalt, strategisch) bei reduzierter sekundärer Psychopathie (Impulsivität) auch der Grund sein könnte, warum es Tätern gelingt, langfristig dem Strafvollzug zu entgehen. Auch die befragten Black Hats reflektierten, dass Impulsivität eine ‚OpSec-Gefahr‘ sein kann:

„Absolutely. Everything I do is calculated, and for me, I see people as tools and not constants. I don't act out of impulse unless impulse serves the plan, as doing so is OpSec suicide. I'm sure you may have also picked up on certain Machiavellian traits throughout my answers.“ (BH10, Z. 201-203)

„I have also started acting less impulsively and am more calculating now (a big reason why I believe I won't be caught).“ (BH09, Z. 151-153)

Black Hats betrachten Impulsivität als ein Sicherheitsrisiko. Die Tatsache, dass sekundäre Psychopathie bei Black Hats (in Summe) weniger stark ausgeprägt ist als primäre Psychopathie, macht es zu einem effektiven Profil, um dem Strafvollzug zu entgehen.

Doch nicht nur Impulsivität kann die Entdeckungswahrscheinlichkeit erhöhen, sondern auch Narzissmus, sofern dieser mit einem starken Geltungsdrang, Wunsch nach Anerkennung oder Selbstdarstellung in sozialen Medien einher geht.

Studie 2 hat gezeigt, dass Black Hat Hacker moderat narzisstischer sind als die Allgemeinbevölkerung ($d = 0.37$). Zum Vergleich lag der Unterschied im Machiavellismus bei $d = 1.56$.

Nur einer von 14 befragten Black Hats zeigte einen auffällig hohen Narzissmus-Score von 4.56 und sagte:

„Yes, I love feeling superior to the people I exploit.“ (BH06, Z.112)

Bei den anderen befragten Black Hats zeigte sich in Aussagen und SD3-Scores ein eher moderater oder geringer Narzissmus:

„No, I don't recognize myself in any of those traits. I do what I do in silence, nobody knows who I am. I avoid point of failures. I need no admiration, no recognition.” (BH01, Z. 149-151)

„I like recognition, and I've definitely felt “smarter than the system” before. But I'm not attention-obsessed.” (BH03, Z. 122-123)

„I don't crave admiration, but I do believe I'm better than most people. Not because I need validation, but because I know how the majority of people think. There's a certain detachment that comes from seeing through the illusions of society.” (BH10, Z. 179-181)

Black Hat BH10 berichtete, dass er nicht nach Bewunderung strebe und Personen regelrecht verachte (erbärmlich finde), die selbiges tun:

„One thing that I do not care for is recognition or notoriety, and I do not have a permanent online identity for such reasons. Those who do focus on achieving such things are, in my eyes, pathetic.” (BH10, Z. 70-72)

Außerdem reflektierten Black Hats auch hier, dass ein zu hoher Narzissmus und übersteigertes Ego zu einer ‚OpSec-Gefahr‘ werden kann:

„I do believe there is a low chance of being caught. If you know what you are doing, take basic precautions, and do not allow greed or ego to cloud your OpSec, the chances of actual legal consequences are slim to none. 90% of the people who get caught are too loud or too trusting.” (BH10, Z. 124-127)

Die qualitativen Daten validieren und vertiefen das in Studie 2 identifizierte Hackerprofil von Black Hat Hackern in Hacker-Foren (außerhalb des Strafvollzugs):

- Machiavellismus: Hoch
- Primäre Psychopathie: Hoch
- Sekundäre Psychopathie: Moderat
- Narzissmus: Moderat

Dieses Profil könnte der Grund sein, warum die Hacker kühl-strategisch Cyberkriminalität begehen, und auch der Grund, warum es ihnen gelingt, Fehler zu vermeiden und dem Strafvollzug zu entgehen. Hacker selbst betonen, dass Narzissmus (ego) und sekundäre Psychopathie (impulsivity) eine OpSec-Gefahr darstellen.

Ein weiteres Ergebnis der zweiten Studie war, dass White Hats zwar weniger psychopathisch und machiavellistisch als Black Hats sind, aber verglichen mit der Allgemeinbevölkerung ebenfalls auffällig sind. Das kann aufgrund der kleinen Fallzahl von nur 4 White Hats nur teilweise qualitativ gestützt werden. Drei der befragten White Hats zeigten keinerlei Triademerkmale, sondern im Gegenteil hochempathisches, altruistisches Verhalten. Ex-Militär-Nachrichtendienstler WH04 gibt Altruismus (zu dienen) als Hauptmotiv an:

„Ich habe mich bewusst für den Weg Behörde, Militär, in meinem ersten Arbeitsleben entschieden, um zu dienen und ich wechsele jetzt einfach nur den Bedarfsträger. Und ich diene, mit dem was ich tue, habe ich die Möglichkeit, die deutsche Wirtschaft sicherer zu machen und vor allem unsere deutsche KRITIS sicherer zu machen und das ist tatsächlich mein primärer Antrieb. (WH04, Z. 118-122)

„Und denke aber, dass ich manchmal eher zu viel Empathie habe und zu viel soziale Kompetenz habe.“ (WH04, Z. 279-281)

Auch Hacker WH02 ist in der ehrenamtlichen Vereinsarbeit aktiv und zeigte teilweise niedrigere SD3-Scores unter den Normwerten der Allgemeinbevölkerung (PSYCH: 2,44, NARC: 2,33, MACH: 2,67).

Nur White Hat WH03 zeigte auffällig hohe Triade-Werte (PSYCH: 3.22, NARC: 3.89, MACH: 3.78), was auch in den Antworten deutlich wurde:

„Total, mir ist egal was andere von mir halten. Ich würde über Leichen gehen meine Ziele zu erreichen. Ich habe ein sehr starkes schwarz / weiß denken und unterscheide sehr schnell zwischen Freund und Feind.“ (WH03, Z. 141-143)

„Empathie ist nicht meine Stärke. Häufig sind Menschen selber schuld.“ (WH03, Z. 132)

WH04 war beim militärischen Nachrichtendienst zuständig für HUMINT (Human Intelligence), also zum Beispiel das Anwerben menschlicher Quellen. Diese Tätigkeit machte es notwendig, Menschen nach ihrem Informationsnutzen zu bewerten, was eine Gewohnheit ist, die auch Jahre später schwer abzulegen zu sein scheint:

„[...] ich glaube, dass mir das durch diese 15 Jahre Intel [Anm.: Nachrichtendienstarbeit] in einem Art Mindset so indoktriniert wurde, dass ich heute gar nicht mehr anders kann, als langfristig zu denken. Also wenn ich heute jemanden

kennenlerne, ist in meinem Mindset immer der Gedanke, wer weiß, ob der nicht irgendwann mal spannend sein könnte für mich. Ich würde den deswegen nicht manipulieren. Das tue ich auch nicht, also nicht bewusst. Aber den Gedankengang habe ich, aber der kommt einfach daher, dass wir damals alle so geprägt wurden. Du weißt nie, wenn du jemanden kennenlernst und er ist noch nicht deine Quelle, ob er nicht übermorgen deine Quelle werden könnte.“ (WH04, Z. 296-304)

Dies ist als eine Art ‚gewöhnheitsmäßige Nutzenorientierung‘ zu bewerten, die sich aber im Gegensatz zu Black Hat Hackern nicht in einem aktiven Manipulieren anderer Menschen niederschlägt.

6.7 Diskussion

6.7.1 Zusammenfassung und Bewertung der zentralen Befunde

Das Ziel der dritten Studie bestand in der Validierung der quantitativen Ergebnisse. Durch die Leitfadeninterviews mit aktiven Black Hat Hackern konnten die wesentlichen quantitativen Befunde validiert werden. Dabei traten besonders drei Mechanismen hervor, die cyberkriminelles Verhalten erklären:

- (1) Hohe Ausprägungen bei primärer Psychopathie und Machiavellismus (also skrupellos-strategisches Handeln und Denken).
- (2) Online-Enthemmung bzw. das Gefühl, Taten im Cyberraum seien ‚nur Theater‘ oder ‚ein Spiel‘.
- (3) Viele Black Hats sehen sich als Gray Hats und haben ausgeprägte Rechtfertigungsstrategien entlang aller acht Mechanismen nach Bandura (1999).

Es lassen sich jedoch nicht drei distinkte ‚Typen‘ unterscheiden im Sinne einer ‚Entweder-Oder-Klassifizierung‘, sondern diese Phänomene vermischen und überlagern sich.

Black Hat Hacker zeigen ein auffälliges Profil in Bezug auf Machiavellismus und primäre Psychopathie (skrupellos, kalt, strategisch), sind jedoch gemäßigt in Bezug auf Narzissmus (Wunsch nach Anerkennung) und sekundäre Psychopathie (Impulsivität). Black Hat Hacker sagen selbst, dass Außendarstellung/ Ego und auch Impulsivität eine Gefahr für die eigene OpSec darstellen und die Entdeckungswahrscheinlichkeit unnötig erhöhen. Dieses

Persönlichkeitsprofil mit hoher Furcht- und Skrupellosigkeit bei gemäßigter Impulsivität könnte somit auch der Grund sein, dass es Tätern oft gelingt, nicht strafrechtlich belangt zu werden. Es ist bei Cyberkriminalität (in Übereinstimmung mit Studie 2) von Motivbündeln auszugehen, wobei intrinsische Motive, wie Herausforderung, besonders hervorzuheben sind, während Geld nicht die Hauptmotivation war und auch in keinem Fall als einziges Motiv genannt wurde.

Die Kompetenz der Polizei im Cyberraum sei nach Black Hat Hackern abhängig von der Ebene und geografisch sehr verschieden, wird jedoch insgesamt als sehr gering eingeschätzt. Alle 14 Black Hats und drei von vier White Hats betonten die besondere Rolle von Social Engineering bei Cyberangriffen. Sowohl Black Hats als auch White Hats sehen künstliche Intelligenz als zweischneidiges Schwert mit Chancen und Risiken. Derzeit nutzen Black Hat Hacker KI primär für Recherchezwecke und z.B. das Erstellen fehlerfreier Phishing-Mails. Zur Codegenerierung oder für automatisierte Angriffe seien die KI-Modelle (noch) nicht fortgeschritten genug.

Überraschend und relevant ist der Befund, dass fast alle Black Hats und White Hats eine identische Entstehungsgeschichte berichten: Über Modding und Cheating in Computerspielen stoßen sie im Alter von 10-17 Jahren auf das Hacking und agieren und lernen ihre Fähigkeiten primär im Selbststudium über Hacker-Foren, YouTube, Telegram und das Darknet. Das ‚richtige Hacking‘ lerne man den Befragten zufolge nicht in Schule oder Studium, sondern eher im Darknet, Foren und dem rechtlichen Graubereich.

Die Frage ist damit weniger, warum Personen Black Hat Hacker werden, sondern warum sie dabeibleiben, statt die Fähigkeiten im Laufe des Heranwachsens in legale Bahnen zu lenken.

6.7.2 Methodische Reflexion

Die vorliegende Untersuchung basierte auf leitfadengestützten, problemzentrierten Interviews, um subjektive Sichtweisen von Hackern möglichst offen zu erfassen und gleichzeitig eine Vergleichbarkeit der Themen zu gewährleisten.

Das methodische Vorgehen orientierte sich am „explanatory sequential design“ (Creswell & Plano Clark, 2018, S. 77), bei dem quantitative Ergebnisse im Anschluss qualitativ erklärt, validiert und vertieft werden sollen. Aus diesem Grund orientierte sich der Leitfaden sehr eng am zuvor verwendeten quantitativen Fragebogen. Zwar wurden Antworten in dieser Studie offen erfasst, das Erhebungsinstrument zeichnete sich jedoch durch einen hohen Grad der Standardisierung aus, um so eine Objektivität und Vergleichbarkeit herzustellen.

Aufgrund der hohen Sicherheitsanforderungen von Black Hat Hackern konnten die Leitfadeninterviews überwiegend nur schriftlich, anonym und kryptografisch verschlüsselt durchgeführt werden, teilweise direkt in Darknet-Chats. Das hat den Nachteil, dass keine Kontrolle der Erhebungssituation möglich war. Der Vorteil bestand aber darin, dass Interviewer-Effekte, also Verzerrungen durch Anwesenheit des Interviewers (West & Blom, 2016), ausgeschlossen waren.

Auch in der Auswertungsphase wurde das Kategoriensystem nicht induktiv am Material entwickelt, sondern es handelte sich um eine „deduktive Kategorienanwendung“ (Mayring, 2010, S. 603), da die Themenstruktur bereits durch den Leitfaden festgelegt war. Insgesamt zeichnete sich das Vorgehen trotz qualitativer Methodik durch einen hohen Grad der Standardisierung und Objektivität aus.

Ein Kritikpunkt und Vorwurf an qualitative Forschung ist die *Selektive Plausibilisierung*:

„So lautet eine häufig geäußerte Kritik, qualitative Forschung mache Interpretationen und Ergebnisse für den Leser lediglich dadurch transparent und nachvollziehbar, dass <illustrative> Zitate aus Interviews oder Beobachtungsprotokollen eingeflochten werden“ (Flick, 2025, S. 488).

Das heißt, die eigenen Hypothesen oder subjektiven Interpretationen werden (so die Kritik) durch einzelne Zitate belegt, wobei der Leser keine Transparenz darüber hat, welche Zitate berücksichtigt und welche weggelassen wurden. Um diesem Kritikpunkt zu begegnen, wurden die vollständigen, thematisch sortierten Codebögen der Black Hats und White Hats dem Anhang beigelegt. Das bedeutet im Codebogen der Black Hats in der Kategorie ‚Motive‘ finden sich lückenlos *alle* Aussagen von Black Hat Hackern zur Motivation der Taten. Somit kann der Leser oder die Leserin transparent nachvollziehen, ob aus der Summe aller Zitate die richtigen Schlussfolgerungen und Generalisierungen gezogen wurden.

Außerdem stehen die Interpretationen („Codes“) unmittelbar neben den Zitaten, aus denen sie abgeleitet wurden, siehe Tabelle 16:

Tabelle 16: Ausschnitt Codebogen: Zitate und Interpretationen

BH05	„I do phishing and bank scams. Well, I'm Involved in any job that is financially motivated“ (Z. 44-45)	Finanzielle Motive
------	--	--------------------

Um subjektive Verzerrungen bei der Codierung von Merkmalen der Dunklen Triade zu vermeiden, wurden die Befragten zusätzlich gebeten, die SD3 (quantitativ) auszufüllen, um die qualitativen Interpretationen zusätzlich quantitativ zu validieren. Einige Hacker (8 von 14 Black Hats und 3 von 4 White Hats) kamen der Bitte nach, sodass ein direkter Bezug zwischen Innenperspektive und SD3-Scores möglich war.

Ebenfalls wurden die angewendeten Kategorien zusätzlich ausgezählt und berichtet, z.B., dass bei 7 von 14 Black Hats umfassende Rechtfertigungsstrategien erkennbar waren. Das Ziel war dabei keine Repräsentativität, sondern eine zusätzliche Nachvollziehbarkeit der Interpretation durch Transparenz, wie häufig eine Kategorie in den Interviewdaten erkennbar war.

Durch die standardisierte Durchführung und intersubjektive Nachvollziehbarkeit der Interpretationen konnten die Gütekriterien von Mayring (2023, S. 123-124) der „Verfahrensdokumentation“, „Argumentative[n] Interpretationsabsicherung“,

„Regelgeleitetheit“ und „Nähe zum Gegenstand“ eingehalten werden. Es ist gelungen, die quantitativen Ergebnisse zu validieren und um die Innenperspektive zu erweitern.

Die Schwäche der Methodik liegt (wie auch bei Studie 2) im Sampling und der Erhebungssituation. Da keine Liste von weltweiten, aktiven Cyberkriminellen vorliegt, sind Methoden der Zufallswahl kaum möglich. Es mussten also Hacker-Foren und innerhalb der Foren Probanden bewusst ausgewählt werden (Relevanzkriterium) oder zum Teil auf Methoden der Selbstselektion zurückgegriffen werden, was mit potentiellen Verzerrungen einhergeht. Da Black Hat Hacker aus allen Teilen der Welt kommen und extrem ‚Opsec-sensitiv‘ agieren, waren persönliche Treffen nicht realisierbar.

Auch die kleine Fallzahl, wie im qualitativen Paradigma üblich, ist nicht statistisch repräsentativ.

Diese methodischen Schwächen sind jedoch im Gesamtkontext des *Mixed Method Designs* (Creswell & Plano Clark, 2018) zu betrachten. Studie 2 hatte eine hohe Fallzahl ($N = 1.185$), aber weniger inhaltliche Tiefe. Studie 3 hatte das Ziel, die statistisch signifikanten Ergebnisse mit einer kleinen Fallzahl von 18 Leitfadeninterviews zu vertiefen, sodass im Gesamtkontext ein schlüssiges Hackerprofil entsteht, das im folgenden Kapitel (Gesamtfazit) dargestellt wird.

7 Allgemeine Diskussion und Schlussfolgerungen

7.1 Zusammenführung der Ergebnisse

Die Hauptforschungsfrage war, inwiefern sich Black Hat Hacker und White Hat Hacker hinsichtlich subklinischer Persönlichkeitsdispositionen der Dunklen Triade (Psychopathie, Machiavellismus und Narzissmus) unterscheiden. Das Ziel der Arbeit bestand darin, durch ein *Mixed Method Design* nach Creswell & Plano Clark (2018) in drei Studien ein klares Profil von Black Hat Hackern zu identifizieren und Unterschiede zu White Hat Hackern zu identifizieren, um die Frage zu beantworten, warum sie cyberkriminell agieren. Ein besseres Verständnis der Ursachen der Kriminalität (Kriminalätiologie) und klar abgrenzbare Täterprofile haben potentiell sowohl für die Prävention als auch für die Strafverfolgung (z.B. Cyberprofiling) praktische Relevanz.

Über kriminelle Hacker im Darknet, also außerhalb des Strafvollzugssystems, existierte kaum empirisches Wissen. Im Folgenden sollen die Ergebnisse der drei Studien zusammengeführt werden, sowie zum bisherigen Forschungsstand (Kapitel 3) in Beziehung gesetzt werden.

Studie 1 (quantitative Inhaltsanalyse der FBI Cyber Most Wanted Fahndungsplakate von 2010 bis 2024) hat ein klares demografisches Profil ergeben, basierend auf behördlich verifizierten Daten: Der ‚typische‘ FBI Most Wanted Hacker im Erhebungszeitraum ist männlich (100 %), durchschnittlich 31 Jahre alt, 75 % kommen aus Russland, China, Nordkorea oder dem Iran, 59 % sind direkt oder indirekt Teil eines Nachrichtendienstes der geopolitischen Konkurrenten der USA. Das FBI bietet bis zu 10 Mio. Dollar Belohnungen, was die Relevanz für die nationale Sicherheit unterstreicht. Zwar stehen die Profile der meistgesuchten Hacker der USA nicht repräsentativ für die Grundgesamtheit aller Black Hat Hacker; die Erkenntnis, dass Hacker mehrheitlich jung und männlich sind, ist empirisch gut belegt, wie im Kapitel 3.3. zum Forschungsstand dargestellt (siehe z.B. BKA, 2015b; Huber, 2019, S 39).

In *Studie 2* (quantitative Online-Befragung) wurden insgesamt $N = 1.185$ Hacker rekrutiert, darunter 334 Black Hat Hacker und 851 White Hat Hacker. Das ist eine der bisher

umfassendsten empirischen Studien mit Hackern außerhalb des Strafvollzugs. Die wesentliche Leistung bestand darin, *aktive* Black Hat Hacker in Hacker-Foren im Darknet und Clearnet zu rekrutieren, um so empirischen Zugang zu Probanden zu bekommen, die im Verborgenen agieren und bisher kaum empirisch berücksichtigt wurden. Durch ein Rekrutierungsvideo und die kompromisslose Sicherstellung der Anonymität der Probanden (Operational Security) konnte ein abgrenzbares Profil von Black Hat Hackern erstellt werden (siehe Abbildung 44).

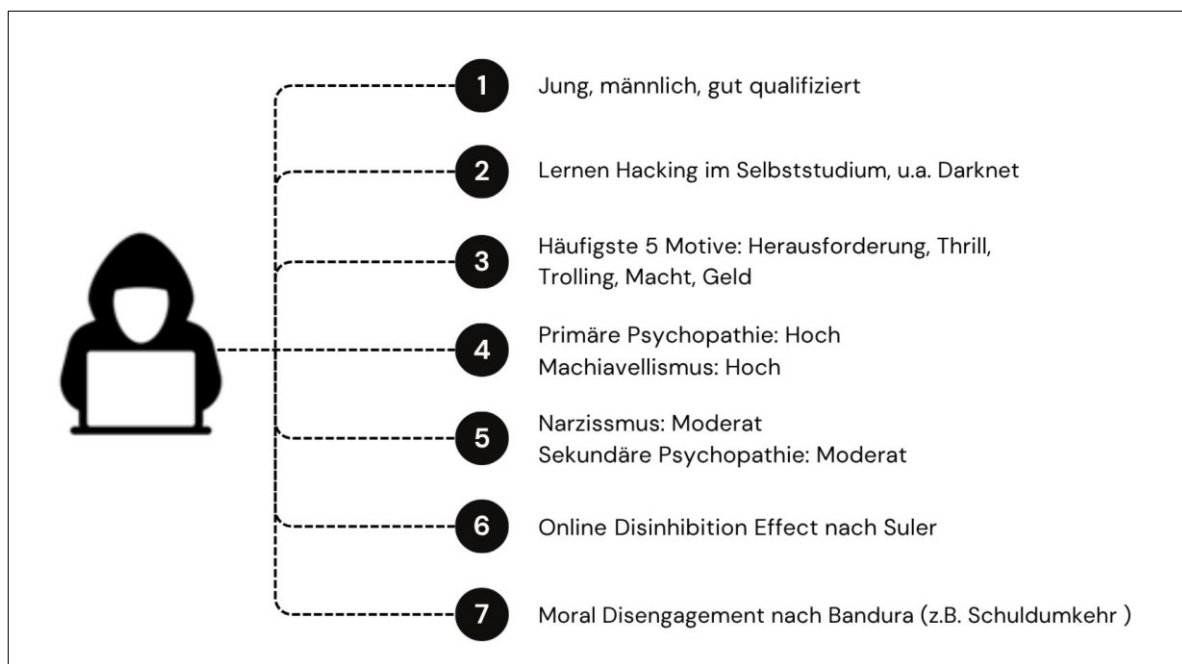


Abbildung 44. Übersicht empirischer Befunde zum Profil von Black Hat Hackern

Quelle: Eigene Darstellung, Piktogramm: Vector Stall (flaticon.com)

Anmerkung. Online Disinhibition Effect, siehe Suler (2004) und Moral Disengagement Theorie, siehe Bandura (1999)

Demografie

Die Stichprobe der Black Hat Hacker war mehrheitlich männlich (89,5 %), jung (69,2 % unter 30) und gut qualifiziert (91,9 % Akademiker oder auf dem Weg dorthin). Die Stichprobe der White Hat Hacker unterschied sich hierin kaum, bis auf ein berufsbedingt leicht höheres Alter (92,4 % männlich, 46,5 % unter 28 Jahre, 93,5 % Akademiker oder auf dem Weg dorthin). Dass Hacker eher jung sind (BKA, 2015b, S. 8) und der Männeranteil ca. 76-94 % beträgt

(S.10), lässt sich auch ein Jahrzehnt später noch bestätigen. Nicht bestätigen lässt sich jedoch die Prognose von Chiesa et al. (2009, S. 90), die bereits vor über 15 Jahren einen zukünftig steigenden Frauenanteil im Hacking vermuteten. Cyberkriminalität ist - wie viele andere Deliktsbereiche auch - noch eine Männerdomäne.

Motive von Black Hat Hackern

Wie bei der Darstellung des aktuellen Forschungsstandes in Kapitel 3.3 ausgeführt wurde, betont das BKA (2015b) in einer Literaturanalyse, es sei bei Hackern von „Motivbündeln“ (S. 28) auszugehen. Das konnte empirisch bestätigt werden. Die Ergebnisse stehen aber im Widerspruch zu der Aussage von Wernert: „[d]er überwiegende Teil der Cyberkriminellen handelt aus finanzieller Motivation“ (2021, S. 39). Im Durchschnitt gaben Black Hat Hacker 4-5 Motive für ihre Taten an ($M = 4.46$, $SD = 2.17$). Die am häufigsten genannten Motive waren Herausforderung (76.3 %), Thrill (59.3 %), Spaß/Trolling (55,7 %) und Machtgefühle (50.9%). Weniger als die Hälfte der Black Hats gab finanziellen Gewinn als Motivkategorie an (48.8 %). Die Frage nach *dem* Motiv von Hackern greift zu kurz, da verschiedene Motive zeitgleich vorliegen. Auch bei Tätern, die finanziell motivierte Taten begehen, sollten intrinsische Motive (wie die Suche nach Herausforderung) daher nicht unterschätzt werden.

Lerntheorien, Moral Disengagement, Online Disinhibition Effect

Was unterscheidet Black Hat Hacker und White Hat Hacker? Warum agieren Black Hats kriminell, während White Hats ihre Fertigkeiten auf legalem Wege monetarisieren?

Zwar gaben 69 % der Black Hat Hacker an, ihre Fähigkeiten in Hacker-Foren (u.a. Darknet oder Telegram) zu lernen, aber das gilt auch für die Mehrheit der White Hat Hacker (56 %). Trotz der Prozentsatzdifferenz scheinen Lerntheorien allein (Darknet = kriminelle Karriere) nur eine schwache Erklärung für cyberkriminelles Verhalten zu sein.

Ein bedeutsamer Mechanismus in Banduras (1999) *Moral Disengagement Theorie* ist die „Attribution of Blame“ (S. 203), also eine Schuldumkehr: „Victims then get blamed for bringing suffering on themselves“ (S.203). Black Hats und White Hats wurden gefragt, inwiefern sie

der Aussage zustimmen, dass Opfer selbst schuld seien, gehackt zu werden, wenn diese schwache Passwörter nutzen. Sowohl Black Hats als auch White Hats stimmten der Aussage deutlich zu. In der Zustimmung unterschieden sich die Hackergruppen jedoch nur leicht ($d = 0.21$). Zusätzlich wurden Black Hat- und White Hat Hackern hypothetische Szenarien von digitalen und analogen Straftaten vorgelegt, um ihre Offline-Skrupellosigkeit und Online-Skrupellosigkeit zu vergleichen (z.B. „I would hack someone's bank account“ vs. „I would steal someone's wallet in real life“). Es konnte ein Online Disinhibition Effect nach Suler (2004) nachgewiesen werden: Der Mittelwert der Online-Skrupellosigkeit unterschied sich signifikant und stark vom Mittelwert der Offline-Skrupellosigkeit, das gilt jedoch für die Gruppe der Black Hat Hacker ($d = 1.01$) und White Hat Hacker ($d = 1.03$) gleichermaßen.

In Kapitel 3 (Forschungsstand) wurde postuliert, dass Cyberkriminalität nicht monokausal erklärbar ist und Lerntheorien, der Online Disinhibition Effect nach Suler (2004) und die Moral Disengagement Theory nach Bandura (1999) eine Rolle bei Black Hat Hackern spielen könnten. Dies konnte bestätigt werden, jedoch bei Black Hat Hackern *und* White Hat Hackern in ähnlicher Stärke. Die Theorien und der Online-Enthemmungseffekt sind daher nicht durch die Unterschiede in der Kriminalitätsbereitschaft zu erklären. Es wurde daher angenommen, dass diese Faktoren *verstärkend* in Bezug auf cyberkriminelles Verhalten wirken können, ausschlaggebend bleibt jedoch die persönliche Disposition.

Die Dunkle Triade

Besonders subklinische Psychopathie und Machiavellismus zeigen deutliche Zusammenhänge mit nahezu allen Arten antisozialen oder kriminellen Verhaltens (siehe Kapitel 3.1). Über aktive Black Hat Hacker in Clear- und Darknet-Foren existierte hingegen kaum empirisches Wissen. Am relevantesten in Bezug auf die Forschungsfrage war die Untersuchung von Gaia et al. (2021), welche herausfanden: „[...] black hat hackers score high on the Machiavellian and psychopathy scales“ (S.23). Kritisch anzumerken ist, dass es sich bei der Stichprobe von Gaia et al. (2021) nicht um ‚echte‘, aktive Black Hat Hacker oder Akteure im Darknet handelte, sondern um ein studentisches Sample der

Computerwissenschaft und des Managements, die einen Fragebogen zu selbstberichteter Computerdelinquenz ausfüllten.

Die Ergebnisse konnten jedoch an ‚echten‘ Hackern ($N = 1.185$) repliziert und bestätigt werden. Abbildung 45 zeigt grafisch die Mittelwerte der Subskalen der *Short Dark Triad* (Jones & Paulhus, 2014) bei den drei Gruppen Black Hats ($n = 334$), White Hats ($n = 851$) und Referenzwerten für die Allgemeinbevölkerung, sowie die gefundenen signifikanten Gruppenunterschiede gemäß Cohen (1988).

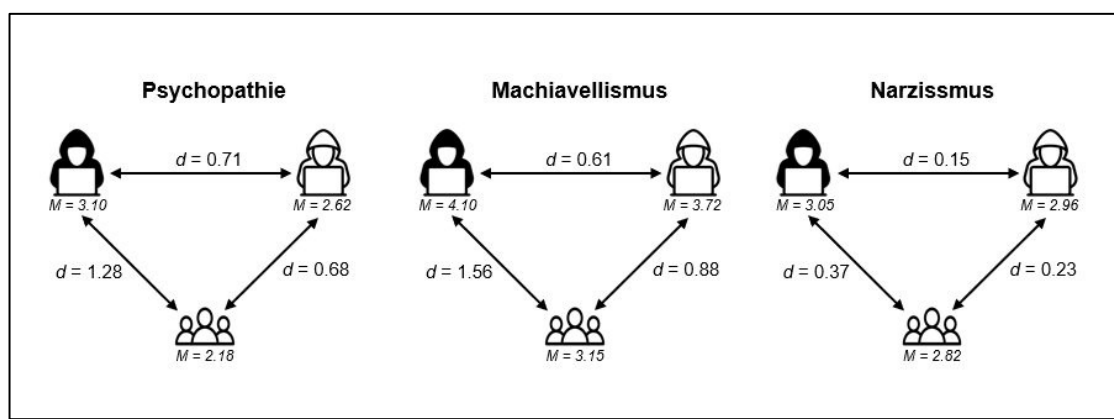


Abbildung 45. Effektgrößen der t -Tests nach Cohen (1988)

Quelle: Eigene Darstellung, Piktogramme: Vector Stall (flaticon.com)

Anmerkung. $n = 334$ Black Hats, $n = 851$ White Hats, Es wurden t -Tests für unabhängige Stichproben zwischen den Hackergruppen durchgeführt und One-Sample t -Tests mit Normwerten der Allgemeinbevölkerung nach Jones & Paulhus (2014). Alle Ergebnisse waren signifikant (zweiseitig) mit $p < .001$, nur der Gruppenunterschied im Narzissmus zwischen Black Hats und White Hats zeigte ein geringeres Signifikanzniveau von $p = .018$ (zweiseitig) bzw. $p = .009$ (einseitig).

Die Abbildung zeigt deutlich - entsprechend der Leithypothese der Arbeit -, dass Black Hat Hacker (subklinisch) psychopathischer und machiavellistischer sind als White Hat Hacker. Im Kontext kriminologischer Theorien wäre dies den „Täterorientierte[n] Theorien“ (Mentzel & Schröder, 2005, S. 36) bzw. Individualtheorien (Kirwan & Power, 2013, S. 17) zuzuordnen.

Dass sich Black Hats und White Hats in psychopathischen und machiavellistischen Persönlichkeitsdispositionen ‚nur‘ moderat voneinander unterscheiden, hat mit dem überraschenden Befund zu tun, dass auch White Hats deutlich machiavellistischer und

psychopathischer als die Allgemeinbevölkerung sind. Nur in der Dimension des subklinischen Narzissmus unterscheiden sich Black Hat Hacker und White Hat Hacker kaum. Im Gegenteil zeigte sich in der binären, logistischen Regression, dass subklinischer Narzissmus bei isolierter Betrachtung leicht die Chance erhöht, White Hat Hacker zu sein. Dieser Befund lässt sich dadurch erklären, dass die Konstrukte der Triade interkorreliert sind (Paulhus & Williams, 2002). Höhere Scores im Narzissmus gehen mit höheren Scores in Psychopathie und Machiavellismus einher, welche wiederum mit dem kriminellen Black Hat Hacking verbunden sind. Betrachtet man Narzissmus jedoch isoliert, zeigen sich eher Zusammenhänge mit White Hat Hacking. Damit konnte Evidenz für eine weitere Vermutung von Gaia et al. (2021) gefunden werden: „white hatters, the good guys, tend to be narcissists“ (S. 23). Für einen Hacker, der ausschließlich narzisstische, nicht aber psychopathische oder machiavellistische Persönlichkeitsdispositionen besitzt, könnte eine Karriere im Scheinwerferlicht interessanter sein als die Dunkelheit und Anonymität des Darknets.

Da das Konstrukt der subklinischen Psychopathie viele Dimensionen enthält und am komplexesten ist, wurde zusätzlich die Levenson Self-Report Psychopathy Scale (Levenson et al., 1995) zur Messung verwendet, um die Faktoren der primären und sekundären Psychopathie differenzieren zu können.

Brinkley et al. (2001, S. 1025) definierten in ihrer Untersuchung einen LSRP-Score in der Höhe von 58 Punkten als Grenzwert, ab der sie von einer hochpsychopathischen Gruppe ausgehen. Der durchschnittliche LSRP-Score der Black Hat Hacker ($n = 258$) lag mit $M = 66.88$ ($SD = 12.31$) deutlich über dem Cut-Off-Score. Black Hat Hacker sind demnach im Durchschnitt als hochpsychopathische Gruppe einzustufen.

Bei primärer und sekundärer Psychopathie unterscheiden sich Black Hats unterschiedlich stark von den Normwerten der Allgemeinbevölkerung. Während sich ein starker Mittelwertunterschied bei primärer Psychopathie ($d = 0.97$) zeigte, war der Unterschied bei sekundärer Psychopathie nur halb so groß ($d = 0.53$).

Primäre Psychopathie ist nach Lykken (1995, S. 133-155) vor allem durch Furchtlosigkeit und strategisches Handeln gekennzeichnet. Sekundäre Psychopathie ist hingegen durch impulsives Verhalten und geringe Selbstkontrolle gekennzeichnet (Hicks & Drislane, 2019, S. 299-300; Lykken, 1995, S. 37). Hacker sind also besonders hinsichtlich ihrer Furchtlosigkeit auffällig, aber gemäßigt, was impulsives Verhalten angeht. Als ‚machiavellistische, primäre Psychopathen‘ ähneln Black Hat Hacker in ihrem Profil damit eher den sogenannten „Successful Psychopaths“ (Mullins-Sweatt, 2010, S. 554) als den gewaltkriminellen Psychopathen. Das Profil von Black Hat Hackern zeichnet sich aus durch:

- hohe Intelligenz
- hohe primäre Psychopathie (Furchtlosigkeit)
- ausgeprägten Machiavellismus
- gemäßigte sekundäre Psychopathie (Impulsivität)
- und gemäßigten Narzissmus (z.B. Selbstdarstellungsdrang)

Korrelation ist nicht mit Kausalität gleichzusetzen und die Daten und Ergebnisse der *t*-Tests lassen keine direkten Kausalschlüsse zu. Die besondere Bedeutung von Psychopathie in Bezug auf Gewaltkriminalität und Aggression ist jedoch empirisch gut belegt (z.B. Porter et al., 2019), sodass DeLisi (2009) Psychopathie als bedeutsamste Erklärung für Kriminalität sieht (S. 256).

Dieser gut abgesicherte empirische Befund der Psychopathieforschung, dass Psychopathie mit Kriminalität zusammenhängt, lässt sich auch auf Black Hat Hacker übertragen, wobei sie in ihrem Profil eher den *erfolgreichen Psychopathen* im Wirtschaftskontext ähneln. Dieses Grundprofil hoher primärer Psychopathie und Machiavellismus bei gleichzeitig gemäßigtem Narzissmus und sekundärer Psychopathie könnte ein wichtiger Grund sein, warum Black Hats kriminell agieren, und auch der Grund, wie es ihnen langfristig gelingt, dem Strafvollzug zu entgehen.

Cyberprofiling: Korrelationen zwischen Modus Operandi, Motiven und Persönlichkeit

Die Basis bzw. die Grundvoraussetzung für Täterprofiling ist die Annahme, dass signifikante Zusammenhänge zwischen Persönlichkeitsmerkmalen und Verhalten bei einer Tat bestehen: „Profiling in effect is based on the assumption that the perpetrator’s decisions and behavior at the crime scene reflect personality traits“ (Chiesa et al. 2009, S. 9). Da es im Fall von *Cyberkriminalität im engeren Sinne* (Hacking) keine Leiche, keine Mordwaffe und auch keinen Tatort im physischen Sinne gibt, war lange fraglich, inwiefern das Profiling im digitalen Raum überhaupt möglich ist (Chiesa et al., 2009, S. 9-12). Es wurde daher empirisch überprüft, ob es Korrelationen zwischen Komponenten der Dunklen Triade und den Motiven und den bevorzugten Angriffsarten von Black Hat Hackern gibt. Das wäre die Grundvoraussetzung, um im Umkehrschluss von Merkmalen der Tat Rückschlüsse auf Merkmale der Täter zu ziehen.

Es konnte gezeigt werden, dass signifikante, aber schwache Korrelationen bestehen, insbesondere zwischen den vier subklinischen Persönlichkeitskonstrukten Psychopathie (SD3), Machiavellismus (SD3), Narzissmus (SD3) und primäre Psychopathie (LSRP) einerseits und den vier Motivkategorien Macht, Thrill, Geld und Rache andererseits.

Wie in Kapitel 3.2 dargestellt wurde, untersuchten Jones et al. (2021) die Dunkle Triade im Zusammenhang mit dem bevorzugten Modus Operandi, wobei sie zeigen konnten, dass Machiavellisten eher zu Social Engineering tendieren, während Narzissmus und Psychopathie mit schnellen, brachialen Angriffsmethoden (wie *Brute Force Angriffe*) verbunden waren. Die Ergebnisse konnten teilweise bestätigt werden. Es zeigten sich schwache Korrelationen zwischen Social Engineering-Angriffen einerseits und Machiavellismus und primärer Psychopathie andererseits. Es konnten jedoch bei Black Hat Hackern - im Widerspruch zu Jones et al. (2021) - keine signifikanten Korrelationen zwischen bevorzugter Angriffsart und Narzissmus sowie sekundärer Psychopathie festgestellt werden.

Insgesamt sind die Ergebnisse Indikator dafür, dass Cyberprofiling grundsätzlich möglich ist, wobei hier weitere Forschung nötig ist, welche Persönlichkeitsdispositionen von Tätern mit welchen Motiven und Angriffsarten verbunden sind.

Nutzung künstlicher Intelligenz für Cyberangriffe

42 % der Black Hat Hacker und 41,5 % der White Hat Hacker haben bereits künstliche Intelligenz für Hacking-Aktivitäten genutzt. Im kriminellen Anwendungsbereich reicht die Nutzung von Recherche und fachlicher Diskussion bis hin zu Malware-Entwicklung, der Generierung von Phishing-Seiten und Automatisierung. Beliebteste Modelle sind derzeit bei Black Hat Hackern ChatGPT und Deepseek, wobei insgesamt 21 verschiedene Modelle genannt wurden, u.a. Modelle wie WormGPT, die ausschließlich für kriminelle Aktivitäten geschaffen wurden. Auch hier konnte der Forschungsstand bzw. die Prognose des BKAs bestätigt werden, die bereits im Bundeslagebild Cybercrime 2023 warnten: „KI steigert die Qualität und Quantität von Cyberangriffen“ (BKA, 2024, S. 24). Es ist davon auszugehen, dass dies nur den Beginn einer Entwicklung darstellt, die die nächsten Jahre prägen wird. Bereits zum jetzigen Zeitpunkt probieren Black Hat Hacker, ihre Cyberangriffe durch KI zu verbessern oder zum Teil zu automatisieren.

Validierung durch Qualitative Interviews mit Black Hat Hackern

In Studie 3 bestand das Ziel darin, erneut Black Hat Hacker in Hacker-Foren im Darknet zu rekrutieren und die quantitativen Daten durch Aussagen von Hackern aus der Innenperspektive zu ergänzen, zu vertiefen und zu validieren. Das Vorgehen entspricht einem *Mixed Method Design* nach Creswell & Plano Clark (2018).

Auch in den Leitfadeninterviews mit Black Hat Hackern bestätigte sich das zuvor identifizierte Profil deutlich. Dabei traten drei zentrale psychologische Mechanismen hervor zur Erklärung von cyberkriminellen Verhalten:

(1) Hohe primäre Psychopathie und Machiavellismus (Motto: „Ich bin kalt und skrupellos“).

Bei 14 von 14 befragten Black Hat Hackern ließen sich entweder machiavellistische Persönlichkeitsdispositionen und/ oder Merkmale primärer Psychopathie codieren (siehe Anhang 8) und somit die Befunde der zweiten Studie replizieren. Die meisten Black Hats entsprechen dem Profil machiavellistischer, primärer Psychopathen.

Beispielhaftes, charakteristisches Zitat:

„Empathy is conditional for me, and I don't feel guilt. I understand emotion much more than I feel it. I analyze people the same way I analyze systems by ways of vulnerabilities, triggers, behavioral loops, etc. I don't necessarily seek chaos, but if it's profitable, I wouldn't flinch either. Emotionally, I am cold. This is not a trait I hide or am ashamed of.” (BH10, Z. 189-193)

Trotz hoher primärer Psychopathie ist die sekundäre Psychopathie (Impulsivität) eher gemäßigt, worin auch Black Hats selbst den Grund sehen, nicht festgenommen zu werden:

„Everything I do is calculated, and for me, I see people as tools and not constants. I don't act out of impulse unless impulse serves the plan, as doing so is OpSec suicide.” (BH10, Z. 201-202)

(2) Der Online-Enthemmungseffekt (Motto: „Es fühlt sich an wie ein fiktives Spiel“).

13 der 14 befragten Black Hats beschrieben deutliche Unterschiede zwischen ihrem Verhalten und ihrer Kriminalitätsbereitschaft online und offline. Lediglich ein Black Hat Hacker (BH10) würde sowohl digital als auch analog stehlen und sieht hierin keinen Unterschied, abgesehen von einer höheren Entdeckungswahrscheinlichkeit. Die anderen Hacker beschrieben alle eine Variante eines Enthemmungsgefühls, dass sich digitale Handlungen unreal anfühlen und vom Selbstbild in der realen Welt abspalten lassen.

Beispielhafte, charakteristische Zitate:

„I feel invisible online [...]” (BH08, Z. 77)

„Online feels more anonymous and theatrical [...]“ (BH13, Z. 78)

„I’m emotional with physical victims, but online, it’s a mask.“ (BH05, Z. 81)

(3) Moral Disengagement nach Bandura (1999) (Motto: „Die Opfer sind selbst schuld“ oder „Ich hacke ja nur Unternehmen.“)

Beispielhaftes Zitat:

„If manipulation gives me benefit, then of course I will. People suffer because of the system and their fault, not because of mine.“ (BH12, Z. 192-193)

14 von 14 befragten Black Hats gaben im Interview mehr oder weniger ausgeprägte Rechtfertigungsstrategien preis, die von leicht beschönigenden Worten bis hin zu einer völligen Schuldexternalisierung reichen. Alle acht Mechanismen der moralischen Rechtfertigung nach Bandura (1999) konnten in den Daten identifiziert werden (siehe Tabelle 15).

In Übereinstimmung mit den quantitativen Ergebnissen ist Cyberkriminalität nicht monokausal erklärbar, sondern ein Zusammenspiel aus Persönlichkeitseigenschaften der Dunklen Triade, dem Online Disinhibition Effect und ausgeprägten Rechtfertigungsstrategien, insbesondere der Schuldexternalisierung. In den Aspekten der Online-Enthemmung und Schuldumkehr unterschieden sich Black Hats und White Hats kaum, während bei Psychopathie und Machiavellismus signifikante Unterschiede mittlerer Stärke identifiziert wurden.

Hieraus die Schlussfolgerung abzuleiten, dass Black Hats aufgrund ihrer Persönlichkeitsdisposition kriminell werden, ist jedoch nicht ganz korrekt, da Studie 3 auch ein überraschendes Ergebnis offenbarte: Sowohl Black Hats als auch White Hats haben fast identische Entstehungsgeschichten berichtet, wie sie im Alter von 10-17 Jahren durch ‚Modding‘ und ‚Cheating‘ in Computerspielen das (illegale) Hacking erlernten.

Drei der vier interviewten White Hats gaben an, in der Kindheit und Jugend Black Hats gewesen zu sein und erst später das Talent in legale Bahnen gelenkt zu haben. Auch quantitativ gaben 56 % der $n = 851$ White Hats der zweiten Studie an, ihre Skills in Hacker-Communities u.a. im Darknet gelernt zu haben. In gewisser Weise dreht das die ‚Baseline‘ bzw. die Ausgangslage herum: Es ist nicht so, dass alle Hacker auf der legalen Seite beginnen und einige dann aufgrund ihrer Persönlichkeit auf die illegale Seite wechseln. Eher andersherum beginnen die meisten Hacker im legalen Graubereich oder als Black Hat Hacker und einige hören im Laufe des Heranwachsens auf, unautorisiert und illegal zu hacken.

In diesem Sinne ist die Dunkle Triade nicht der Grund, warum Black Hats mit dem Hacken *beginnen*, sondern der Grund, warum sie nie damit aufgehört haben.

Aus den hier gewonnenen Daten lässt sich insgesamt ein Drei-Phasen-Modell der Cyberkriminalität ableiten:

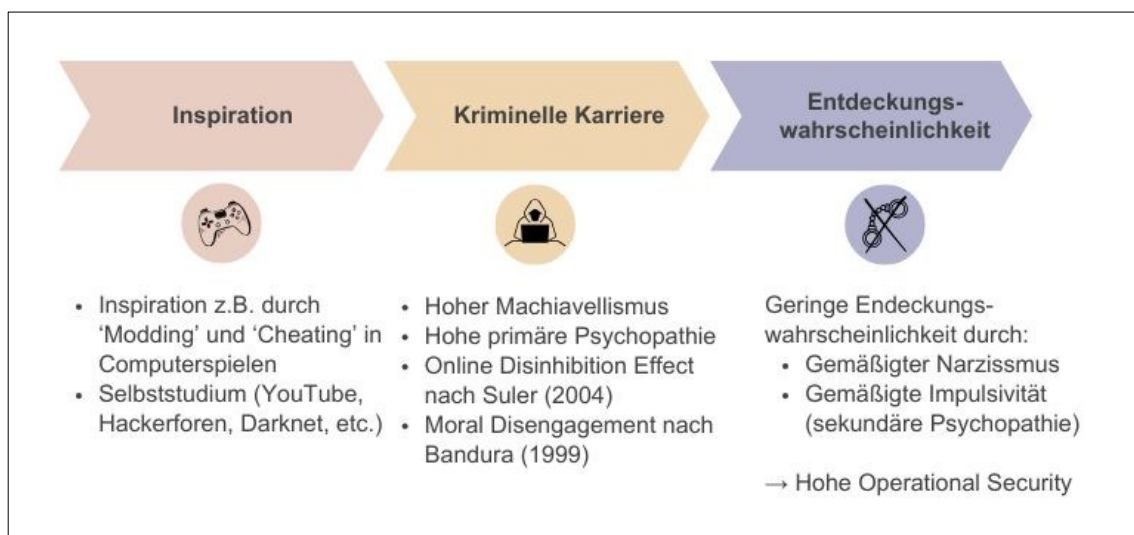


Abbildung 46. Drei-Phasen-Modell der Hacker-Karriere

Quelle: Eigene Darstellung, Piktogramme erstellt mit Hilfe der KI-Software Canva

Phase 1: Sowohl die Hacker, welche später als Black Hats agieren, als auch die Hacker, die später als White Hats agieren, lernen ihre Fähigkeiten häufig auf der ‚dunklen Seite‘ oder im rechtlichen Graubereich. Oftmals im Kindheits- oder Jugendalter (teilweise bereits im Alter

von 10 Jahren) erfolgt die erste Inspiration häufig durch ‚Modding‘ und ‚Cheating‘ in Computerspielen:

„As you will find, if you ask enough hackers, it is often video games, and this applies to me as well. I started hacking in video games when I was 12, probably 13. It very quickly escalated to hacking others' online accounts to continue playing in the game after they were caught. (BH09, Z. 104-106)

„Ich fand Videospiele super und hatte durch „Modding“ den Einstieg gefunden. :-)“ (WH01, Z. 140)

„Mit 10 ist mein Interesse gewachsen. Viel Videospiele, viel YouTube, erste Linux Server (für TeamSpeak etc.)... wollte immer mehr wissen. 4chan. Angriffe auf Mastercard und Visa, selbst als Teen viel geddoSt.“ [Anmerkung: DDoS-Angriffe durchgeführt] (WH03Z. 95-97)

Zwei der drei Zitate stammen von White Hat Hackern. Durch Selbststudium werden erste kleine Hacks möglich, wie das Sperren von Computern in Kaufhäusern, Angriffe gegen die eigene Schule, Carding (Kreditkartenbetrug), das Hacken des WiFi-Netzwerks der Nachbarn und DDoS-Angriffe.

Phase 2: White Hat Hacker sind diejenigen, die den Pfad der Cyberkriminalität im Laufe des Heranwachsens verlassen:

„Ich lebe legal, um nachts ruhig schlafen zu können.“ (WH01, Z. 105-106)

Black Hats gelingt es offensichtlich trotz Cyberkriminalität ruhig schlafen zu können, wofür die beschriebenen drei Mechanismen identifiziert werden konnten:

- Persönlichkeitsmerkmale der Dunklen Triade (besonders primäre Psychopathie und Machiavellismus)
- Online-Enthemmungsfaktoren
- Umfassende Rechtfertigungsstrategien (entlang aller 8 *Moral Disengagement Mechanismen* nach Bandura, 1999).

Cyberkriminalität ist demnach nicht monokausal erklärbar, sondern ein komplexes Zusammenspiel dieser und möglicherweise weiterer Faktoren.

Phase 3: Im Sinne des Modells spielt die Dunkle Triade nicht nur eine Rolle bei der Frage, warum Black Hats sich dauerhaft für eine kriminelle Karriere entscheiden, sondern auch bei der Frage, wie hoch die Entdeckungswahrscheinlichkeit und somit die Wahrscheinlichkeit der Verurteilung ist.

Black Hats haben selbst reflektiert, dass Impulsivität und Narzissmus eine ‚Opsec-Gefahr‘ darstellen können, also die eigene Sicherheit gefährden:

„I don't act out of impulse unless impulse serves the plan, as doing so is OpSec suicide.“ (BH10, Z. 202)

„I have also started acting less impulsively and am more calculating now (a big reason why I believe I won't be caught).“ (BH09, Z. 151-153)

„I do believe there is a low chance of being caught. If you know what you are doing, take basic precautions, and do not allow greed or ego to cloud your OpSec, the chances of actual legal consequences are slim to none.“ (BH10, Z. 124-126)

Der gemäßigte Narzissmus (z.B. Selbstdarstellungsdrang) und die gemäßigte Impulsivität sind möglicherweise der Grund, warum es ihnen gelingt, langfristig der Strafverfolgung zu entgehen.

Die Merkmale der Dunklen Triade zeigen positive Zusammenhänge mit zahlreichen Arten destruktiven Verhaltens (siehe z.B.: Schwarzinger, 2020, S. 57, zur Übersicht Kapitel 3.1.1 und 3.1.2). Das gilt besonders für Psychopathie und Machiavellismus. Nach Furtner (2017) „zählt Narzissmus zur hellsten und positivsten Dimension, während Psychopathie am wenigsten adaptiv und sozial akzeptiert ist“ (S. 6).

Summa summarum konnte gezeigt werden, dass diese Zusammenhänge und ‚Rangfolge der Dunkelheit‘ auch zwischen der Dunklen Triade und Cyberkriminalität bestehen: Narzissmus ist bei isolierter Betrachtung leicht mit dem White Hat Hacking verbunden, während Psychopathie und Machiavellismus deutlich mit dem Black Hat Hacking assoziiert sind.

Oder, wie Black Hat Hacker es selbst formulieren:

„Emotionally, I am cold. This is not a trait I hide or am ashamed of.“ (BH10, Z. 189-193)

7.2 Praktische Relevanz und Ausblick

Damit „selektive Prävention“ (Bürger & Kaess, 2024, S. 405) möglich wird, müssen potentielle Risikogruppen vorerst identifiziert werden.

In Abb. 44, Abb. 45 und Abb. 46 wurde ein klares Black Hat Profil und Drei-Phasen-Modell aufgezeigt, woraus sich ein klar abgrenzbares und erkennbares Risikoprofil ergibt:

Potentielle Black Hat Hacker sind jung, männlich, intelligent, computeraffin und interessieren sich häufig schon in Kindheit und Jugend für Modding und Cheating in Computerspielen, primär motiviert durch die Suche nach Herausforderung, Spaß/Trolling und Thrill. Wenn zusätzlich Persönlichkeitseigenschaften der Dunklen Triade oder ausgeprägte Rechtfertigungsmechanismen oder Enthemmungsfaktoren hinzukommen, steigt die Wahrscheinlichkeit, dass aus der jugendlichen Neugier eine spätere kriminelle Hackerkarriere wird.

Die Herausforderung besteht darin, dieses Talent im Hacking in jungen Jahren in legale Bahnen zu lenken. Das Problem beginnt oft schon früh: Wenn Kinder oder Jugendliche besonders computeraffin sind, ist die Wahrscheinlichkeit, dass dies als Problem oder gar Störung gesehen wird, größer, als dass es als Talent gesehen wird. Typische Sätze von Eltern wie: „Du sitzt von morgens bis abends vor dem Computer, geh doch mal raus“, mögen in der Sache richtig und gut gemeint sein, machen aber auch deutlich, dass Eltern oft das Verständnis oder die Medienkompetenz fehlt, zu begreifen, was ihre Kinder im Cyberspace tun, und es tendenziell eher als Problem gesehen wird, nicht als Talent. Auch in dem Begriff ‚daddeln‘ wird gerne jegliche Online-Aktivität von Kindern und Jugendlichen desinteressiert unter einem despektierlichen Sammelbegriff vereint.

Die Computeraffinität an sich ist kein Problem, im Gegenteil, sie ist ein Talent. Wenn dieses Talent jedoch nicht anerkannt und gefördert wird, dann wird sich die Herausforderung und Anerkennung auf anderem Wege gesucht, z.B. in Gaming-Communities oder Hacker-Foren im Clear- und Darknet.

Nach Ansicht des Forschenden sollte die Intervention nicht darin bestehen, Interesse am Hacking ‚abschalten‘ zu wollen, was wahrscheinlich ohnehin nicht möglich ist, sondern in legale Bahnen zu lenken. Jung, computeraffin und auf der Suche nach Herausforderung zu sein, ist eine gute Basis und kann auch legal genutzt werden.

Aufgrund der Neuroplastizität ist potentiell alles veränderbar und bereits 2015 konnten Konicar und Kollegen zeigen, dass Psychopathie mit SCP-Neurofeedback-Training potentiell behandelbar sein könnte. Insbesondere wenn die Neurofeedback-Intervention in Form eines Computerspiels aufgebaut ist und das intrinsische Motiv der Herausforderung und Neugier anspricht, wäre das ein vielsprechender Ansatz bei jungen Hackern, da es ihrer Lebensrealität und Motiven entspricht.

Auch jede Maßnahme, um (jungen) Hackern im kontrollierten Rahmen eine Herausforderung zu bieten, erscheint auf Basis der Befunde sinnvoll. Zahlreiche staatliche Institutionen und Unternehmen laden Hacker proaktiv ein, Schwachstellen zu finden, und belohnen sie dafür. Sogenannte *Bug Bounty Programme* zahlen Prämien für Sicherheits-Schwachstellen, die gefunden und gemeldet werden, statt sie auszunutzen. Auch sogenannte *Capture the Flag*-Wettbewerbe oder *Hackathons* haben das Ziel, Hackern im kontrollierten Rahmen eine Herausforderung zu bieten. So wie musikalische Kinder in die Bigband der Schule aufgenommen werden und rhetorisch talentierte Kinder von ihren Schulen schnell auf Wettbewerbe, wie ‚Jugend debattiert‘ aufmerksam gemacht werden, so müsste auch Computeraffinität, bzw. das ‚Nerd-Sein‘, als Talent erkannt und entsprechend gefördert werden. Für manche Hacking-Talente könnte auch eine Karriere beim Nachrichtendienst oder der Polizei potentiell interessant sein, da sie hier in fremde Systeme eindringen und spionieren dürfen, nur eben im Sinne der nationalen Sicherheit, statt Cybererpressungen gegen Unternehmen zu begehen.

Die Daten zu Hackerprofilen, Motiven und KI-Nutzung für Cyberangriffe können auch für die Cybersicherheit oder Strafverfolgungsbehörden relevant sein. In Anbetracht der Tatsache, dass 76.3 % der Black Hats ‚Herausforderung‘ als Motiv nennen, ist beispielsweise von einer

Firmenkommunikation, dass man ‚unhackbar‘ sei, eher abzuraten, da es als direkte Challenge oder Einladung verstanden werden könnte.

Die Relevanz der Ergebnisse zeigt sich in vier zentralen Punkten:

- (1) **Schließung einer Forschungslücke:** Die Studien liefern differenzierte empirische Daten zur Dunklen Triade im Kontext von Cyberkriminalität und ergänzen die Psychopathieforschung um Erkenntnisse zu Täterprofilen von Black Hat Hackern.
- (2) **Relevanz für gezielte Prävention:** Das klar umrissene Profil (jung, männlich, gut qualifiziert, computeraffin, Interesse an Modding und Cheats in Computerspielen), sowie das psychologische Profil (machiavellistisch, hohe primäre Psychopathie, mit kontrollierter Impulsivität und reduziertem Narzissmus) sind relevant für gezielte Präventionsmaßnahmen.
- (3) **Relevanz für Strafverfolgung:** Potentiell kann das Wissen zu Täterprofilen im Bereich *Cybercrime im engeren Sinne* auch für Cyberprofiling genutzt werden (siehe auch: Huber, 2019, S. 38-39). Die identifizierten Korrelationen zwischen Persönlichkeitsmerkmalen, Modus Operandi und Motiven sind ein Indiz, dass Täterprofiling im Bereich Cybercrime grundsätzlich möglich ist. Bei der wachsenden Anzahl von Ransomware-Gruppierungen wird die ‚attribution‘, also die Zuordnung von Taten zu Tätern oder Gruppierungen, immer bedeutsamer für die Strafverfolgungsbehörden und Nachrichtendienste.
- (4) **Implikationen für künftige Forschung und Bedrohungsanalysen:** Auch die Daten, wie Täter künstliche Intelligenz bisher nutzen, bieten wichtige Anhaltspunkte für künftige Bedrohungslagen. Es ist weitere Forschung nötig zum Cyberprofiling, den Zusammenhängen zwischen Hacking und Gaming und Persönlichkeitseigenschaften von Hackern. Auch zu dem Thema Hacking als Suchtverhalten, das einige Befragte beschrieben, ist weitere Forschung nötig. 30,8 % der Black Hat Hacker haben „Feelings of Addiction“ (Suchtgefühle) als Motivkategorie angegeben. Auch psychophysiologische

Experimente, z.B. zur Furchtlosigkeit an Hackern in Gefängnissen, wären aufschlussreich, um das Profil von Hackern genauer zu verstehen.

Die gewonnenen Befunde könnten somit einen Beitrag zur Entwicklung von Präventions- und Cyberabwehrstrategien auf allgemeiner Ebene sein. Die konkreten Identitäten der hier befragten Black Hat Hacker sind und waren dem Forschenden zu keinem Zeitpunkt bekannt.

7.3 Methodische Reflexion

In den jeweiligen Diskussionsteilen der einzelnen Studien wurden bereits die methodischen Stärken und Schwächen jeweils kritisch gewürdigt und sollen hier nicht wiederholt werden.

Insgesamt war es eine Herausforderung, aktive Black Hat Hacker, u.a. im Darknet, zu finden und für empirische Forschung zu gewinnen. Es war einer der ersten Versuche, aktive Black Hat Hacker direkt empirisch zu befragen.

Das angewendete *Mixed Method Design* nach Creswell & Plano Clark (2018) erwies sich als nützlich, um sich dem Forschungsgegenstand aus drei verschiedenen methodischen Perspektiven anzunähern. Nach dem Prinzip der „Methodentriangulation“ (Flick, 2004, S. 42) werden quantitative und qualitative Methoden so kombiniert, dass sich die methodischen Stärken und Schwächen gegenseitig kompensieren und die Ergebnisse mit verschiedenen Methoden validiert werden.

In Studie 1 wurden FBI-Fahndungsplakate in Bezug auf demografische Daten inhaltsanalytisch ausgewertet. Der Vorteil ist die Non-Reaktivität des Forschungsgegenstandes und dass es sich um behördlich erfasste Daten handelt und um keine Selbstauskunft der Täter. Die Erkenntnistiefe der Methodik ist jedoch beschränkt.

In Studie 2 wurden insgesamt 1.185 Hacker befragt, darunter 334 Black Hat Hacker, die in Hacker-Foren im Clear- und Darknet rekrutiert wurden. Hierbei wurden etablierte Standardskalen mit bekannter Konstruktvalidität und Reliabilität zur Erfassung der Dunklen Triade und Psychopathie eingesetzt und es konnte gezeigt werden, dass Black Hat Hacker signifikant psychopathischer und machiavellistischer sind als White Hat Hacker. Nachteil der

Methodik ist, dass Antworten mit Standardskalen erfasst wurden und die Realität so notwendigerweise auf Skalenwerte reduziert wurde, ohne dass Hacker selbst zu Wort kamen. Um diese Schwäche zu kompensieren, sollte Studie 3 die quantitativen Daten als „explanatory sequential design“ (Creswell & Plano Clark, 2018, S. 77) validieren, indem Hacker selbst zu Wort kommen. Mit einer kleinen Fallzahl von 14 Black Hat Hackern und 4 White Hat Hackern wurden problemzentrierte Leitfadeninterviews durchgeführt, um an die Innenperspektive (insbesondere der Black Hats) zu kommen. Um der Gefahr der Subjektivität oder „Selektive[n] Plausibilisierung“ (Flick, 2025, S. 488) zu begegnen, wurde ein hoher Grad der Standardisierung gewählt und die intersubjektive Nachvollziehbarkeit der Interpretationen durch klare Dokumentation gewährleistet.

Studie 2 beinhaltete eine große Fallzahl, aber weniger Tiefe und Studie 3 eine kleine Fallzahl, aber mehr Tiefe. Erst durch die Kombination der Methoden (Triangulation) entstand ein ganzheitliches Bild: „Dabei wird von einer wechselseitigen Ergänzung im methodischen Blick auf einen Gegenstand ausgegangen, wobei diese Ergänzung in der komplementären Kompensation der Schwäche und blinden Flecke der jeweiligen Einzelmethode liegt“ (Flick, 2025, S. 44).

Auf diesem Wege konnte ein klares Bild aufgezeigt werden zu Hackerprofilen und der Rolle der Dunklen Triade bei Cyberkriminalität.

Die Hauptschwäche der Studien liegt darin, dass bei aktiven Black Hat Hackern im Darknet keine Zufallswahl, sondern nur eine Selbstselektion oder bewusste Auswahl möglich war. Auch die Form der Befragung war aufgrund der geografischen Verteilung und Sicherheitsanforderungen der Hacker meist nur online und unter hohen Anonymitätsvorkehrungen möglich.

Im Rahmen dieser Arbeit sollten jedoch aktive (erfolgreiche) Hacker außerhalb von Gefängnissen befragt werden. Da die Aufklärungsquoten gering sind, sind nur wenige Hacker inhaftiert. Besonders aufschlussreich sind jedoch gerade die Aussagen von Hackern, denen es gelingt, langfristig unentdeckt zu bleiben. Gerade Aussagen von Hackern, die nicht

inhaftiert sind und es ggf. auch nie sein werden, sind für Strafverfolgungsbehörden und Nachrichtendienste potentiell besonders interessant.

Es konnte durch das methodische Vorgehen auch gezeigt werden, dass es aufwändig, aber nicht unmöglich ist, auch im Darknet seriös zu forschen und Hacker als Probanden zu gewinnen. Für potentielle Replikations- oder Folgestudien sei jedoch abschließend angemerkt, dass Forschung im Darknet mit extrem hohen Anforderungen an Sicherheit, Verantwortung und Ethik einhergehen muss.

Die absolute Anonymität und Sicherheit (OpSec) der Probanden wurde u.a. mit kryptografischer Verschlüsselungstechnik sichergestellt: Kontaktaufnahmen über das Tor-Netzwerk, Kommunikation über PGP-Verschlüsselung und spezielle anonyme E-Mail-Dienste und die Redigierung der Interviewtranskripte hinsichtlich des Ideolekts, sodass auch mit forensischer Linguistik und KI weder jetzt noch in 20 Jahren eine Deanonymisierung der Probanden möglich ist. Es wurden Maßnahmen zur Sicherstellung der Anonymität und Sicherheit ergriffen, die weit über das ansonsten übliche Maß hinausgehen.

Neben der forschungsethischen Verpflichtung, die Probanden zu schützen, ist auch der Eigenschutz wichtig. Aktive Kriminelle zu kontaktieren, ist mit dem Risiko verbunden, selbst angegriffen zu werden. Es wurden vorab höchste Cybersecurity-Maßnahmen ergriffen, ein separates Gerät für Darknet-Forschung und VPN-Verbindungen in separatem WLAN genutzt und eine Cyberversicherung abgeschlossen, wobei es trotzdem zu einem Fall von *Doxxing* u.a. der Büroadresse des Forschenden im Darknet kam, die daraufhin aus Sicherheitsgründen gewechselt wurde.

Auch rechtlich wurde eine Strafrechtskanzlei beauftragt, um die genauen rechtlichen Grenzen und Rahmenbedingungen zu kennen und zu jedem Zeitpunkt strikt einzuhalten und ethisch zu handeln.

Seriöse Forschung im Darknet ist also möglich, geht aber mit hohen Anforderungen einher und setzt ethisches, rechtskonformes, verantwortungsvolles und sicherheitsbewusstes Handeln voraus.

Literaturverzeichnis

- Acker, F.-H. (2023). White Gloves Theory. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminologie 1* (S. 39-70). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-35439-8_2
- Aiken, M. P., Davidson, J. & Amann, P. (2016). *Youth Pathways into Cybercrime*. Europol. Verfügbar unter: <https://www.europol.europa.eu/cms/sites/default/files/documents/pathways-white-paper.pdf>
- Aiken, M. P., Davidson, J. C., Walrave, M., Ponnet, K. S., Phillips, K. & Farr, R. R. (2024). Intention to Hack? Applying the Theory of Planned Behaviour to Youth Criminal Hacking. *Forensic Sciences*, 4(1), 24-41. doi: 10.3390/forensicsci4010003
- Alpers, G. W. & Eisenbarth, H. (2008). *Psychopathic Personality Inventory-Revised. Deutsche Version*. Göttingen: Hogrefe.
- Al-Qarni, E. A. (2023). Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies. *International Journal of Advanced Computer Science and Applications*, 14(5), 135-140. doi: 10.14569/IJACSA.2023.0140513
- Amo, L., Gaia, J., Murray, D., Sanders, G. L., Sanders, S. P., Upadhyaya, S. & Wang, X. (2023). Primary and Secondary Control as Antecedents to the Dark Traits in Predicting Attraction to Hacking Behavior. *Journal of Organizational Psychology*, 23(3), 99-111. doi: 10.33423/jop.v23i3.6488
- Amos, B., Longpré, N. & Roos, M. (2024). The Dark Triad of Personality: Attitudes and Beliefs Towards White-Collar Crime. *Journal of White Collar and Corporate Crime*, 5(1), 58-73. doi: 10.1177/2631309X221120002
- AnonSec. (2025). *Telegram-Kanal*. Verfügbar unter: <https://t.me/anonsec16>
- Anonym (Auftragshacker). (2025). *Darknet-Auftragshacker*. Verfügbar unter: jn6weomv6klvnwdwcgu55miabpwklsmmyaf5qrkt4miif4shrqmvdhqd.onion/index¹⁹
- Anonymous Planet. (2023). *The Hitchhiker's Guide to Online Anonymity*. Verfügbar unter: <https://archive.org/details/the-hitchhikers-guide-to-online-anonymity-version-1.1.9-august-2023>
- Babiak, P., Neumann, C. S. & Hare, R. D. (2010). Corporate psychopathy. Talking the walk. *Behavioral Sciences & the Law*, 28(2), 174-193. doi: 10.1002/bsl.925
- Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review*, 84(2), 191-215. doi: 10.1037/0033-295X.84.2.191
- Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. *Personality and Social Psychology Review*, 3(3), 193-209. doi: 10.1207/s15327957pspr0303_3
- Baughman, H. M., Dearing, S., Giammarco, E. & Vernon, P. A. (2012). Relationships between bullying behaviours and the Dark Triad: A study with adults. *Personality and Individual Differences*, 52(5), 571-575. doi: 10.1016/j.paid.2011.11.020

¹⁹ Haftungsausschluss für Links: Links zu Hacking-Foren, Gruppen und Seiten (teils im Darknet) werden aus Transparenzgründen angegeben, sofern diese zitiert wurden. Probanden-Gesuche wurden soweit möglich nach Abschluss der Feldphase gelöscht. Seiten im Darknet sind nur über das Tor-Netzwerk erreichbar und mit erheblichen Risiken verbunden. Vom Besuch wird ausdrücklich abgeraten.

- Benning, S. D., Patrick, C. J., Hicks, B. M., Blonigen, D. M. & Krueger, R. F. (2003). Factor structure of the psychopathic personality inventory: validity and implications for clinical assessment. *Psychological Assessment*, 15(3), 340-350. doi: 10.1037/1040-3590.15.3.340
- Benning, S. D., Venables, N. C., & Hall, J. R. (2019). Successful Psychopathy. In C. J. Patrick (Hrsg.), *Handbook of psychopathy*, (2. Aufl., S. 585-610). New York: The Guilford Press.
- Bergk, A. & Raschke, L. (2023). Die neue Aufgabe der internen Kommunikation: schwierige Unternehmenspersönlichkeiten erkennen. In A. Bergk, R. Frandrup & C. Morasch (Hrsg.), *Corporate Psychopathy. Studienergebnisse, Herausforderungen und die Rolle der Internen Kommunikation im Umgang mit der Dunklen Triade in Unternehmen* (S. 83-93). Berlin: Springer Gabler.
- Best Carding World. (2025). *Darknet-Hackerforum*. Verfügbar unter: bestteermb42clir6ux7xm76d4jjodh3fpahjgqbdbmfrgp4skg2wqd.onion/
- Birbaumer, N., Veit, R., Lotze, M., Erb, M., Hermann, C., Grodd, W. & Flor, H. (2005). Deficient fear conditioning in psychopathy. A functional magnetic resonance imaging study. *Archives of General Psychiatry*, 62(7), 799-805. doi: 10.1001/archpsyc.62.7.799
- Bitkom. *Studie Wirtschaftsschutz 2023*. Verfügbar unter: <https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf>
- Boddy, C. R. (2014). Corporate Psychopaths, Conflict, Employee Affective Well-Being and Counterproductive Work Behaviour. *Journal of Business Ethics*, 121(1), 107-121. doi: 10.1007/s10551-013-1688-0
- Bortz, J. & Schuster, C. (2010). *Statistik für Human- und Sozialwissenschaftler mit 163 Tabellen* (7., Aufl.). Berlin/ Heidelberg: Springer.
- Branković, I., Dinić, B. M. & Jonason, P. K. (2023). How traditional stalking and cyberstalking correlate with the Dark Tetrad traits? *Current Psychology*, 42(30), 26238-26242. doi: 10.1007/s12144-022-03681-z
- Breachform. (2025). *Darknet-Hackerforum*. Verfügbar unter: breifr4yaz477lolmydcr6xteargckje62y7gdl6deevnix57rhct7egd.onion
- Breuer, F. (2010). Wissenschaftstheoretische Grundlagen qualitativer Methodik in der Psychologie. In G. Mey & K. Mruck (Hrsg.), *Handbuch Qualitative Forschung in der Psychologie* (S. 35-49). Wiesbaden: VS Verlag für Sozialwissenschaften. doi: 10.1007/978-3-531-92052-8_2
- Brewer, G., Hunt, D., James, G. & Abell, L. (2015). Dark Triad traits, infidelity and romantic revenge. *Personality and Individual Differences*, 83, 122-127. doi: 10.1016/j.paid.2015.04.007
- Briken, P. & Tozdan, S. (2018). Psychopathie, antisoziale Persönlichkeitsstörung und Sexualdelinquenz. *Forensische Psychiatrie, Psychologie, Kriminologie*, 12(3), 199-206. doi: 10.1007/s11757-018-0482-3
- Brinkley, C. A., Schmitt, W. A., Smith, S. S. & Newman, J. P. (2001). Construct validation of a self-report psychopathy scale: does Levenson's self-report psychopathy scale measure the same constructs as Hare's psychopathy checklist-revised? *Personality and Individual Differences*, 31(7), 1021-1038. doi: 10.1016/S0191-8869(00)00178-1
- Brooks, N. & Fritzson, K. (2020). The Assessment of Psychopathic Personality Across Settings. In K. Fritzson, N. Brooks & S. Croom (Hrsg.), *Corporate psychopathy:*

- Investigating destructive personalities in the workplace* (S. 107-150). Cham, Schweiz: Palgrave Macmillan.
- Brooks, N., Fritzon, K. & Watt, B. (2020). Overview of Theories and Empirical Findings Relevant to Psychopathic Personality Characteristics Amongst High-Functioning Populations. In K. Fritzon, N. Brooks & S. Croom (Hrsg.), *Corporate psychopathy: Investigating destructive personalities in the workplace* (S. 1-46). Cham, Schweiz: Palgrave Macmillan.
- Brosius, H.-B., Haas, A. & Unkel, J. (2022). *Methoden der empirischen Kommunikationsforschung* (8. Aufl.). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-34195-4
- Bruce, M., Lusthaus, J., Kashyap, R., Phair, N. & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PloS One*, 19(4), e0297312. doi: 10.1371/journal.pone.0297312
- Brunell, A. B., Gentry, W. A., Campbell, W. K., Hoffman, B. J., Kuhnert, K. W. & Demarree, K. G. (2008). Leader emergence. The case of the narcissistic leader. *Personality & Social Psychology Bulletin*, 34(12), 1663-1676. doi: 10.1177/0146167208324101
- Buckels, E. E., Jones, D. N. & Paulhus, D. L. (2013). Behavioral confirmation of everyday sadism. *Psychological Science*, 24(11), 2201-2209. doi: 10.1177/0956797613490749
- Buckels, E. E., Trapnell, P. D. & Paulhus, D. L. (2014). Trolls just want to have fun. *Personality and Individual Differences*, 67, 97-102. doi: 10.1016/j.paid.2014.01.016
- Bundesamt für Cybersicherheit (BACS). (2024). *Woche 7: «Mods» und «Cheats» - Das sollten Sie bei Videospielen beachten*. Verfügbar unter: https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/wochenrueckblick_7.html
- Bundesamt für Sicherheit in der Informationstechnik (BSI). (2024). *Generative KI-Modelle. Chancen und Risiken für Industrie und Behörden*. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Generative_KI-Modelle.pdf?__blob=publicationFile&v=5
- Bundesamt für Sicherheit in der Informationstechnik (BSI). (2025a). *Darknet und Deep Web. Wir bringen Licht ins Dunkle*. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Darknet-und-Deep-Web/darknet-und-deep-web_node.html
- Bundesamt für Sicherheit in der Informationstechnik (BSI). (2025b). *DoS- und DDoS-Attacken. Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS)*. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/DoS-Denial-of-Service/dos-denial-of-service_node.html
- Bundeskriminalamt (BKA). (2015a). *Hacktivisten. Abschlussbericht zum Projektteil der Hellfeldebeforschung*. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015HacktivistenProjektteilHellfeldebeforschung.pdf?__blob=publicationFile&v=6
- Bundeskriminalamt (BKA). (2015b). *Täter im Bereich Cybercrime. Eine Literaturanalyse*. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2015TaeterImBereichCybercrime.pdf?__blob=publicationFile&v=6

- Bundeskriminalamt (BKA). (2019). *Bundeslagebild Cybercrime 2018*. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2018.pdf?__blob=publicationFile&v=4
- Bundeskriminalamt (BKA). (2023). *Bundeslagebild Cybercrime 2022*. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2022.pdf?__blob=publicationFile&v=5
- Bundeskriminalamt (BKA). (2024). *Bundeslagebild Cybercrime 2023*. Verfügbar unter: <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2023.html?nn=229942>
- Bundeskriminalamt (BKA). (2025a). *Bundeslagebild Cybercrime 2024*. Verfügbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2024.pdf?__blob=publicationFile&v=3
- Bundeskriminalamt (BKA). (2025b). *Die Underground Economy*. Verfügbar unter: <https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2021/Code2.html>
- Bürger, A. & Kaess, M. (2024). Universelle und selektive Prävention. In J. M. Fegert, F. Resch, M. Kaess, M. Döpfner, K. Konrad, T. Legenbauer, P. Plener (Hrsg.), *Psychiatrie und Psychotherapie des Kindes- und Jugendalters* (3. Aufl., S. 405-422). Berlin/Heidelberg: Springer. doi: 10.1007/978-3-662-66744-6
- Chiesa, R., Ciappi, S. & Ducci, S. (2009). *Profiling hackers. The science of criminal profiling as applied to the world of hacking*. Boca Raton: CRC Press.
- Christie, R. & Geis, F. L. (1970). *Studies in Machiavellianism*. New York: Academic Press. doi: 10.1016/C2013-0-10497-7
- Cleckley, H. (1950/2015). *The mask of sanity. An attempt to clarify some issues about the so-called psychopathic personality* (2. Aufl.). Mansfield Centre, CT: Martino Publishing.
- Coats, D. R. (2019). *Worldwide Threat Assessment of the US Intelligence Community*. Verfügbar unter: <https://www.intelligence.gov/assets/documents/archive/2019-ATA-SFR--SSCI.pdf>
- Cohen, A. K. (1955). *Delinquent boys: the culture of the gang*. Glencoe, IL: Free Press.
- Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences* (2. Aufl.). Hillsdale, NJ: Lawrence Erlbaum Associates. doi: 10.4324/9780203771587
- Cohen, L. E. & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, 44(4), 588-608. doi: 10.2307/2094589
- Coid, J. & Ullrich, S. (2010). Antisocial personality disorder is on a continuum with psychopathy. *Comprehensive Psychiatry*, 51(4), 426-433. doi: 10.1016/j.compsych.2009.09.006
- Coid, J., Yang, M., Ullrich, S., Roberts, A. & Hare, R. D. (2009). Prevalence and correlates of psychopathic traits in the household population of Great Britain. *International Journal of Law and Psychiatry*, 32(2), 65-73. doi: 10.1016/j.ijlp.2009.01.002
- Coid, J., Yang, M., Ullrich, S., Roberts, A., Moran, P., Bebbington, P. & Hickey, N. (2009). Psychopathy among prisoners in England and Wales. *International Journal of Law and Psychiatry*, 32(3), 134-141. doi: 10.1016/j.ijlp.2009.02.008
- Collani, G. (2014). Deutsche Versionen des Narcissistic Personality Inventory (NPI-d). Zusammenstellung sozialwissenschaftlicher Items und Skalen (ZIS). Bonn: GESIS. doi: 10.6102/zis51

- Collison, K. L., Miller, J. D. & Lynam, D. R. (2021). Examining the factor structure and validity of the Triarchic Model of Psychopathy across measures. *Personality Disorders*, 12(2), 115-126. doi: 10.1037/per0000394
- Conti, M., Dragoni, N. & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials*, 18(3), 2027-2051. doi: 10.1109/COMST.2016.2548426
- CrackedSH. (2025). *Clearnet-Hackerforum*. Verfügbar unter: <https://www.cracked.sh>
- Creswell, J. W. & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3. Aufl.). Thousand Oaks, CA: SAGE Publications.
- CryptBB. (2025). *Darknet-Hackerforum*. Verfügbar unter: cryptbbtg65gibadeeo2awe3j7s6evg7eklserehqr4w4e2bis5tebid.onion
- DarknetArmy. (2025). *Darknet-Hackerforum*. Verfügbar unter: cdna777ucpo4unwxrw5mzs4iqm5qz3uepw3k5mvwb7tnufryvsgy5yd.onion
- Dave, K. T. (2013). Brute-force attack 'seeking but distressing'. *International Journal of Innovations in Engineering and Technology* 2(3), 75-78.
- DeLisi, M. (2009). Psychopathy is the Unified Theory of Crime. *Youth Violence and Juvenile Justice*, 7(3), 256-273. doi: 10.1177/1541204009333834
- Deutsche Gesellschaft für Online Forschung (DGOF). (2021). *Richtlinie für die Befragung von Minderjährigen*. Verfügbar unter: <https://www.dgof.de/wp-content/uploads/2021/01/RL-Minderjaehrigen-neu-2021.pdf>
- Deutsche Gesellschaft für Psychologie (DGPs). (2018). *Ethisches Handeln in der psychologischen Forschung* (1. Aufl.). Göttingen: Hogrefe. <http://doi.org/10.1026/02802-000>
- Douglas, K. S., Vincent, G. M. & Edens, J. F. (2019). Risk for Criminal Recidivism: The Role of Psychopathy. In C. J. Patrick (Hrsg.), *Handbook of psychopathy*, (2. Aufl., S. 662-681). New York: The Guilford Press.
- Dread. (2025a). *Kommentar im Darknet Unterforum d/Socialengineering (Nutzer anonym)*. Verfügbar unter: dreadytognbh7m5nlmqsgzzlxjy75iuxkulewbhxcorupbqahact2yd.onion/post/1e6aa04d9ec0c0f8564b
- Dread. (2025b). *Startseite des Darknet-Forums Dread*. Verfügbar unter: <http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/>
- Dread. (2025c). *Titelbild im Darknet-Unterforum d/OpSec*. Verfügbar unter: dreadytognbh7m5nimqsogzzlxjy75iuxkulewbhxcorupbqahact2yd.onion/d/OpSec/wiki?id=ea7f4385
- Dread. (2025d). *Unterforum d/fraud (Darknet)*. Verfügbar unter: dreadytognbh7m5nimqsogzzlxjy75iuxkulewbhxcorupbqahact2yd.onion/
- Dread. (2025e). *Unterforum d/hacking (Darknet)*. Verfügbar unter: dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/
- Dreißigacker, A., Skarczynski, B. von, Bergmann, M. C. & Wollinger, G. R. (2020). Cyberangriffe gegen private Internetnutzer*innen. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie. Kriminologie für das digitale Zeitalter* (S. 319-344). Wiesbaden: Springer VS.
- Duradoni, M., Gursesli, M. C., Martucci, A., Gonzalez Ayarza, I. Y., Colombini, G. & Guazzini, A. (2023). Dark Personality Traits and Counterproductive Work Behavior: A

- PRISMA Systematic Review. *Psychological Reports*, 128(6), 3939-3966. doi: 10.1177/00332941231219921
- Dutton, K. (2014). *Psychopathen. Was man von Heiligen, Anwälten und Serienmördern lernen kann* (6. Aufl.). München: dtv.
- Elsenhans, T. (1912/1920). *Lehrbuch der Psychologie*. Tübingen: Mohr.
- European Union Agency for Fundamental Rights. (2017). *Consent to use data on children*. Verfügbar unter: <https://fra.europa.eu/en/publication/2017/mapping-minimum-age-requirements-concerning-rights-child-eu/consent-use-data-children>
- Externbrink, K. & Keil, M. (2018). *Narzissmus, Machiavellismus und Psychopathie in Organisationen*. Wiesbaden: Springer Fachmedien.
- Falkenbach, D., Poythress, N., Falki, M. & Manchak, S. (2007). Reliability and validity of two self-report measures of psychopathy. *Assessment*, 14(4), 341-350. doi: 10.1177/1073191107305612
- FBI. (2025a). *Cyber Most Wanted*. Verfügbar unter: <https://www.fbi.gov/wanted/cyber>
- FBI. (2025b). *Osama bin Laden*. Verfügbar unter: <https://www.fbi.gov/history/famous-cases/osama-bin-laden>
- Flick, U. (2004). *Triangulation. Eine Einführung* (1. Aufl.). Wiesbaden: VS Verlag für Sozialwissenschaften.
- Flick, U. (2010). Gütekriterien qualitativer Forschung. In G. Mey & K. Mruck (Hrsg.), *Handbuch Qualitative Forschung in der Psychologie* (S. 395-407). Wiesbaden: VS Verlag für Sozialwissenschaften. doi: 10.1007/978-3-531-92052-8_28
- Flick, U. (2025). *Qualitative Sozialforschung. Eine Einführung* (11. Aufl.). Hamburg: Rowohlt Taschenbuch Verlag.
- Frandrup, R. (2023). Dark Triad: die Macht von narzisstischen, machiavellistischen und psychopathischen Führungskräften in der Arbeitswelt. In A. Bergk, R. Frandrup & C. Morasch (Hrsg.), *Corporate Psychopathy. Studienergebnisse, Herausforderungen und die Rolle der Internen Kommunikation im Umgang mit der Dunklen Triade in Unternehmen* (S. 3-13). Berlin: Springer Gabler.
- Furnham, A., Richards, S. C. & Paulhus, D. L. (2013). The Dark Triad of Personality: A 10 Year Review. *Social and Personality Psychology Compass*, 7(3), 199-216. doi: 10.1111/spc3.12018
- Furtner, M. (2017). *Dark Leadership: Narzisstische, machiavellistische und psychopathische Führung*. Wiesbaden: Springer Gabler.
- Fyshchuk, I., Noesgaard, M. S. & Nielsen, J. A. (2024). Managing cyberattacks in wartime: The case of Ukraine. *Public Administration Review*, 85, 1-9. doi: 10.1111/puar.13895
- Gaia, J., Murray, D., Sanders, G., Sanders, S., Upadhyaya, S., Wang, X & Yoo, C. (2022). The interaction of dark traits with the perceptions of apprehension. *Proceedings of the 55th Hawaii International Conference on System Sciences*, 2227-2236. doi: 10.24251/HICSS.2022.279
- Gaia, J., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. (2021). Dark Traits and Hacking Potential. *Journal of Organizational Psychology*, 21(3), 23-46. doi: 10.33423/jop.v21i3.4307
- George, D. & Mallery, P. (2003). *SPSS for Windows step by step: A simple guide and reference* (4. Aufl.). Boston: Allyn and Bacon.
- GhostSec. (2025). *Telegram-Kanal*. Verfügbar unter: <https://t.me/GhostSec>

- Giammarco, E. A. & Vernon, P. A. (2014). Vengeance and the Dark Triad: The role of empathy and perspective taking in trait forgivingness. *Personality and Individual Differences*, 67, 23-29. doi: 10.1016/j.paid.2014.02.010
- Gillespie, S. M. & Garofalo, C. (2024). Psychopathy. In G. M. Davies, A. R. Beech & M. F. Colloff (Hrsg.), *Forensic Psychology: Crime, justice, law interventions* (4. Aufl., S. 77-102). Hoboken, NJ: Wiley-Blackwell.
- Gillespie, S. M., Jones, A. & Garofalo, C. (2023). Psychopathy and dangerousness: An umbrella review and meta-analysis. *Clinical Psychology Review*, 100, 102240. doi: 10.1016/j.cpr.2022.102240
- Glenn, A. L. & Raine, A. (2014). *Psychopathy. An introduction to biological findings and their implications*. New York/London: New York University Press.
- Grigg, D. W. (2010). Cyber-Aggression: Definition and Concept of Cyberbullying. *Australian Journal of Guidance and Counselling*, 20(2), 143-156. doi: 10.1375/ajgc.20.2.143
- Gylfason, H. F., Sveinsdottir, A. H., Vésteinsdóttir, V. & Sigurvinsdottir, R. (2021). Haters Gonna Hate, Trolls Gonna Troll: The Personality Profile of a Facebook Troll. *International Journal of Environmental Research and Public Health*, 18(11), 5722. doi: 10.3390/ijerph18115722
- Haider, J. (2023). Strafverteidigung im digitalen Zeitalter: über neue Anforderungen, Strafbarkeitsfallen und Drogenhandel über soziale Netzwerke. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminologie 1* (S. 501-541). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-35439-8_21
- Hare, R. D. (1991). *Hare Psychopathy Checklist-Revised (PCL-R)*. Toronto: Multi-Health Systems. doi: 10.1037/t01167-000
- Hare, R. D. (2005). *Gewissenlos. Die Psychopathen unter uns*. Wien: Springer.
- Hare, R. D. & Neumann, C. S. (2008). Psychopathy as a clinical and empirical construct. *Annual Review of Clinical Psychology*, 4, 217-46. doi: 10.1146/annurev.clinpsy.3.022806.091452
- Hautzinger, M. & Thies, E. (2009). *Klinische Psychologie: Psychische Störungen kompakt*. Weinheim: Beltz.
- Hazelwood, R. R. & Warren, J. I. (2003). Linkage analysis: Modus operandi, ritual, and signature in serial sexual crime. *Aggression and Violent Behavior*, 8(6), 587-598. doi: 10.1016/S1359-1789(02)00106-4
- Hemphill, J. F., Hare, R. D. & Wong, S. (1998). Psychopathy and recidivism: A review. *Legal and Criminological Psychology*, 3(1), 139-170. doi: 10.1111/j.2044-8333.1998.tb00355.x
- Henkel, T. (2020). Darknet - die dunkle Seite des Internets? In T. G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie. Kriminologie für das digitale Zeitalter* (S. 175-191). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-28507-4_7
- Henning, H. & Six, B. (1977). Konstruktion einer Machiavellismus-Skala. *Zeitschrift für Sozialpsychologie*, 8, 185-198.
- Henning, H., & Six, B. (1997). Machiavellismus. Zusammenstellung sozialwissenschaftlicher Items und Skalen (ZIS). Bonn: GESIS. doi: 10.6102/zis126
- Hickey, E. W., Walters, B. K., Drislane, L. E., Palumbo, I. M., & Patrick, C. J. (2019). Deviance at its darkest: Serial murder and psychopathy. In C. J. Patrick (Hrsg.), *Handbook of psychopathy*, (2. Aufl., S. 570-584). New York: The Guilford Press.

- Hicks, B. M. & Drislane, L. E. (2019). Variants ("subtypes") of psychopathy. In C. J. Patrick (Hrsg.), *Handbook of psychopathy*, (2. Aufl., S. 297-332). New York: The Guilford Press.
- Hofmann, M. J., Mokros, A. & Schneider, S. (2024). The joy of being frightened: Fear experience in psychopathy. *Journal of Personality*, 92(2), 321-341. doi: 10.1111/jopy.12890
- Hoheisel-Gruler, R. (2020). Der digitale Raum ist kein (grund-)rechtsfreier Raum. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie. Kriminologie für das digitale Zeitalter* (S. 71-108). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-28507-4_3
- Holt, T. J. (2019). Computer Hacking and the Hacker Subculture. In *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (S. 1-18). Cham, Schweiz: Palgrave Macmillan. doi: 10.1007/978-3-319-90307-1_31-1
- Holt, T. J., Burruss, G. W. & Bossler, A. M. (2010). Social Learning and Cyber-Deviance: Examining the importance of a full Social Learning Model in a virtual world. *Journal of Crime and Justice*, 33(2), 31-61. doi: 10.1080/0735648X.2010.9721287
- Holt, T. J., Griffith, M., Turner, N., Greene-Colozzi, E., Chermak, S. & Freilich, J. D. (2023). Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. *Criminology & Public Policy*, 22(4), 825-848. doi: 10.1111/1745-9133.12646
- Hosker-Field, A. M., Gauthier, N. Y. & Book, A. S. (2016). If not fear, then what? A preliminary examination of psychopathic traits and the Fear Enjoyment Hypothesis. *Personality and Individual Differences*, 90, 278-282. doi: 10.1016/j.paid.2015.11.016
- Huber, E. (2019). *Cybercrime. Eine Einführung*. Wiesbaden: Springer VS.
- Huber, E. & Pospisil, B. (2020). Problematik der Hell- und Dunkelfeldanalyse im Bereich Cybercrime. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie. Kriminologie für das digitale Zeitalter* (S. 109-133). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-28507-4_4
- Imageboard 4chan. (2025). *Technology-Board*. Verfügbar unter: <https://boards.4chan.org/g/>
- Interpol. (2021). *National Cybercrime Strategy Guidebook*. Verfügbar unter: https://www.interpol.int/content/download/16455/file/Cyber_Strategy_Guidebook.pdf
- Jauk, E. & Dieterich, R. (2019). Addiction and the Dark Triad of Personality. *Frontiers in Psychiatry*, 10, 662. doi: 10.3389/fpsyt.2019.00662
- Jonason, P. K., Lyons, M., Baughman, H. M. & Vernon, P. A. (2014). What a tangled web we weave: The Dark Triad traits and deception. *Personality and Individual Differences*, 70, 117-119. doi: 10.1016/j.paid.2014.06.038
- Jonason, P. K., Slomski, S. & Partyka, J. (2012). The Dark Triad at work. How toxic employees get their way. *Personality and Individual Differences*, 52(3), 449-453. doi: 10.1016/j.paid.2011.11.008
- Jonason, P. K. & Webster, G. D. (2010). The dirty dozen. A concise measure of the dark triad. *Psychological Assessment*, 22(2), 420-432. doi: 10.1037/a0019265
- Jones, D. N., Padilla, E., Curtis, S. R. & Kiekintveld, C. (2021). Network discovery and scanning strategies and the Dark Triad. *Computers in Human Behavior*, 122, 106799. doi: 10.1016/j.chb.2021.106799
- Jones, D. N. & Paulhus, D. L. (2014). Introducing the short Dark Triad (SD3): A brief measure of dark personality traits. *Assessment*, 21(1), 28-41. doi: 10.1177/1073191113514105

- Karpman, B. (1941). On the need of separating psychopathy into two distinct clinical types: the symptomatic and the idiopathic. *Journal of Criminal Psychopathology*, (3), 112-137.
- Katagiri, N. (2024). Advanced persistent threats and the “big four”: State-sponsored hackers in China, Iran, Russia, and North Korea in 2003-2021. *Comparative Strategy*, 43(3), 280-299. doi: 10.1080/01495933.2024.2317251
- Kebschull, U. (2023). *Computer Hacking. Eine Einführung zur Verbesserung der Computersicherheit in komplexen IT-Infrastrukturen*. Berlin/Heidelberg: Springer. doi: 10.1007/978-3-662-67030-9
- Kerem, E., Fishman, N. & Josselson, R. (2001). The Experience of Empathy in Everyday Relationships: Cognitive and Affective Elements. *Journal of Social and Personal Relationships*, 18(5), 709-729. doi: 10.1177/0265407501185008
- Kerns, Q., Payne, B., & Abegaz, T. (2021). *Double-Extortion Ransomware: A Technical Analysis of Maze Ransomware*. In K. Arai (Hrsg.), *Proceedings of the Future Technologies Conference (FTC) 2021, Band 3* (S. 82-94). Cham, Schweiz: Springer. doi: 10.1007/978-3-030-89912-7_7
- Kiehl, K. A. & Hoffman, M. B. (2011). The criminal psychopath: History, neuroscience, treatment, and economics. *Jurimetrics*, 51, 355-397.
- Kirwan, G. & Power, A. (2013). *Cybercrime. The psychology of online offenders*. Cambridge: Cambridge University Press.
- Konicar, L., Veit, R., Eisenbarth, H., Barth, B., Tonin, P., Strehl, U. & Birbaumer, N. (2015). Brain self-regulation in criminal psychopaths. *Scientific Reports*, 5, 9426. doi: 10.1038/srep09426
- Konrath, S., Meier, B. P. & Bushman, B. J. (2014). Development and validation of the Single Item Narcissism Scale (SINS). *PloS One*, 9(8), e103469. doi: 10.1371/journal.pone.0103469
- Kshetri, N. (2016). Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change*, 66(3), 313-338. doi: 10.1007/s10611-016-9629-3
- Küfner, A. C. P., Dufner, M. & Back, M. D. (2015). Das Dreckige Dutzend und die Niederträchtigen Neun. *Diagnostica*, 61(2), 76-91. doi: 10.1026/0012-1924/a000124
- Lamnek, S. & Krell, C. (2016). *Qualitative Sozialforschung* (6. Aufl). Weinheim/Basel: Beltz.
- LeDoux, J. (2007). The amygdala. *Current Biology*, 17(20), R868-74. doi: 10.1016/j.cub.2007.08.005
- Levenson, M. R., Kiehl, K. A. & Fitzpatrick, C. M. (1995). Assessing psychopathic attributes in a noninstitutionalized population. *Journal of Personality and Social Psychology*, 68(1), 151-158. doi: 10.1037//0022-3514.68.1.151
- Lewin, K. (1951). *Field Theory in Social Science*. New York: Harper.
- Liginlal, D., Sim, I. & Khansa, L. (2009). How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, 28(3-4), 215-228. doi: 10.1016/j.cose.2008.11.003
- Lilienfeld, S. O. & Andrews, B. P. (1996). Development and preliminary validation of a self-report measure of psychopathic personality traits in noncriminal populations. *Journal of Personality Assessment*, 66(3), 488-524. doi: 10.1207/s15327752jpa6603_3
- Lilienfeld, S. O., Waldman, I. D., Landfield, K., Watts, A. L., Rubenzer, S. & Faschingbauer, T. R. (2012). Fearless dominance and the U.S. presidency: implications of psychopathic

- personality traits for successful and unsuccessful political leadership. *Journal of Personality and Social Psychology*, 103(3), 489-505. doi: 10.1037/a0029392
- Lilienfeld, S.O. & Widows, M.R. (2005). *Psychopathic Personality Inventory-Revised (PPI-R): Professional Manual*. Lutz, FL: Psychological Assessment Resources.
- LinkedIn. (2025). *Unternehmensprofil Mark T. Hofmann*. Verfügbar unter: <https://de.linkedin.com/company/mark-t-hofmann>
- Lipp, W. (1987). Subkultur. In U. Ammon, N. Dittmar & K. J. Mattheier (Hrsg.), *Sociolinguistics / Soziolinguistik. Ein internationales Handbuch zur Wissenschaft von Sprache und Gesellschaft* (Bd. 1, S. 196-199). Berlin/Boston: De Gruyter. doi: 10.1515/9783110858020-037
- Lykken, D. T. (2019). Psychopathy, Sociopathy, and Antisocial Personality Disorder. In C. J. Patrick (Hrsg.), *Handbook of psychopathy*, (2. Aufl., S. 22-32). New York: The Guilford Press.
- Lykken, D. T. (1995). *The Antisocial Personalities*. Hillsdale, NJ: Lawrence Erlbaum Associates.
- Lyons, M., Houghton, E., Brewer, G. & O'Brien, F. (2022). The Dark Triad and Sexual Assertiveness Predict Sexual Coercion Differently in Men and Women. *Journal of Interpersonal Violence*, 37(7-8), NP4889-NP4904. doi: 10.1177/0886260520922346
- Machiavelli, N. (2016). *Der Fürst* (10. Aufl.). Hamburg: Nikol Verlag.
- MalwareForums. (2025). *Telegram-Kanal*. Verfügbar unter: <https://t.me/malwareforums>
- Maples, J. L., Lamkin, J. & Miller, J. D. (2014). A test of two brief measures of the dark triad: the dirty dozen and short dark triad. *Psychological Assessment*, 26(1), 326-331. doi: 10.1037/a0035084
- March, E. (2022). Psychopathy: Cybercrime and cyber abuse. In P.B. Marques, M. Paulino & L. Alho (Hrsg.), *Psychopathy and Criminal Behavior* (S. 423-444). London: Academic Press. doi: 10.1016/B978-0-12-811419-3.00015-7
- Martineau, M., Spiridon, E. & Aiken, M. (2023). A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sciences*, 3(3), 452-477. doi: 10.3390/forensicsci3030032
- Martins, R. (2017). Anonymous' Cyberwar Against ISIS and the Asymmetrical Nature of Cyber Conflicts. *Cyber Defense Review*, 2 (3), 95-105.
- Matthews, J., & Goerzen, M. (2019). Black Hat Trolling, White Hat Trolling, and Hacking the Attention Landscape. In *Companion Proceedings of the 2019 World Wide Web Conference* (S. 523-528). ACM. doi: 10.1145/3308560.3317598
- Mayring, P. (2023). *Einführung in die qualitative Sozialforschung. Eine Anleitung zum qualitativen Denken* (7. Aufl.). Weinheim/Basel: Beltz.
- McHoskey, J. W., Worzel, W. & Szyarto, C. (1998). Machiavellianism and psychopathy. *Journal of Personality and Social Psychology*, 74(1), 192-210. doi: 10.1037//0022-3514.74.1.192
- Mentzel, T. & Schröder, D. (2005). Einführung in die Kriminologie. In R. Berthel, T. Mentzel, K. Neidhardt, D. Schröder & T. Spang (Hrsg.), *Grundlagen der Kriminalistik / Kriminologie* (Lehr- und Studienbriefe Kriminalistik / Kriminologie, Band 1, S. 19-48). Hilden: Verlag Deutsche Polizeiliteratur.
- Meris Botnet. (2025). *Telegram-Kanal*. Verfügbar unter: https://t.me/meris_botnet

- Miller, J. D., Gentile, B., Wilson, L. & Campbell, W. K. (2013). Grandiose and vulnerable narcissism and the DSM-5 pathological personality trait model. *Journal of Personality Assessment*, 95(3), 284-290. doi: 10.1080/00223891.2012.685907
- Miller, J. D., Hyatt, C. S., Maples-Keller, J. L., Carter, N. T. & Lynam, D. R. (2017). Psychopathy and Machiavellianism: A Distinction Without a Difference? *Journal of Personality*, 85(4), 439-453. doi: 10.1111/jopy.12251
- Möhring, W. & Schlütz, D. (2013). Standardisierte Befragung: Grundprinzipien, Einsatz und Anwendung. In W. Möhring & D. Schlütz (Hrsg.), *Handbuch standardisierte Erhebungsverfahren in der Kommunikationswissenschaft* (S. 183-200). Wiesbaden: Springer VS. doi: 10.1007/978-3-531-18776-1_10
- Mullins-Sweatt, S. N., Glover, N. G., Derefinko, K. J., Miller, J. D. & Widiger, T. A. (2010). The search for the successful psychopath. *Journal of Research in Personality*, 44(4), 554-558. doi: 10.1016/j.jrp.2010.05.010
- Musolff, C. (2002). Täterprofile und Fallanalyse. Eine Bestandsaufnahme. In C. Musolff & J. Hoffmann (Hrsg.), *Täterprofile bei Gewaltverbrechen. Mythos, Theorie und Praxis des Profiling* (S. 1-33). Berlin/Heidelberg/New York: Springer.
- National Crime Agency (NCA). (2017). *Pathways Into Cybercrime*. Verfügbar unter: <https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file>
- Neprash, H. T., McGlave, C. C., Cross, D. A., Virnig, B. A., Puskarich, M. A., Huling, J. D., Rozenshtein, A. Z. & Nikpay, S. (2022). Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. *JAMA Health Forum*, 3(12), e224873. doi: 10.1001/jamahealthforum.2022.4873
- Nevin, A. D. (2015). *Cyber-Psychopathy: Examining the Relationship between Dark E-Personality and Online Misconduct* (Dissertation). The University of Western Ontario, Ontario. Verfügbar unter: https://www.academia.edu/14044453/Cyber_Psychopathy_Examining_the_Relationship_between_Dark_E_Personality_and_Online_Misconduct
- Nicholls, A. R., Madigan, D. J., Backhouse, S. H. & Levy, A. R. (2017). Personality traits and performance enhancing drugs: The Dark Triad and doping attitudes among competitive athletes. *Personality and Individual Differences*, 112, 113-116. doi: 10.1016/j.paid.2017.02.062
- NullBB. (2025). *Cleartnet-Hackerforum*. Verfügbar unter: <https://nulledbb.com>
- O'Boyle, E. H., Forsyth, D. R., Banks, G. C. & McDaniel, M. A. (2012). A meta-analysis of the Dark Triad and work behavior. A social exchange perspective. *The Journal of Applied Psychology*, 97(3), 557-579. doi: 10.1037/a0025679
- Otto, C. (2020). Digitale Rechtsdurchsetzung. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie. Kriminologie für das digitale Zeitalter* (S. 611-623). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-28507-4_23
- Owen, G. & Savage, N. (2016). Empirical analysis of Tor Hidden Services. *IET Information Security*, 10(3), 113-118. doi: 10.1049/iet-ifs.2015.0121
- Pabian, S., Backer, C. J. de & Vandebosch, H. (2015). Dark Triad personality traits and adolescent cyber-aggression. *Personality and Individual Differences*, 75, 41-46. doi: 10.1016/j.paid.2014.11.015
- Pastwa-Wojciechowska, B., Kaźmierczak, M. & Błażek, M. (2012). Self-esteem and styles of coping with stress versus strategies of planning in people with psychopathic

- personality disorders. *Medical Science Monitor: International Medical Journal of Experimental and Clinical Research*, 18(2), 119-124. doi: 10.12659/msm.882467
- Patrick, C. J. (2006). Back to the Future: Cleckley as a Guide to the Next Generation of Psychopathy Research. I. In C. J. Patrick (Hrsg.), *Handbook of psychopathy* (S. 605-617). New York, NY: Guilford Press.
- Patrick, C. J. (2019). Psychopathy as masked pathology. In C. J. Patrick (Hrsg.), *Handbook of psychopathy*, (2. Aufl., S. 3-21). New York: The Guilford Press.
- Patrick, C. J., Fowles, D. C. & Krueger, R. F. (2009). Triarchic conceptualization of psychopathy. Developmental origins of disinhibition, boldness, and meanness. *Development and Psychopathology*, 21(3), 913-938. doi: 10.1017/S0954579409000492
- Paulhus, D. L. (2014). Toward a Taxonomy of Dark Personalities. *Current Directions in Psychological Science*, 23(6), 421-426. doi: 10.1177/0963721414547737
- Paulhus, D. L. & Jones, D. N. (2015). Measures of Dark Personalities. In G. J. Boyle, D. H. Saklofske & G. Matthews (Hrsg.), *Measures of personality and social psychological constructs* (S. 562-594). San Diego, CA: Academic Press. doi: 10.1016/B978-0-12-386915-9.00020-6
- Paulhus, D. L. & Williams, K. M. (2002). The Dark Triad of personality. Narcissism, Machiavellianism, and psychopathy. *Journal of Research in Personality*, 36(6), 556-563. doi: 10.1016/S0092-6566(02)00505-6
- Paulhus, D. L., Neumann, C. S., & Hare, R. D. (2009). Manual for the Self-Report Psychopathy Scale. Toronto, CA: Multi-Health Systems.
- Perenc, L. (2022). Psychopathic personality disorder and cybercriminality: an outline of the issue. *Current Issues in Personality Psychology*, 10(4), 253-264. doi: 10.5114/cipp.2022.114205
- Petrides, K. V., Vernon, P. A., Schermer, J. A. & Veselka, L. (2011). Trait emotional intelligence and the dark triad traits of personality. *Twin Research and Human Genetics*, 14(1), 35-41. doi: 10.1375/twin.14.1.35
- Pitch. (2025f). *Darknet-Hackerforum*. Verfügbar unter: pitchprash4aqilfr7sbmuwve3pnkpyqlwxjbj2q5o4szcfeea6d27yd.onion/
- Plank, H. (2020). Ist der Begriff „Cyberkriminalität“ in Forschung und Praxis hinreichend konturiert und somit adäquater (Sozial-)Kontrolle zugänglich? In T. G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie. Kriminologie für das digitale Zeitalter* (S. 13-70). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-28507-4_2
- Porter, S., Birt, A. R. & Boer, D. P. (2001). Investigation of the criminal and conditional release profiles of Canadian federal offenders as a function of psychopathy and age. *Law and Human Behavior*, 25(6), 647-661. doi: 10.1023/a:1012710424821
- Porter, S., Woodworth, M., Earle, J., Drugge, J. & Boer, D. (2003). Characteristics of sexual homicides committed by psychopathic and nonpsychopathic offenders. *Law and Human Behavior*, 27(5), 459-470. doi: 10.1023/a:1025461421791
- Porter, S., Woodworth, M. T. & Black, P. J. (2019). Psychopathy and Aggression. In C. J. Patrick (Hrsg.), *Handbook of psychopathy*, (2. Aufl., S. 611-634). New York: The Guilford Press.
- Psederska, E., Yankov, G. P., Bozgunov, K., Popov, V., Vasilev, G. & Vassileva, J. (2020). Validation of the Levenson Self-Report Psychopathy Scale in Bulgarian Substance-Dependent Individuals. *Frontiers in Psychology*, 11, 1110. doi: 10.3389/fpsyg.2020.01110

- Raskin, R. & Terry, H. (1988). A principal-components analysis of the Narcissistic Personality Inventory and further evidence of its construct validity. *Journal of Personality and Social Psychology*, 54(5), 890-902. doi: 10.1037/0022-3514.54.5.890
- Raskin, R. N., & Hall, C. S. (1979). A narcissistic personality inventory. *Psychological Reports*, 45(2), 590. doi: 10.2466/pr0.1979.45.2.590
- Reddit. (2025). *Subreddit DarkWireSys*. Verfügbar unter: <https://www.reddit.com/r/DarkWireSys/>
- Rennie, L. & Shore, M. (2007). An Advanced Model of Hacking. *Security Journal*, 20(4), 236-251. doi: 10.1057/palgrave.sj.8350019
- Rheinberg, F. & Tramp, N. (2006). Anreizanalyse intensiver Nutzung von Computern in der Freizeit. *Zeitschrift für Psychologie / Journal of Psychology*, 214(2), 97-107. doi: 10.1026/0044-3409.214.2.97
- Rössler, P. & Geise, S. (2013). Standardisierte Inhaltsanalyse: Grundprinzipien, Einsatz und Anwendung. In W. Möhring & D. Schlütz (Hrsg.), *Handbuch standardisierte Erhebungsverfahren in der Kommunikationswissenschaft* (S. 269-287). Wiesbaden: Springer VS. doi: 10.1007/978-3-531-18776-1_15
- Rüdiger, T.-G. (2018). Das Broken Web: Herausforderung für die Polizeipräsenz im digitalen Raum. In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Digitale Polizeiarbeit* (S. 259-299). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-19756-8_14
- Rüdiger, T.-G. (2023). Cyberkriminologie - Kriminologische Ansätze für eine digitale Weltgesellschaft? In T.-G. Rüdiger & P. S. Bayerl (Hrsg.), *Handbuch Cyberkriminologie 1* (S. 1-35). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-35450-3_1-1
- Sarkar, S., Clark, B. S. & Deeley, Q. (2011). Differences between psychopathy and other personality disorders: evidence from neuroimaging. *Advances in Psychiatric Treatment*, 17(3), 191-200. doi: 10.1192/apt.bp.107.004747
- Schütte, N. & Blickle, G. (2017). Psychopathie im Arbeitsleben: ein Trendbericht. Psychopathie als gemeinsame Wurzel von Spitzenleistung und schädigendem Verhalten. *Wirtschaftspsychologie*, 3, 93-101.
- Schwarzinger, D. (2020). *Die Dunkle Triade der Persönlichkeit in der Personalauswahl*. Göttingen: Hogrefe.
- Selzer, N. & Oelrich, S. (2021). Saint or Satan? Moral Development and Dark Triad Influences on Cybercriminal Intent. In M. Weulen Kranenborg & R. Leukfeldt (Hrsg.), *Cybercrime in Context: The human factor in victimization, offending, and policing* (S.175-194). Cham, Schweiz: Springer. doi: 10.1007/978-3-030-60527-8_11
- Serin, R. C. & Amos, N. L. (1995). The role of psychopathy in the assessment of dangerousness. *International Journal of Law and Psychiatry*, 18(2), 231-238. doi: 10.1016/0160-2527(95)00008-6
- Shymko, V. (2025). Identifying Key Idiolect Markers in Sociolinguistic Profiling: A Scoping Review and Analytical Framework for Real-world Applications. *SAGE Open*, 15(2). doi: 10.1177/21582440251334276
- SinisterLY. (2025). *Cleanet-Hackerforum*. Verfügbar unter: <https://sinister.ly>
- Skeem, J. L. & Cooke, D. J. (2010). Is criminal behavior a central component of psychopathy? Conceptual directions for resolving the debate. *Psychological Assessment*, 22(2), 433-445. doi: 10.1037/a0008512

- Skeem, J. L., Polaschek, D. L. L., Patrick, C. J. & Lilienfeld, S. O. (2011). Psychopathic Personality: Bridging the Gap Between Scientific Evidence and Public Policy. *Psychological Science in the Public Interest*, 12(3), 95-162. doi: 10.1177/1529100611426706
- Statista. (2025a). *Anzahl der gerichtlich Verurteilten in Deutschland nach Geschlecht von 2013 bis 2023*. Verfügbar unter: <https://de.statista.com/statistik/daten/studie/1068769/umfrage/rechtskraeftig-verurteilte-personen-in-deutschland-nach-geschlecht/>
- Statista. (2025b). *Countries with the biggest share of prevented cyber attacks worldwide from September to November 2022*. Verfügbar unter: <https://www.statista.com/statistics/1372561/cyber-attack-country-targets-prevention/>
- Statista (2025c). *Estimated cost of cybercrime worldwide 2018-2029. (in trillion U.S. dollars)*. Verfügbar unter: <https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide>
- Statistisches Bundesamt. (2025a). *Bruttoinlandsprodukt (BIP)*. Verfügbar unter: <https://www.destatis.de/DE/Themen/Wirtschaft/Volkswirtschaftliche-Gesamtrechnungen-Inlandsprodukt/Tabellen/bip-bubbles.html>
- Statistisches Bundesamt. (2025b). *Definition "Aufklärungsquote"*. Verfügbar unter: <https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Glossar/aufklaerungsquote.html>
- Steffensmeier, D. & Allan, E. (1996). Gender and Crime: Toward a Gendered Theory of Female Offending. *Annual Review of Sociology*, 22(1), 459-487. doi: 10.1146/annurev.soc.22.1.459
- Stone, M. H. (2001). Serial sexual homicide: biological, psychological, and sociological aspects. *Journal of Personality Disorders*, 15(1), 1-18. doi: 10.1521/pedi.15.1.1.18646
- Stryker, C. (2011). *Epic Win for Anonymous: How 4chan's Army Conquered the Web*. New York: Overlook Press.
- Suler, J. (2004). The online disinhibition effect. *Cyberpsychology & Behavior: The Impact of the Internet, Multimedia and Virtual Reality on Behavior and Society*, 7(3), 321-326. doi: 10.1089/1094931041291295
- Sutherland, E. H. (1939). *Principles of Criminology* (3. Aufl.). Philadelphia: J.B. Lippincott.
- Taddicken, M. (2013). Online-Befragung. In W. Möhring & D. Schlütz (Hrsg.), *Handbuch standardisierte Erhebungsverfahren in der Kommunikationswissenschaft* (S. 201-217). Wiesbaden: Springer VS. doi: 10.1007/978-3-531-18776-1_11
- Tavakkoli, N., Çetin, O., Ekmekcioglu, E. & Savaş, E. (2025). From frontlines to online: examining target preferences in the Russia-Ukraine conflict. *International Journal of Information Security*, 24, 64. doi: 10.1007/s10207-025-00981-w
- Tennakoon, H. (2021). Can the 'Dark Triad' traits be a predictor of cyber hate speech? *Academia Letters*, 1965. doi: 10.20935/AL1965
- Ternes, M., Babin, C., Woodworth, A. & Stephens, S. (2019). Academic misconduct: An examination of its association with the dark triad and antisocial behavior. *Personality and Individual Differences*, 138, 75-78. doi: 10.1016/j.paid.2018.09.031
- The Tor Project. (2025). *History*. Verfügbar unter: <https://www.torproject.org/about/history/>

- Thiel, C. (2020). Liebesschwindel im Cyberspace. In T. G. Rüdiger & P. S. Bayerl (Hrsg.), *Cyberkriminologie. Kriminologie für das digitale Zeitalter* (S. 241-267). Wiesbaden: Springer VS. doi: 10.1007/978-3-658-28507-4_10
- Tidy, J. (2024). *Telegram: 'The dark web in your pocket'*. BBC. Verfügbar unter: <https://www.bbc.com/news/articles/cdey4prn3e1o>
- Udris, R. (2014). Cyberbullying among high school students in Japan: Development and validation of the Online Disinhibition Scale. *Computers in Human Behavior*, 41, 253-261. doi: 10.1016/j.chb.2014.09.036
- Vector Stall. (o.j.). *Piktogramme*. Verfügbar unter: <https://www.flaticon.com/authors/vector-stall>
- Vick, J. & Roters, F. (2003). *Account-Missbrauch im Internet. Ein Sammelverfahren mit anschließender kriminologischer Auswertung*, BKA. Verfügbar unter: <https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/Publikationsreihen/Forschungsergebnisse/2003AccountMissbrauchImInternet.html>
- Vize, C. E., Lynam, D. R., Collison, K. L. & Miller, J. D. (2018). Differences among dark triad components: A meta-analytic investigation. *Personality Disorders*, 9(2), 101-111. doi: 10.1037/per0000222
- Volkmer, S. A., Gaube, S., Raue, M. & Lerner, E. (2023). Troll story: The dark tetrad and online trolling revisited with a glance at humor. *PloS One*, 18(3), e0280271. doi: 10.1371/journal.pone.0280271
- Vortex. (2025). *Darknet-Marktplatz*. Verfügbar unter: mq7ozbnrqdj6cof3yakegs44kmo6vl3ajcyzdeya3zjtmi65jtmwqid.onion/home
- Wayback Machine. (2025a). *Archivierung Website Uni Tübingen*. Verfügbar unter: https://web.archive.org/web/20250000000000*/https://uni-tuebingen.de/
- Wayback Machine. (2025b). *Archivierung FBI Cyber Most Wanted*. Verfügbar unter: https://web.archive.org/web/20250000000000*/https://www.fbi.gov/wanted/cyber
- Wernert, M. (2021). *Internetkriminalität. Grundlagenwissen, erste Maßnahmen und polizeiliche Ermittlungen* (4. Aufl.). Stuttgart/München: Boorberg.
- West, B. T. & Blom, A. G. (2016). Explaining Interviewer Effects: A Research Synthesis. *Journal of Survey Statistics and Methodology*, 5(2), 175-211. doi: 10.1093/jssam/smw024
- Widom, C. S. (1977). A methodology for studying noninstitutionalized psychopaths. *Journal of Consulting and Clinical Psychology*, 45(4), 674-683. doi: 10.1037/0022-006X.45.4.674
- Yang, Y. & Raine, A. (2019). The Neuroanatomical Bases of Psychopathy: A Review of Brain Imaging Findings. In C. J. Patrick (Hrsg.), *Handbook of psychopathy*, (2. Aufl., S. 380-400). New York: The Guilford Press.
- ZDV Universität Tübingen (2025). *Zentrum für Datenverarbeitung (ZDV)*. Verfügbar unter: <https://uni-tuebingen.de/einrichtungen/zentrum-fuer-datenverarbeitung/aktuelles/>
- Zhang, Y., Gros, T. & Mao, E. (2021). Gender Disparity in Students' Choices of Information Technology Majors. *Business Systems Research Journal*, 12(1), 80-95. doi: 10.2478/bsrj-2021-0006²⁰

²⁰ Für die Literaturverwaltung und -organisation wurde das Programm Citavi verwendet.

Anhang

	Seite
Anhang 1: Codebuch.....	304
Anhang 2: Fragenkatalog (SoSci-Survey).....	310
Anhang 3: Stellungnahme Kujus Strafverteidigung	324
Anhang 4: SPSS-Outputs	326
Anhang 5: Erklärung zu verwendeten Hilfsmitteln und Software	342
Anhang 6: Einwilligungserklärung und Interviewleitfaden	343
Anhang 7: Kategoriensystem	347
Anhang 8: Codebogen Black Hat Hacker	348
Anhang 9: Codebogen White Hat Hacker	363

Anhang 1: Codebuch

Quantitative Inhaltsanalyse der FBI Most Wanted Hacker 2010-2024

Analyseeinheit:

Ein FBI Cyber Most Wanted Fahndungsplakat im PDF-Format.

Auswahleinheit/ Aufgreifkriterien

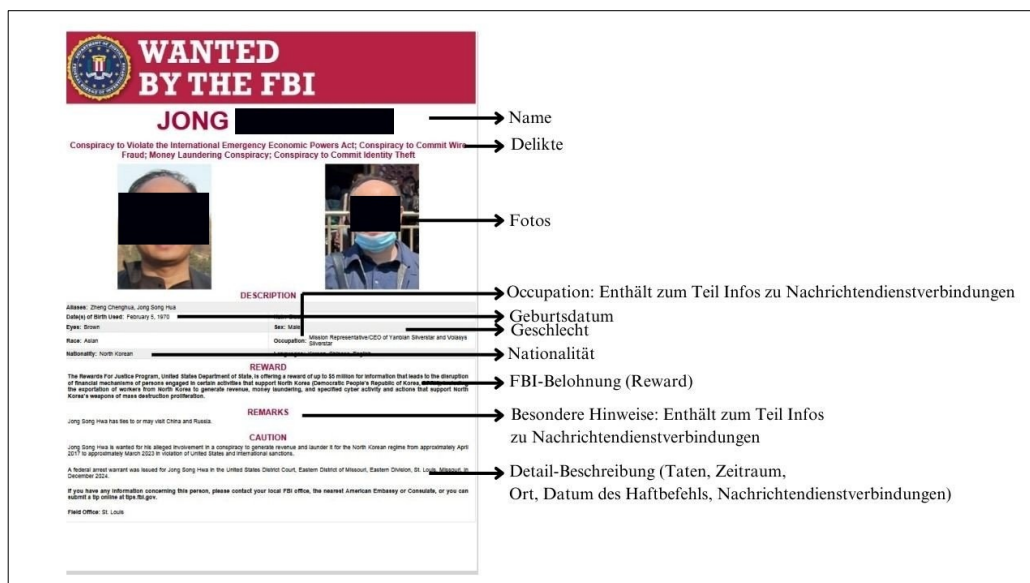
Als Untersuchungsgegenstand ausgewählt wurden lediglich diejenigen Fahndungsplakate, welche:

- (1) nach einzelnen, identifizierbaren Personen fahnden (keine Gruppenfahndungen).
- (2) nach Personen fahnden, die Black Hat Hacker sind, also *Cybercrime im engeren Sinne* begangen haben.

Material

Die Fallzahl ist $N = 145$. Ausgangsmaterial für die Codierung ist eine vorbereitete SPSS-Datei mit 145 Zeilen (Datenansicht), in der alle zu codierenden Hacker namentlich aufgelistet sind. Die Variable name_ID ist vorausgefüllt.

Ebenfalls liegen 145 Fahndungsplakate im PDF-Format vor, die Dateinamen der PDFs entsprechen der Variable „Name“. Zur Codierung ist jeweils die PDF-Datei mit dem entsprechenden Namen zu öffnen und folgende Kategorien zu codieren. Die Abbildung zeigt beispielhaft ein Fahndungsplakat und wo welche Informationen zu finden sind.



Quelle: FBI (2025a), <https://www.fbi.gov/wanted/cyber>

Anmerkung. Anonymisierung durch den Autor.

Kategorie SPSS-Variable (Skalenniveau)	Ausprägungen/ Codes/ Format/ Fehlende Werte	Codieranweisung
Name <i>name_ID</i> (nominal)	VORNAME NACHNAME - 999 = fehlender Wert	Der Name in Großbuchstaben ist bereits vorausgefüllt in der SPSS-Datei zur eindeutigen Identifikation der einzelnen Fälle.
Geschlecht <i>geschlecht</i> (nominal)	1 = männlich 2 = weiblich -999 = fehlender Wert	Geschlecht (male, female) wird vom FBI im oberen Drittel des Plakats angegeben.
Nationalität <i>nationalität</i> (nominal)	Land auf Deutsch Beispiel: Russland China -999 = fehlender Wert	Es geht darum, zu codieren, aus welchem Land die Bedrohung kommt. Nationalität wird vom FBI im oberen Drittel des Plakats genannt. In seltenen Fällen findet sich die Information zur Nationalität im Fließtext unter Details/Caution. Falls jemand offiziell im Auftrag eines Landes handelt, wird dies als Nationalität codiert. Ist jemand also z.B. Teil des russischen Militärgheimdienstes ist „Russland“ als Nationalität zu codieren, unabhängig von anderen Informationen. Begründung: Um Teil des Nachrichtendienstes oder militärischer Spezialeinheiten zu werden, setzt dies die Staatsbürgerschaft voraus.
Nachrichtendienstverbindung/ staatliche Verbindung <i>intel</i> (nominal)	1 = Ja (Hinweis vorhanden) 2 = Nein (kein Hinweis enthalten)	 Quelle: https://www.fbi.gov/wanted/cyber Es wird codiert, ob sich auf dem Plakat ein Hinweis zu einer Verbindung zu staatlichen Einheiten befindet (Militär, Regierung, Geheimdienst). Die Zugehörigkeit zu einer Militär- oder Nachrichtendiensteinheit wird meist im oberen Drittel im Bereich „Occupation“ angegeben. In anderen Fällen findet sich dieser Hinweis auch unter „Remarks“ oder geht aus dem Fließtext bei „Caution/ Details“ hervor. Auch Fotos in Uniform geben einen ersten Hinweis, reichen jedoch allein nicht aus. Sollte an einer der genannten Stellen ein eindeutiger Hinweis auf staatliche Organe, Militär oder Nachrichtendienstverbindung bestehen wird dies als „1“ codiert. Es müssen nicht zwingend direkte Mitarbeiter des Geheimdienstes oder von Militäreinheiten sein, auch andere Hinweise auf indirekte Verbindung zu staatlichen Einheiten wird als „1“ codiert. Beispiele für Nachrichtendiensteinheiten sind: • GRU (Russland) • Islamic Revolutionary Guard Corps (IRGC) (Iran) • FSB

Kategorie SPSS-Variable (Skalenniveau)	Ausprägungen/ Codes/ Format/ Fehlende Werte	Codieranweisung
		- North Korean government's Reconnaissance General Bureau (RGB) - People's Liberation Army (PLA) of the People's Republic of China (PRC) - Democratic People's Republic of Korea, DPRK APTs (Advanced Persistent Threats) sind Hackergruppen, die häufig dafür bekannt sind, staatlich unterstützt zu werden oder in enger Verbindung zu Geheimdiensten zu stehen. Auch dies wird als „1“ codiert, z.B.: APT41, APT40, APT28, APT33, APT18 Weitere staatliche Verbindungen können z.B. Mitarbeiter staatlicher „Research Center“ sein, die häufig ebenfalls in Cyber- & Wirtschaftsspionage involviert sind.
Belohnung <i>fbi_reward</i> metrisch	Zahl in USD, ohne Währungszeichen, Punkte oder Kommata: 1000000	Die ausgelobte Belohnung wird - sofern es eine gibt - mittig auf dem Plakat mit der Überschrift „reward“ in USD genannt.
Geburtsdatum <i>date_birth</i> nominal	Monat und Jahr werden im Format MM-JJJJ codiert. Beispiel: 03-2004 12-1997 Falls nur das Jahr genannt wird, Format: JJJJ -999 = keine Angabe	Geburtsdatum im Format „MM-JJJJ“ übernehmen. Es steht im oberen Drittel des Plakats im Bereich „Date(s) of Birth used“. Wenn das Geburtsdatum nicht ganz sicher ist und mehrere Daten genannt sind, die weniger als 3 Jahre auseinanderliegen (z.B. 01-1991 und 01-1993) wird der Mittelwert aus den Jahren gebildet und nur das Jahr im Format JJJJ codiert. Liegen die Daten weiter als 3 Jahre auseinander wird -999 (fehlender Wert) codiert. Nennt das FBI ein Alter (z.B. 19) statt dem Geburtsjahr, wird dies vom aktuellen Jahr (2024) abgezogen: 2024-19 = Geburtsdatum 2005
Mittlerer Tatzeitpunkt <i>mitt_tatzeitpunkt</i> nominal	Monat und Jahr im Format: MM-JJJJ Falls nur eine Jahreszahl genannt wird: JJJJ -999 = keine Angabe	In den meisten Fällen nennt das FBI im Fließtext unter „Caution/Details“ einen Tatzeitraum wie z.B.: “It is alleged that, between September of 2011 and January of 2014, (...)” Die Grundformel zur Bestimmung des mittleren Tatzeitpunkts lautet: Alle Monate des Zeitraums zählen, durch 2 teilen und dies auf den Startzeitpunkt addieren.

Kategorie SPSS-Variable (Skalenniveau)	Ausprägungen/ Codes/ Format/ Fehlende Werte	Codieranweisung
		Die genannten Monate werden voll mitgezählt, was folgende Berechnung ergibt: Zeitraum: September of 2011 bis January of 2014 4 Monate in 2011 + gesamtes Jahr 2012 und gesamtes Jahr 2013 + 1 Monat in 2014 = 29 Monate Die Hälfte von 29 Monaten sind 14,5. Es wird aufgerundet, da der 15. Monat bereits angebrochen ist. 09-2011 (Startzeitpunkt) + 15 Monate = 12-2012 Beispiel 2: 2011-2013 Es werden die vollen Jahre gezählt, wenn keine abweichenden Informationen vorhanden sind. 2011-2013 = 36 Monate. Die Hälfte sind 18 Monate. Startzeitpunkt 01-2011 + 18 Monate = 07-2012 Beispiel 3: 2010-2013 = 48 Monate. Die Hälfte sind 24 Monate. Startzeitpunkt 01-2010 + 24 Monate = 01-2012 Beispiel 4: Wird nur z.B. „since 2011“ als Tatzeitpunkt genannt ist dies als 01-2011 zu codieren. Weitere Zeitangaben und Sonderfälle und wie diese zu codieren sind: • Spring: Codieren als April: 04-JJJJ • Summer: Codieren als Juli: 07-JJJJ • Fall: Codieren als Oktober: 10-JJJJ • Winter: Codieren als Januar: 01-JJJJ • Seit 2011 (ohne Monat): 01-2011 • Until Present day = Ende Erhebungszeitraum 12-2024 — Kontexteinheit: Wenn kein genauer Tatzeitpunkt oder Monat genannt ist, es sich aber auf ein Großereignis bezieht, wie „US Election 2016“ oder „2018 Winter Olympic Games“, kann mittels Google der Monat identifiziert werden:

Kategorie SPSS-Variable (Skalenniveau)	Ausprägungen/ Codes/ Format/ Fehlende Werte	Codieranweisung
		US Wahl 2016: 11-2016 Olympische Winterspiele 2018: 02-2018 Werden innerhalb eines Fahndungsplakates mehrere Taten mit jeweils eigenen Tatzeiträumen genannt, wird nur die erstgenannte Tat codiert.
Datum Haftbefehl	Monat und Jahr im Format: MM-JJJJ Falls nur eine Jahreszahl genannt wird: JJJJ -999 = keine Angabe	In der Rubrik „Details“ werden Angaben zur Tat gemacht und meist Ort + Datum des Haftbefehls bzw. der ersten juristischen/strafrechtlichen Maßnahme. Es geht bei dieser Codierung darum, das Datum der ersten strafrechtlichen Maßnahme zu codieren, das möglichst dicht an der Tat liegt. Ziel ist es bei den Hackern, bei denen kein Tatzeitraum genannt ist, sich mittels dieses Datums der Tatzeit anzunähern. <u>Die zeitliche Nähe zur Tat ist das entscheidende Merkmal.</u> Codiert wird also <u>immer das erste genannte Datum</u>. Oft werden Urteile später geändert, revidiert, erweitert oder umgewandelt. Von Interesse ist immer nur das früheste Datum, egal um welche Art von strafrechtlicher oder juristischer Maßnahme es sich handelt. Beispiel: On January 21, 2016, a grand jury in the United States District Court, Southern District of New York, indicted (...) Code: 01-2016 <u>Weitere mögliche Formulierungen:</u> • “a federal arrest warrant was issued” • “A federal grand jury sitting in the District of Columbia returned an indictment” • “a criminal complaint was filed in the United States District Court”

Berechnung der Variable Tatalter

Bei den Fällen bei denen sowohl das Geburtsdatum als auch der (mittlere) Tatzeitpunkt codiert werden konnte, lautet die Formel:

Alter zur Tatzeit = Mittlerer Tatzeitpunkt - Geburtsdatum

Für diejenigen Fälle, bei denen kein Tatzeitpunkt codiert werden konnte (-999), aber das Datum des Haftbefehls, wird hieraus ein ungefährender Tatzeitpunkt errechnet.

Im ersten Schritt muss hierzu die Frage beantwortet werden:

Wie viele Jahre liegt das Datum des Haftbefehls durchschnittlich hinter der Tatzeit?

Hierzu werden alle Fälle herangezogen, bei denen Tatzeitpunkt und Datum des Haftbefehls codiert werden konnten.

Der Haftbefehl liegt im Durchschnitt _____ Jahre (Zahl eintragen, 1 Dezimalstelle), *SD* = _____ (Zahl eintragen) hinter dem mittleren Tatzeitpunkt.

Die Formel zur Annäherung an den Tatzeitpunkt lautet daher:

Geschätzter Tatzeitpunkt = Datum Haftbefehl - ____ Jahre

Bei den Fällen, bei denen nur Geburtsdatum und Datum des Haftbefehls codiert werden konnten, lautet die Formel:

Alter zur Tatzeit = (Datum Haftbefehl - ____ Jahre) - Geburtsdatum

Anhang 2: Fragenkatalog (SoSci-Survey)

1. Are you breaking the rules? Which category describes you (most accurately)?

☐

White Hat Hacker
(e.g. Pentester, **IT Security** Staff, Analyst, Ethical Hacker, Security Researcher)

☐

Black Hat Hacker
(ANY form of **unauthorized or criminal** hacking within last 12 months)

☐

I have **nothing** to do with any form of Coding, Hacking or Cybersecurity.

2. What is your Gender?

☐

male

☐

female

3. What is your age group?

[Please choose] ▾

4. Your Nationality (optional)

5. Highest level of academic education (until now).

- ☐ High School Diploma/ Abitur
- ☐ Bachelor's Degree (Undergraduate)
- ☐ Masters Degree (Graduate)
- ☐ Doctoral/ PhD
- ☐ Others (please specify)

6. Please indicate how much you agree with each of the following statements.

Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
				
It's not wise to tell your secrets.				
☐	☐	☐	☐	☐
I like to use clever manipulation to get my way.				
☐	☐	☐	☐	☐
Whatever it takes, you must get the important people on your side.				
☐	☐	☐	☐	☐
Avoid direct conflict with others because they may be useful in the future.				
☐	☐	☐	☐	☐
It's wise to keep track of information that you can use against people later.				
☐	☐	☐	☐	☐
You should wait for the right time to get back at people (take revenge).				
☐	☐	☐	☐	☐
There are things you should hide from other people because they don't need to know.				
☐	☐	☐	☐	☐
Make sure your plans benefit you, not others.				
☐	☐	☐	☐	☐
Most people can be manipulated.				
☐	☐	☐	☐	☐

7. Please indicate how much you agree with each of the following statements.

Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
				
People see me as a natural leader.				
☐	☐	☐	☐	☐
I hate being the center of attention.				
☐	☐	☐	☐	☐
Many group activities tend to be dull (boring) without me.				
☐	☐	☐	☐	☐
I know that I am special because everyone keeps telling me so.				
☐	☐	☐	☐	☐
I like getting to know important people.				
☐	☐	☐	☐	☐
I feel embarrassed if someone compliments me.				
☐	☐	☐	☐	☐
I have been compared to famous people.				
☐	☐	☐	☐	☐
I am an average person.				
☐	☐	☐	☐	☐
I insist on getting the respect I deserve.				
☐	☐	☐	☐	☐

8. Please indicate how much you agree with each of the following statements.

Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
				
I like to get revenge on authorities.				
☐	☐	☐	☐	☐
I avoid dangerous situations.				
☐	☐	☐	☐	☐
Payback (revenge) needs to be quick and nasty.				
☐	☐	☐	☐	☐
People often say I'm out of control.				
☐	☐	☐	☐	☐
It's true that I can be mean to others.				
☐	☐	☐	☐	☐
People who mess with me always regret it.				
☐	☐	☐	☐	☐
I have never gotten into trouble with the law.				
☐	☐	☐	☐	☐
I enjoy having sex with people I hardly know.				
☐	☐	☐	☐	☐
I'll say anything to get what I want.				
☐	☐	☐	☐	☐

9. How did you primarily learn your hacking skills?

Multiple answers possible.

- ☐ Self-study (Books, Blogs, Tutorials, YouTube)
- ☐ Hacker Communities (Forums, Events, Darknet, 4chan, Discord, Telegram)
- ☐ Mentor
- ☐ Hands-On Challenges (CTFs, Bug Bounties, Hackathons)
- ☐ Formal Education (University, Courses, Workshops)
- ☐ Others (Please Specify)

10. Did you already use AI-Tools for Hacking or Social Engineering purposes?

(e.g. WormGPT, Deepseek, ChatGPT)

- ☐ No
- ☐ Yes (Please Specify)

11. Generally I prefer the following type of attack:

- ☐ Social Engineering (Phishing, Manipulation, Human Error)
- ☐ Technical Hacks without Human Error (Exploits, DDoS, Zero Days, Brute Force)

12. Please check all motives, that describe your motivation for hacking.

You can choose multiple answers.

- ☐ Financial interests (money)
- ☐ I enjoy the challenge/ technical problem solving/test my own skills.
- ☐ Peer-recognition in hacking culture/ Status
- ☐ Feeling of power
- ☐ Feeling of addiction
- ☐ I enjoy the „Thrill“/ adrenaline.
- ☐ I reject authorities/ it's a form of rebellion.
- ☐ I hack to bring about political or social change.
- ☐ I hack purely for fun, entertainment, trolling.
- ☐ Frustration/ Revenge
- ☐ Others (Please Specify)

13. Please rate the following statements based on your personal opinion.

Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
If people have weak passwords, it's their own fault if they get hacked.				
☐	☐	☐	☐	☐
I would stream movies illegally.				
☐	☐	☐	☐	☐
I would sneak into a movie theater without paying.				
☐	☐	☐	☐	☐
I would hack someones bank account.				
☐	☐	☐	☐	☐
I would steal somesones wallet in real life.				
☐	☐	☐	☐	☐
I would hack companies for profit.				
☐	☐	☐	☐	☐
I would steal from companies in real life.				
☐	☐	☐	☐	☐
The police are incompetent when it comes to handling Cybercrime.				
☐	☐	☐	☐	☐
I believe there is a very low chance of being caught when engaging in illegal hacking activities.				
☐	☐	☐	☐	☐

14. Any remarks/ comments? (optional)

You are 80% done. These are the last but very important questions.

15. Please indicate the degree to which you agree or disagree with each statement.

	Strongly Disagree	Disagree Somewhat	Agree Somewhat	Agree Strongly
Success is based on survival of the fittest; I am not concerned about the losers.	☐	☐	☐	☐
For me, what's right is whatever I can get away with.	☐	☐	☐	☐
In today's world, I feel justified in doing anything I can get away with to succeed.	☐	☐	☐	☐
My main purpose in life is getting as many goodies as I can.	☐	☐	☐	☐
Making a lot of money is my most important goal.	☐	☐	☐	☐
I let others worry about higher values; my main concern is with the bottom line.	☐	☐	☐	☐
People who are stupid enough to get ripped off usually deserve it.	☐	☐	☐	☐
Looking out for myself is my top priority.	☐	☐	☐	☐
I tell other people what they want to hear so that they will do what I want them to do.	☐	☐	☐	☐
I would be upset if my success came at someone else's expense.	☐	☐	☐	☐
I often admire a really clever scam.	☐	☐	☐	☐

I make a point of trying not to hurt others in pursuit of my goals.

☐☐☐☐

I enjoy manipulating other people's feelings.

☐☐☐☐

I feel bad if my words or actions cause someone else to feel emotional pain.

☐☐☐☐

Even if I were trying very hard to sell something, I wouldn't lie about it.

☐☐☐☐

Cheating is not justified because it is unfair to others.

☐☐☐☐

16. The last question. Please read the last 10 statements and indicate how much you agree.

	Strongly Disagree	Disagree Somewhat	Agree Somewhat	Agree Strongly
I find myself in the same kinds of trouble, time after time.	☐	☐	☐	☐
I am often bored.	☐	☐	☐	☐
I find that I am able to pursue one goal for a long time.	☐	☐	☐	☐
I don't plan anything very far in advance.	☐	☐	☐	☐
I quickly lose interest in tasks I start.	☐	☐	☐	☐
Most of my problems are due to the fact that other people just don't understand me.	☐	☐	☐	☐
Before I do anything, I carefully consider the possible consequences.	☐	☐	☐	☐
I have been in a lot of shouting matches with other people.	☐	☐	☐	☐
When I get frustrated, I often "let off steam" by blowing my top.	☐	☐	☐	☐
Love is overrated.	☐	☐	☐	☐

=== Thank you for completing this questionnaire! ===

Here are your results:

Dark Trait	Your Score (on a Scale 1-5)	Average Score (Non-Hackers)
Psychopathy	⇒ psycho ⇐	2.4
Machiavellianism	⇒ mach ⇐	3.1
Narcissism	⇒ narc ⇐	2.8

Important Note:

The scale used in this study to measure Psychopathy, Narcissism, and Machiavellianism aims to capture subclinical expressions of these personality traits and does not constitute a diagnosis. The results represent merely a snapshot of certain tendencies in your personality and should not be interpreted as a medical or psychological diagnosis. If you have concerns about your mental health or wish to obtain a professional diagnosis, we recommend consulting a qualified psychologist or psychiatrist.

Explanation of Traits:

Narcissism:

Narcissism refers to an exaggerated sense of self-importance and a strong need for admiration and validation from others. Individuals with high levels of narcissism tend to view themselves as unique or special and expect others to recognize this. A common feature is a lack of empathy for others and a tendency to prioritize their own needs above those of others.

Psychopathy:

Psychopathy is characterized by a general lack of empathy, guilt, or remorse. People with psychopathic tendencies often engage in impulsive and risky behaviors without concern for the consequences. They tend to be manipulative, cold, and unemotional.

Machiavellianism:

Machiavellianism refers to manipulative and opportunistic behavior, where one's goals are pursued at the expense of others. Individuals high in Machiavellianism often manipulate others, avoid conflicts when it benefits them, and place their own interests above others. Their behavior is often driven by a strategic, long-

term perspective.

Note:

The traits mentioned above are part of the "Dark Triad" of personality and may appear in varying degrees in different individuals. It is important to emphasize that these traits are not necessarily pathological, and many people may exhibit some degree of these traits without developing a personality disorder.

Questions? Contact: cyberpsych.study@protonmail.com

Mark Hofmann, 2025

Anhang 3: Stellungnahme Kujus Strafverteidigung



KUJUS Strafverteidigung • Pfaffendorfer Str. 25 • 04105 Leipzig

Herr
Mark Thorben Hofmann



Tommy Kujus
Rechtsanwalt
Fachanwalt für Strafrecht
Pfaffendorfer Str. 25
04105 Leipzig

tel 0341 - 978 56 290
mail info@kujus-strafverteidigung.de
web kujus-strafverteidigung.de

Unser Zeichen: **271/25**

Leipzig, den 19.09.2025

Mark Thorben Hofmann
Ihr Zeichen:

Sehr geehrter Herr Hofmann,

die Nutzung des Darknets bewegt sich in einem Spannungsfeld zwischen legitimer Anonymität und strafrechtlichen Risiken. Doch was ist im Darknet straflos und was schon strafbar?

Das hartnäckige Missverständnis, schon das Betreten des Darknets sei strafbar, ist nicht zutreffend. Maßgeblich für eine mögliche Strafbarkeit ist nicht der Ort oder die Technik, sondern das konkrete Verhalten. Das Strafrecht kennt keinen eigenständigen Tatbestand „Darknet“. Wer Anonymität sucht oder geschützt kommunizieren möchte, kann hierfür grundsätzlich Tor und vergleichbare Anonymisierungsdienste ebenso nutzen wie Seiten im sog. „Darknet“ aufrufen. Das bloße Aufrufen von .onion-Adressen, das Lesen von Foren oder der Betrieb rechtmäßiger, eigener Angebote bewegt sich im zulässigen Bereich. Auch Recherchen zu wissenschaftlichen, journalistischen oder forensischen Zwecken sind möglich, solange auf frei zugängliche Informationen zurückgegriffen wird und keine Zugangssperren überwunden werden.



KUJUS Strafverteidigung
Pfaffendorfer Str. 25, 04015 Leipzig
Steuer-Nr.: [REDACTED]

Deutsche Kreditbank



Seite 1 von 2

Die zulässige Nutzung setzt jedoch klare Selbstbeschränkungen voraus. Die reine Informationsbeschaffung ist straflos. Dies schließt insbesondere das Erstellen von Accounts in Foren und Portalen ein. Auch das Anmelden in Foren und das Lesen und Erstellen von Beiträgen ist *per se* nicht strafbar. Eine Strafbarkeit liegt erst dann vor, wenn unbefugt fremde Passwörter und Daten ausgelesen, rechtswidrig erlangte Informationen angekauft oder weitergegeben oder verbotenen Inhalte heruntergeladen oder gespeichert werden. Gleiches gilt für scheinbare „Research“-Handlungen, die in Wahrheit die Teilnahme an kriminellen Aktivitäten sind – etwa Testkäufe von Waffen oder Drogen. Wer seriös forscht, trennt strikt Beobachtung von Teilnahme, arbeitet mit wirksamen Einwilligungen, protokolliert Auftrag und Umfang und vermeidet jede Speicherung illegaler Inhalte.

Die rechtliche Linie zur Strafbarkeit im Darknet lässt sich deshalb wie folgt ziehen: Das Darknet als Raum ist nicht verboten. Zulässig bleiben Anonymität, verschlüsselte Kommunikation, das Lesen und Bereitstellen legaler Inhalte sowie wissenschaftliche und journalistische Recherche. Die Strafbarkeit beginnt dort, wo Straftatbestände verletzt werden – etwa durch unbefugte Zugriffe, den Umgang mit rechtswidrig erlangten Daten, das Abrufen verbotener Inhalte oder die Beteiligung an illegalen Geschäften.

Es gilt daher: Nicht das Betreten des Darknets ist strafbar, sondern das konkrete Verhalten im Darknet.

Mit freundlichen Grüßen

Tommy Kujus
Rechtsanwalt
Fachanwalt für Strafrecht



Anhang 4: SPSS-Outputs

a. Reliabilitätskoeffizienten aller verwendeten und gebildeten Skalen

(Sub)Skala	Cronbachs Alpha	Anzahl der Items
Psychopathie (SD3)	0.73	9
Narzissmus (SD3)	0.65	9
Machiavellismus (SD3)	0.78	9
Primäre Psychopathie (LSRP)	0.88	16
Sekundäre Psychopathie (LSRP)	0.64	10
LSRP-Gesamtskala	0.86	26
Online-Skrupellosigkeit	0.66	3
Offline-Skrupellosigkeit	0.77	3
Entdeckungswahrscheinlichkeit	0.57	2

b. t-Tests für unabhängige Stichproben SD3-Scores

Gruppenstatistiken

	Hacker Label	N	Mittelwert	Std.- Abweichung	Standardfehl- er des Mittelwertes
SD3_PSYCH_Score	Black Hat Hacker	334	3,0995	,72073	,03944
	White Hat Hacker	851	2,6220	,65336	,02240
SD3_MACH_Score	Black Hat Hacker	334	4,1008	,60986	,03337
	White Hat Hacker	851	3,7150	,64486	,02211
SD3_NARC_Score	Black Hat Hacker	334	3,0506	,62721	,03432
	White Hat Hacker	851	2,9570	,60229	,02065

Test bei unabhängigen Stichproben

		Levene-Test der Varianzgleichheit		t-Test für die Mittelwertgleichheit							
		F	Sig.	T	df	Signifikanz		Mittlere Differenz	Differenz für Standardfehler	95% Konfidenzintervall der Differenz	
						Einseitiges p	Zweiseitiges p			Unterer Wert	Oberer Wert
SD3_PSYCH_Score	Varianzen sind gleich	4,575	,033	10,987	1183	<,001	<,001	,47745	,04346	,39220	,56271
	Varianzen sind nicht gleich			10,528	559,639	<,001	<,001	,47745	,04535	,38837	,56654
SD3_MACH_Score	Varianzen sind gleich	2,482	,115	9,407	1183	<,001	<,001	,38582	,04101	,30535	,46629
	Varianzen sind nicht gleich			9,639	641,020	<,001	<,001	,38582	,04003	,30722	,46442
SD3_NARC_Score	Varianzen sind gleich	,942	,332	2,377	1183	,009	,018	,09352	,03935	,01632	,17072
	Varianzen sind nicht gleich			2,335	587,509	,010	,020	,09352	,04005	,01486	,17218

Effektgrößen bei unabhängigen Stichproben

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
SD3_PSYCH_Score	Cohen's d	,67301	,709	,580	,839
	Hedges' Korrektur	,67343	,709	,579	,838
	Glass' Delta	,65336	,731	,599	,862
SD3_MACH_Score	Cohen's d	,63521	,607	,478	,736
	Hedges' Korrektur	,63561	,607	,478	,736
	Glass' Delta	,64486	,598	,468	,728
SD3_NARC_Score	Cohen's d	,60941	,153	,027	,280
	Hedges' Korrektur	,60980	,153	,027	,280
	Glass' Delta	,60229	,155	,028	,282

c. t-Tests für unabhängige Stichproben LSRP-Scores

Gruppenstatistiken

	Hacker Label	N	Mittelwert	Std.- Abweichung	Standardfehl er des Mittelwertes
LSRP_Gesamtscore	Black Hat Hacker	258	2,5468	,46152	,02811
	White Hat Hacker	639	2,2339	,42057	,01664
LSRP_Primary_Psychopathy	Black Hat Hacker	258	2,6579	,61626	,03837
	White Hat Hacker	639	2,1928	,56074	,02218
LSRP_Secodary_Psychopathy	Black Hat Hacker	258	2,4353	,50711	,03157
	White Hat Hacker	639	2,2750	,46366	,01834

Test auf Homogenität der Varianzen

		Levene-Test der Varianzgleichheit	
		F	Sig.
LSRP_Gesamtscore	Varianzen sind gleich	1,877	,171
LSRP_Primary_Psychopathy	Varianzen sind gleich	2,576	,109
LSRP_Secodary_Psychopathy	Varianzen sind gleich	1,072	,301

Test bei unabhängigen Stichproben

		t-Test für die Mittelwertgleichheit							
		Signifikanz				Mittlere Differenz	Differenz für Standardfehler	95% Konfidenzintervall der Differenz	
		T	df	Einseitiges p	Zweiseitiges p			Unterer Wert	Oberer Wert
LSRP_Gesamtscore	Varianzen sind gleich	9,867	895	<,001	<,001	,31274	,03169	,25053	,37494
	Varianzen sind nicht gleich	9,574	446,520	<,001	<,001	,31274	,03267	,24854	,37693
LSRP_Primary_Psychopathy	Varianzen sind gleich	10,925	895	<,001	<,001	,46516	,04258	,38160	,54873
	Varianzen sind nicht gleich	10,496	437,832	<,001	<,001	,46516	,04432	,37806	,55227
LSRP_Secodary_Psychopathy	Varianzen sind gleich	4,561	895	<,001	<,001	,16031	,03515	,09132	,22930
	Varianzen sind nicht gleich	4,391	439,802	<,001	<,001	,16031	,03651	,08855	,23207

Effektgrößen bei unabhängigen Stichproben

		Standardisier er ^a	Punktschätzu ng	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
LSRP_Gesamtscore	Cohen's d	,42969	,728	,579	,876
	Hedges' Korrektur	,43005	,727	,579	,875
	Glass' Delta	,42057	,744	,593	,894
LSRP_Primary_Psychop athy	Cohen's d	,57723	,806	,656	,955
	Hedges' Korrektur	,57772	,805	,656	,954
	Glass' Delta	,56074	,830	,678	,981
LSRP_Secodary_Psychop athy	Cohen's d	,47654	,336	,191	,482
	Hedges' Korrektur	,47694	,336	,191	,481
	Glass' Delta	,46366	,346	,200	,491

d. t-Tests für unabhängige Stichproben Entdeckungswahrscheinlichkeit und Schuldumkehr

Gruppenstatistiken

	Hacker Label	N	Mittelwert	Std.- Abweichung	Standardfehl- er des Mittelwertes
Entdeckungs- wahrscheinlichkeit	Black Hat Hacker	321	3,7103	1,03389	,05771
	White Hat Hacker	834	3,3225	,97738	,03384
Opfer selbst schuld	Black Hat Hacker	321	4,02	1,201	,067
	White Hat Hacker	834	3,76	1,226	,042

Test bei unabhängigen Stichproben

		Levene-Test der Varianzgleichheit		t-Test für die Mittelwertgleichheit							
		F	Sig.	T	df	Signifikanz		Mittlere Differenz	Differenz für Standardfehler	95% Konfidenzintervall der Differenz	
						Einseitiges p	Zweiseitiges p			Unterer Wert	Oberer Wert
Entdeckungswahrscheinlichkeit	Varianzen sind gleich	3,612	,058	5,942	1153	<,001	<,001	,38774	,06525	,25972	,51576
	Varianzen sind nicht gleich			5,798	552,870	<,001	<,001	,38774	,06690	,25633	,51914
Opfer selbst schuld	Varianzen sind gleich	,996	,319	3,259	1153	<,001	,001	,261	,080	,104	,418
	Varianzen sind nicht gleich			3,288	591,211	<,001	,001	,261	,079	,105	,417

Effektgrößen bei unabhängigen Stichproben

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
Entdeckungswahrscheinlichkeit	Cohen's d	,99338	,390	,261	,520
	Hedges' Korrektur	,99403	,390	,260	,520
	Glass' Delta	,97738	,397	,266	,527
Opfer selbst schuld	Cohen's d	1,219	,214	,085	,343
	Hedges' Korrektur	1,220	,214	,085	,343
	Glass' Delta	1,226	,213	,084	,342

e. Binäre Logistische Regression

Zusammenfassung der Fallverarbeitung

Ungewichtete Fälle ^a		N	Prozent
Ausgewählte Fälle	Einbezogen in Analyse	1185	100,0
	Fehlende Fälle	0	,0
	Gesamt	1185	100,0
Nicht ausgewählte Fälle		0	,0
Gesamt		1185	100,0

Codierung abhängiger Variablen

Ursprünglicher Wert	Interner Wert
,00	0
1,00	1

Block 0: Anfangsblock

Klassifizierungstabelle^{a,b}

		Vorhergesagt		
		hackerlabel_reversed		Prozentsatz der Richtigen
		,00	1,00	
Schritt 0	Beobachtet			
	hackerlabel_reversed			
		,00	1,00	
		851	0	100,0
		1,00	0	,0
Gesamtprozentsatz				71,8

Variablen in der Gleichung

		RegressionskoeffizientB	Standardfehler	Wald	df	Sig.	Exp(B)
Schritt 0	Konstante	-,935	,065	209,813	1	<,001	,392

Variablen nicht in der Gleichung

			Wert	df	Sig.
Schritt 0	Variablen	SD3_PSYCH_Score	109,728	1	<,001
		SD3_MACH_Score	82,472	1	<,001
		SD3_NARC_Score	5,632	1	,018
	Gesamtstatistik		133,005	3	<,001

Block 1 = Einschluss*Omnibus-Tests der Modellkoeffizienten*

		Chi-Quadrat	df	Sig.
Schritt 1	Schritt	141,373	3	<,001
	Block	141,373	3	<,001
	Modell	141,373	3	<,001

Modellzusammenfassung

Schritt	-2 Log-Likelihood	Cox & Snell R-Quadrat	Nagelkerkes R-Quadrat
1	1268,061 ^a	,112	,162

Klassifizierungstabelle^a

		Vorhergesagt		
		hackerlabel_reversed		Prozentsatz der Richtigen
	Beobachtet	,00	1,00	
Schritt 1	hackerlabel_reversed	,00	802	49
		1,00	255	79
Gesamtprozentsatz				74,3

^a. Der Trennwert lautet ,500

Variablen in der Gleichung

		Regressionskoeffizient B	Standardfehler	Wald	df	Sig.	Exp(B)
Schritt 1 ^a	SD3_PSYCH_Score	,825	,120	47,382	1	<,001	2,282
	SD3_MACH_Score	,675	,134	25,284	1	<,001	1,963
	SD3_NARC_Score	-,272	,123	4,925	1	,026	,762
	Konstante	-5,115	,528	93,934	1	<,001	,006

^a. In Schritt 1 eingegebene Variablen: SD3_PSYCH_Score, SD3_MACH_Score, SD3_NARC_Score.

f. One-Sample t-Test, Black Hat Hacker SD3-PSYCH vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 2.18							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
SD3_PSYCH_Score	23,315	333	<,001	<,001	,91947	,8419	,9970

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
SD3_PSYCH_Score	Cohen's d	,72073	1,276	1,131	1,420
	Hedges' Korrektur	,72236	1,273	1,128	1,416

g. One-Sample t-Test, White Hat Hacker SD3-PSYCH vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 2.18							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
SD3_PSYCH_Score	19,736	850	<,001	<,001	,44201	,3981	,4860

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
SD3_PSYCH_Score	Cohen's d	,65336	,677	,602	,751
	Hedges' Korrektur	,65394	,676	,601	,750

h. One-Sample t-Test, Black Hat Hacker SD3-MACH vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 3.15							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
SD3_MACH_Score	28,492	333	<,001	<,001	,95080	,8852	1,0164

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
SD3_MACH_Score	Cohen's d	,60986	1,559	1,399	1,718
	Hedges' Korrektur	,61124	1,556	1,396	1,714

i. One-Sample t-Test, White Hat Hacker SD3-MACH vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 3.15							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
SD3_MACH_Score	25,558	850	<,001	<,001	,56498	,5216	,6084

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
SD3_MACH_Score	Cohen's d	,64486	,876	,797	,955
	Hedges' Korrektur	,64543	,875	,796	,954

j. One-Sample t-Test, Black Hat Hacker SD3-NARC vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 2.82							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
SD3_NARC_Score	6,718	333	<,001	<,001	,23057	,1631	,2981

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
SD3_NARC_Score	Cohen's d	,62721	,368	,257	,478
	Hedges' Korrektur	,62862	,367	,256	,477

k. One-Sample t-Test, White Hat Hacker SD3-NARC vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 2.82							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
SD3_NARC_Score	6,638	850	<,001	<,001	,13704	,0965	,1776

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
SD3_NARC_Score	Cohen's d	,60229	,228	,159	,296
	Hedges' Korrektur	,60283	,227	,159	,295

I. One-Sample t-Test, Black Hat Hacker Primäre Psychopahie vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 32.99							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
LSRP_Primary_Sum	15,536	257	<,001	<,001	9,53713	8,3283	10,7480

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
LSRP_Primary_Sum	Cohen's d	9,86017	,967	,819	1,114
	Hedges' Korrektur	9,88906	,964	,816	1,111

m. One-Sample t-Test, White Hat Hacker Primäre Psychopahie vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 32.99							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
LSRP_Primary_Sum	5,901	638	<,001	<,001	2,09451	1,3976	2,7915

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
LSRP_Primary_Sum	Cohen's d	8,97187	,233	,155	,312
	Hedges' Korrektur	8,98243	,233	,155	,312

n. One-Sample t-Test, Black Hat Hacker Sekundäre Psychopahie vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 21.68							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
LSRP_Secondary_Sum	8,466	257	<,001	<,001	2,67271	2,0510	3,2944

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
LSRP_Secondary_Sum	Cohen's d	5,07105	,527	,396	,657
	Hedges' Korrektur	5,08591	,526	,395	,655

o. One-Sample t-Test, White Hat Hacker Sekundäre Psychopahie vs. Allgemeinbevölkerung

Test bei einer Stichprobe

Testwert = 21.68							
	T	df	Signifikanz		Mittlere Differenz	95% Konfidenzintervall der Differenz	
			Einseitiges p	Zweiseitiges p		Unterer Wert	Oberer Wert
LSRP_Secondary_Sum	5,831	638	<,001	<,001	1,06961	,7094	1,4298

Effektgrößen bei einer Stichprobe

		Standardisierter ^a	Punktschätzung	95% Konfidenzintervall	
				Unterer Wert	Oberer Wert
LSRP_Secondary_Sum	Cohen's d	4,63663	,231	,152	,309
	Hedges' Korrektur	4,64209	,230	,152	,309

p. Korrelationen Dunkle Triade (SD3) und Hacking-Motive

Korrelationen

		SD3_PSYCH_Score	SD3_MACH_Score	SD3_NARC_Score	Motives: Financial Interests (money)	Motives: I enjoy the challenge/ technical problem solving/test my own skills.	Motives: Peer-recognition in hacking culture/ Status	Motives: Feeling of power	Motives: Feeling of addiction	Motives: I enjoy the Thrill/ adrenaline.	Motives: I reject authorities/ it's a form of rebellion.	Motives: I hack to bring about political or social change.	Motives: I hack purely for fun, entertainment -trolling.	Motives: Frustration/ Revenge
SD3_PSYCH_Score	Pearson-Korrelation	1	.507**	.339*	.263*	-.065	.089	.264*	.239*	.260*	.228*	.085	.022	.209*
	Sig. (2-seitig)		<.001	<.001	<.001	.243	.111	<.001	<.001	<.001	<.001	.129	.698	<.001
	N	1185	1185	1185	321	321	321	321	321	321	321	321	321	321
SD3_MACH_Score	Pearson-Korrelation	.507**	1	.312**	.170*	.040	.073	.226*	.183*	.207*	.084	.083	.070	.202*
	Sig. (2-seitig)	<.001		<.001	.002	.477	.199	<.001	<.001	<.001	.134	.140	.214	<.001
	N	1185	1185	1185	321	321	321	321	321	321	321	321	321	321
SD3_NARC_Score	Pearson-Korrelation	.339*	.312**	1	.218*	-.037	.051	.236*	.095	.134*	.043	.048	-.019	.087
	Sig. (2-seitig)	<.001	<.001		<.001	.506	.365	<.001	.089	.017	.448	.390	.732	.120
	N	1185	1185	1185	321	321	321	321	321	321	321	321	321	321
Motives: Financial Interests (money)	Pearson-Korrelation	.263*	.170*	.218*	1	-.069	.046	.208*	.169*	.083	.127*	.087	-.116*	-.002
	Sig. (2-seitig)	<.001	.002	<.001		.217	.424	<.001	.002	.139	.023	.119	.033	.978
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: I enjoy the challenge/ technical problem solving/test my own skills.	Pearson-Korrelation	-.065	.040	-.037	-.069	1	.107	.046	.085	.186*	.056	-.029	.144*	.022
	Sig. (2-seitig)	.243	.477	.506	.217		.055	.415	.128	<.001	.321	.808	.010	.691
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: Peer-recognition in hacking culture/ Status	Pearson-Korrelation	.089	.073	.051	.046	.107	1	.305*	.232*	.155*	.175*	.162*	.077	.109
	Sig. (2-seitig)	.111	.189	.365	.424	.055		<.001	<.001	.005	.002	.004	.170	.051
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: Feeling of power	Pearson-Korrelation	.264*	.226*	.236*	.208*	.046	.305*	1	.461*	.400*	.241*	.063	.095	.147*
	Sig. (2-seitig)	<.001	<.001	<.001	<.001	.415	<.001		<.001	<.001	<.001	.259	.090	.008
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: Feeling of addiction	Pearson-Korrelation	.239*	.183*	.095	.169*	.085	.232*	.461*	1	.404*	.184*	.062	.099	.134*
	Sig. (2-seitig)	<.001	<.001	.089	.002	.128	<.001	<.001		<.001	<.001	.268	.077	.016
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: I enjoy the Thrill/ adrenaline.	Pearson-Korrelation	.260*	.207*	.134*	.083	.186*	.155*	.400*	.404*	1	.119	.041	.198*	.138*
	Sig. (2-seitig)	<.001	<.001	.017	.139	<.001	.005	<.001	<.001		.034	.459	<.001	.013
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: I reject authorities/ it's a form of rebellion.	Pearson-Korrelation	.229*	.084	.043	.127*	.058	.175*	.241*	.164*	.119*	1	.397*	-.042	.171*
	Sig. (2-seitig)	<.001	.134	.448	.023	.321	.002	<.001	<.001	.034		<.001	.452	.002
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: I hack to bring about political or social change.	Pearson-Korrelation	.085	.083	.048	.087	-.029	.162*	.063	.062	.041	.397*	1	-.111*	.231*
	Sig. (2-seitig)	.129	.140	.390	.119	.608	.004	.259	.268	.459	<.001		.046	<.001
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: I hack purely for fun, entertainment, trolling.	Pearson-Korrelation	.022	.070	-.019	-.116*	.144*	.077	.095	.099	.198*	-.042	-.111*	1	.003
	Sig. (2-seitig)	.698	.214	.732	.033	.010	.170	.090	.077	<.001	.452	.046		.953
	N	321	321	321	321	321	321	321	321	321	321	321	321	321
Motives: Frustration/ Revenge	Pearson-Korrelation	.209*	.202*	.087	-.002	.022	.109	.147*	.134*	.138*	.171*	.231*	.003	1
	Sig. (2-seitig)	<.001	<.001	.120	.978	.691	.051	.008	.016	.013	.002	<.001	.953	
	N	321	321	321	321	321	321	321	321	321	321	321	321	321

** Die Korrelation ist auf dem Niveau von 0.01 (2-seitig) signifikant.

* Die Korrelation ist auf dem Niveau von 0.05 (2-seitig) signifikant.

q. Korrelationen Dunkle Triade (SD3) und Angriffsart (Modus Operandi)

Korrelationen

		Tyoe_of_Attack_reverse	SD3_PSYCH_Score	SD3_MACH_Score	SD3_NARC_Score	LSRP_Primary_Sum	LSRP_Secondary_Sum
Tyoe_of_Attack_reverse	Pearson-Korrelation	1	,167**	,209**	,098	,215**	,104
	Sig. (2-seitig)		,002	<,001	,074	<,001	,094
	N	332	332	332	332	263	258
SD3_PSYCH_Score	Pearson-Korrelation	,167**	1	,429**	,359**	,555**	,352**
	Sig. (2-seitig)	,002		<,001	<,001	<,001	<,001
	N	332	334	334	334	263	258
SD3_MACH_Score	Pearson-Korrelation	,209**	,429**	1	,284**	,537**	,185**
	Sig. (2-seitig)	<,001	<,001		<,001	<,001	,003
	N	332	334	334	334	263	258
SD3_NARC_Score	Pearson-Korrelation	,098	,359**	,284**	1	,370**	,080
	Sig. (2-seitig)	,074	<,001	<,001		<,001	,199
	N	332	334	334	334	263	258
LSRP_Primary_Sum	Pearson-Korrelation	,215**	,555**	,537**	,370**	1	,286**
	Sig. (2-seitig)	<,001	<,001	<,001	<,001		<,001
	N	263	263	263	263	263	258
LSRP_Secondary_Sum	Pearson-Korrelation	,104	,352**	,185**	,080	,286**	1
	Sig. (2-seitig)	,094	<,001	,003	,199	<,001	
	N	258	258	258	258	258	258

**·Die Korrelation ist auf dem Niveau von 0,01 (2-seitig) signifikant.

r. Korrelationen Black Hat/ White Hat und Dunkle Triade

(1 = Black Hat, 2 = White Hat)

Korrelationen

		SD3_PSYCH_Score	SD3_MACH_Score	SD3_NARC_Score	Hacker Label
SD3_PSYCH_Score	Pearson-Korrelation	1	,507**	,339**	-,304*
	Sig. (2-seitig)		<,001	<,001	<,001
	N	1185	1185	1185	1185
SD3_MACH_Score	Pearson-Korrelation	,507**	1	,312**	-,264*
	Sig. (2-seitig)	<,001		<,001	<,001
	N	1185	1185	1185	1185
SD3_NARC_Score	Pearson-Korrelation	,339**	,312**	1	-,069
	Sig. (2-seitig)	<,001	<,001		,018
	N	1185	1185	1185	1185
Hacker Label	Pearson-Korrelation	-,304*	-,264*	-,069	1
	Sig. (2-seitig)	<,001	<,001	,018	
	N	1185	1185	1185	1185

**·Die Korrelation ist auf dem Niveau von 0,01 (2-seitig) signifikant.

*·Die Korrelation ist auf dem Niveau von 0,05 (2-seitig) signifikant.

s. **t-Test bei abhängigen Stichproben: Primäre vs. Sekundäre Psychopathie bei Black Hat Hackern**

Statistik bei gepaarten Stichproben

		Mittelwert	N	Std.- Abweichung	Standardfehl er des Mittelwertes
Paaren 1	LSRP_Primary_Psychopathy	2,6579	258	,61626	,03837
	LSRP_Secodary_Psychopathy	2,4353	258	,50711	,03157

Test bei gepaarten Stichproben

		Gepaarte Differenzen					Signifikanz			
		Mittelwert	Std.- Abweichung	Standardfehl er des Mittelwertes	95% Konfidenzintervall der Differenz		T	df	Einseitiges p	Zweiseitiges p
					Unterer Wert	Oberer Wert				
Paaren 1	LSRP_Primary_Psychop athy - LSRP_Secodary_Psychop athy	,22267	,67704	,04215	,13967	,30568	5,283	257	<,001	<,001

Effektgrößen bei Stichproben mit paarigen Werten

			Standardisier er ^a	Punktschätzu ng	95% Konfidenzintervall	
					Unterer Wert	Oberer Wert
Paaren 1	LSRP_Primary_Psychop athy - LSRP_Secodary_Psychop athy	Cohen's d	,67704	,329	,203	,454
		Hedges' Korrektur	,67902	,328	,203	,453

t. t-Test bei abhängigen Stichproben: Online- vs. Offline-Skrupellosigkeit bei Black Hat Hackern

Statistik bei gepaarten Stichproben

		Mittelwert	N	Std.- Abweichung	Standardfehl er des Mittelwertes
Paaren 1	Online_Verhalten	3,6489	321	,98986	,05525
	Offline_Verhalten	2,6501	321	1,14036	,06365

Test bei gepaarten Stichproben

		Gepaarte Differenzen					Signifikanz			
		Mittelwert	Std.- Abweichung	Standardfehl er des Mittelwertes	95% Konfidenzintervall der Differenz		T	df	Einseitiges p	Zweiseitiges p
					Unterer Wert	Oberer Wert				
Paaren 1	Online_Verhalten - Offline_Verhalten	,99688	,98301	,05487	,88894	1,10483	18,169	320	<,001	<,001

Effektgrößen bei Stichproben mit paarigen Werten

			Standardisier ^a		95% Konfidenzintervall	
				Punktschätzung	Unterer Wert	Oberer Wert
Paaren 1	Online_Verhalten - Offline_Verhalten	Cohen's d	,98301	1,014	,879	1,148
		Hedges' Korrektur	,98532	1,012	,877	1,146

u. t-Test bei abhängigen Stichproben: Online- vs. Offline-Skrupellosigkeit bei White Hat Hackern

Statistik bei gepaarten Stichproben

		Mittelwert	N	Std.- Abweichung	Standardfehl er des Mittelwertes
Paaren 1	Online_Verhalten	2,7294	834	,97271	,03368
	Offline_Verhalten	1,9037	834	,88992	,03082

Test bei gepaarten Stichproben

		Gepaarte Differenzen					Signifikanz			
		Mittelwert	Std.- Abweichung	Standardfehl er des Mittelwertes	95% Konfidenzintervall der Differenz		T	df	Einseitiges p	Zweiseitiges p
					Unterer Wert	Oberer Wert				
Paaren 1	Online_Verhalten - Offline_Verhalten	,82574	,80017	,02771	,77135	,88012	29,802	833	<,001	<,001

Effektgrößen bei Stichproben mit paarigen Werten

			Standardisier er ^a	Punktschätzu ng	95% Konfidenzintervall	
					Unterer Wert	Oberer Wert
Paaren 1	Online_Verhalten - Offline_Verhalten	Cohen's d	,80017	1,032	,948	1,116
		Hedges' Korrektur	,80089	1,031	,947	1,115

Anhang 5: Erklärung zu verwendeten Hilfsmitteln und Software

Im Rahmen der vorliegenden Dissertation wurden folgende Hilfsmittel und Programme verwendet.

Verwendete Software:

- SPSS Version 31.0
- SoSci Survey
- Microsoft Word
- Citavi
- Microsoft PowerPoint

Zum Zwecke der:

- Statistischen Datenanalyse
- Technische Erstellung des Fragebogens
- Textverarbeitung
- Literaturverwaltung und Hilfe bei der Erstellung des Literaturverzeichnisses
- Anfertigung eigener Abbildungen

Verwendete KI-Tools:

- Canva
- ChatGPT
- DeepL Translate

Zum Zwecke der:

- Generierung lizenzfreier KI-Bilder und Piktogramme mit ChatGPT und Canva an den gekennzeichneten Stellen
- Korrektur Rechtschreib- und Grammatikfehler
- Übersetzung einzelner Fachbegriffe

Verwendete Darknet-Zugänge und verschlüsselte Kommunikationsmittel:

- TOR-Browser (www.torproject.org)
- Kleopatra GPG4win
- Signal, Telegram
- Protonmail

Zum Zwecke der:

- Probandengewinnung und Kommunikation mit Hackern und Beachtung strenger Beschränkungen und Anonymitätsgewährleistung

Anhang 6: Einwilligungserklärung und Interviewleitfaden

Consent & Purpose of the Study

Purpose & Scope:

This anonymous study on *Hacking Behavior and the Dark Triad Personality Traits* is part of my doctoral thesis at the University of Tübingen (Germany).

The goal is not to demonize hackers, but to truly understand some aspects of hacker culture, personalities, ethical viewpoints and mindset.

The questionnaire consists of 17 open-ended questions. You may answer them at your own pace, in any length and you may skip or stop at any time. There are no known risks involved. Please **do not share any identifying information**, such as names, addresses or anything that could compromise your anonymity. It's not about finding out *who* you are; it's just about finding out *how* you are.

I respect OpSec: Guaranteed Anonymity & Data Handling

I fully respect and understand OpSec. The data collected in this study will be fully anonymized and cannot be linked back to you: No names, email addresses, handles, or platforms used for initial contact will be associated with your answers. Any critical or revealing content or phrasing will be redacted. Original emails and contact information will be permanently deleted. What remains is an **anonymous transcript, stripped of any references to your real identity or hacker pseudonym**. These anonymous answers will be used for scientific and educational purposes only.

Once your answers have been submitted and anonymized, they can no longer be withdrawn, as they are no longer attributable to you.

Questions? Contact me directly:

Mark Hofmann - cyberpsych.study@protonmail.com

Questions:

Consent: I read the information and I agree to participate under these conditions and confirm I am at least 18 years old. (Yes / No)

-
- 1. Would you describe yourself as a Black Hat, White Hat, or something else? (Feel free to use your own terms.)**

2. What kind of hacking activities are you involved in? Has this changed over time?

3. Please describe your motivation for hacking, and whether it has changed over time.

Consider the following potential motives and feel free to elaborate on which of them play a role in your activities:

- Financial interests
- Enjoyment of challenge / technical problem-solving / testing your skills
- Peer recognition / status within hacker culture
- Feeling of power
- Addiction
- Thrill or adrenaline rush
- Rebellion / rejection of authority
- Political or social activism
- Fun / entertainment / trolling
- Frustration or revenge
- Other (please specify)

4. Would you agree with the following statement?

"If people have weak passwords and poor security, it's their own fault if they get hacked."
Why or why not?

5. Let's talk about the difference between cyberspace and real life.

- Would you hack an individual's bank account online?
- Would you steal from someone in real life?
- Would you hack companies online?
- Would you steal from companies in real life?

What are the differences for you, if any?

6. If there's a difference in your behavior online and offline, why is that?

7. Do you agree with the following statement?

"I believe there's a very low chance of being caught when engaging in hacking activities."

8. Do you agree with the following statement?

“The police are incompetent when it comes to handling cybercrime.”

9. How did your hacking journey begin? At what age? What first inspired you to explore this world? (e.g., video games, cheat codes, YouTube, 4chan, ...)

10. How did you develop your hacking skills? Please mention any sources or learning methods: self-study, forums, CTFs, mentorship, darknet, etc.

11. What do you think about the future of hacking in light of AI and deepfakes? Have you already used AI tools for your activities?

12. In your opinion, what role do social engineering and psychology play in hacking?

13. Please read the following definition of Narcissism:

Narcissism refers to an exaggerated sense of self-importance and a strong need for admiration and validation from others. Individuals with high levels of narcissism tend to view themselves as unique or special and expect others to recognize this. A common feature is a lack of empathy and the prioritization of one's own needs over those of others.

It is not a black-and-white label but exists on a continuum. Do you recognize any of these traits in yourself?

14. Please read the following definition of Psychopathy:

Psychopathy is characterized by a general lack of empathy, guilt, or remorse. People with psychopathic tendencies often behave impulsively and take risks without considering the consequences. They may appear cold, manipulative, and emotionally detached.

Again, this exists on a spectrum. Do you see any of these traits in yourself?

15. Please read the following definition of Machiavellianism:

Machiavellianism refers to manipulative, strategic, and self-serving behavior. Individuals high in Machiavellianism often pursue their goals at others' expense, avoid conflict when it suits them, and prioritize their own interests. Their actions are usually guided by long-term strategy rather than emotion.

Do you recognize any aspects of this in yourself?

16. I respect your OpSec. Please do not share any information that could make you personally identifiable. However, to get a general sense of who you are, it would be helpful to know your **approximate age, gender, and nationality**, for example something like: **"male, 30-35, USA"** is more than enough.

17. Take the Short Dark Triad Test:

The *Dark Triad* of personality includes Machiavellianism, Psychopathy, and Narcissism. It would be very interesting to get your scores on this 3-min multiple choice test. It's attached as a txt-file. If you want you can fill it out and send it together with your answers. I can give you your scores and how you compare to the general population and other hackers.

Thanks for participating!

Anhang 7: Kategoriensystem

Deduktive Kategorienanwendung:

Themenbereiche Interviewleitfaden	Kategorien
Profile und Motive	Selbstidentifikation
	Motive
	Freiwillige allgemeine soziodemografische Angaben (Altersgruppe, Geschlecht, Land)
Enthemmung und Rechtfertigung	Schuldexternalisierung
	Online- vs. Offline-Persona (Online Disinhibition Effect)
	Entdeckungswahrscheinlichkeit & OpSec
Beginn der Hackerkarriere	Quelle der Hackingfähigkeiten
Rolle von Social Engineering & KI	Rolle von Social Engineering beim Hacking
	Rolle der KI beim Hacking
Dunkle Triade der Persönlichkeit	Psychopathie
	Narzissmus
	Machiavellismus

Anhang 8: Codebogen Black Hat Hacker

Deduktive Kategorienanwendung

Thematisches Codieren nach Flick (2025)

- Jede Textstelle wird zusammen mit der Quelle (Interview ID) in die passende Kategorie eingefügt
- Code/ Interpretation: Fassen die Kernaussage oder Bedeutung in eigenen Worten zusammen.

Kategorie: Selbstidentifikation

ID	Textstelle Interview	Code/ Interpretation
BH01	„Before everything else, I'm an engineer. But life turned into despair, and to survive I had to become something else, I had to create a persona that would help me get my life back.“ (Z. 39-40)	Selbstbild als „Ingenieur“
BH01	„I don't put any label on myself, it's just me.“ (Z. 40-41)	Mag keine Label
BH01	„But if I had to, then I would say that I'm a survivor.“ (Z. 41)	Sieht sich als Survivor
BH01	„Being a hacker doesn't mean someone is a cyber-criminal, there is a distinction, [...]“ (Z. 98)	Unterscheidung Hacker vs. Cyberkrimineller
BH01	„[...] but to become a good hacker you must break things, in order to put them back together, to test them, to reverse engineering them and exploit them, for knowledge, for passion of doing things and trying things.“ (Z. 98-101)	Black Hat - White Hat verschwimmende Grenzen
BH02	Hackt unautorisiert, z.B. „dumping databases by finding SQL-vulnerabilities“ (Z. 43-44), betrachtet sich aber als „Gray Hat!“ (Z. 39)	Selbstbild als Gray Hat (Moral Justification)
BH03	„I'd say Gray Hat. I don't do harm for fun or profit, but I definitely don't ask for permission before poking around.“ (Z. 39-40)	Selbstbild als Gray Hat (Moral Justification)
BH04	„I actually consider myself as both Black Hat and Gray Hat, because as a Black Hat Hacker I hack things illegally for fun, enjoyment, entertainment, training, experience, experiment and being bored. As a Gray Hat Hacker I hack stuff for good things, such as hacking scammers, Doxxers, Pedos, drug dealers, weapon dealers and human traffickers, later exposing them.“ (Z. 39-42)	Realistisches Selbstbild: Taten im Einklang mit Selbstidentifikation
BH05	„I'm a Black Hat Hacker and I operate outside the law and I'm fully aware of it. I'm not here to help co-operations. I exploit them based on needs.“ (Z. 39-40) „I'm a Black Hat Hacker, yes. I do phishing and bank scams. Well, I'm Involved in any job that is financially motivated.“ (Z. 44-45)	Realistisches Selbstbild: Taten im Einklang mit Selbstidentifikation
BH06	„I'm a Black Hat Hacker and I do it because I can.“ (Z. 39) „I've been into Account takeovers, botnet controls and doxxing.“ (Z. 43)	Realistisches Selbstbild: Taten im Einklang mit Selbstidentifikation
BH07	„In a way, no one is Black Hat or White Hat entirely.“ (Z. 40)	Black Hat - White Hat verschwimmende Grenzen
BH07	„I am Gray Hat.“ (Z. 41)	Ist Black Hat Auftragshacker, sieht sich als Gray Hat
BH07	„I take tasks for helping others, it can even be hacking someone's phone or device, or finding info about someone, analyzing the requests or network packets, or even more: malware, RATs, and many things“ (Z. 50-52) „[...] of course, all are illegal. I help with good intentions too, though it all depends on perspective: for law, I am evil, for them, I am their brother.“ (Z. 42-46)	Auftragshacker, sieht sich aber als Gray Hat, da er seinen Auftraggebern ja hilft

ID	Textstelle Interview	Code/ Interpretation
BH07	„Scammers are just the ones who don't have hacking skills; they just wish for money. We wish for fun, money, and other things too. I don't mean we are good people; it is just that our ways are more professional and fired.“ (Z. 101-103)	Scammer = nur durch Geld motiviert und technisch schlecht
BH08	Agiert als Black Hat und sieht sich als „Black Hat Hacker.“ (Z. 39)	Realistisches Selbstbild: Taten im Einklang mit Selbstidentifikation
BH09	„Currently I mainly develop exploits“ (Z. 44) „I am certainly not White Hat. I consider myself a Gray Hat now, used to do more Black Hat activity before.“ (Z. 39-40)	Entwickelt Exploits, sieht sich aber als „Gray Hat“
BH09	„Many private-sector White Hats were once Black/Gray Hats, probably many are still moonlighting, as such skilled people help police catch less-skilled people to keep a target off their back. This is, of course, not the general rule, but I am saying this can happen and does happen, and I find it funny.“ (Z. 88-91)	Viele Black Hats arbeiten auch als White Hats
BH09	„You have to consider, where did these professionals get the knowledge? Let me tell you: they don't teach you these things in schools LOL.“ (Z. 92-93)	Nicht möglich White Hat zu werden, ohne Black Hat gewesen zu sein
BH10	Eindeutige Black Hat Aktivität: „Yes, I would, and do, hack and steal from the bank accounts of individuals.“ (Z. 85) „Most of my time is spent on the acquisition and sale of private data. This is mostly done through ransomware and extortion.“ (Z. 46-50) „In terms of 'Black/White/etc.' I would consider myself to be in somewhat of a gray area, as I do not necessarily act based on morals or the law, for that matter, but rather financial gain.“ (Z. 39-41)	Begeht Ransomware-Erpressung, sieht sich aber als Gray Hat
BH11	„I focus on corporate espionage, like data breaches and wallet exploitation, from low-end scams to strategic operations.“ (Z. 43-44) „I'm a Black Hat Hacker with a code, mostly it's all about leverage.“ (Z. 39) „I rarely hack individuals, but focus mainly on companies.“ (Z. 73)	Realistisches Selbstbild: Taten im Einklang mit Selbstidentifikation
BH12	„I see myself as a Black Hat and Gray Hat Hacker.“ (Z. 39-40) „I am involved in professional hacking on Instagram, and I am very specialized in it. I also work on other things like phishing, social engineering, hijacking, malware injection for other social media platforms, or taking control of victims' devices. I also crack RDPs and hack websites with low security.“ (Z. 44-47)	Realistisches Selbstbild: Taten im Einklang mit Selbstidentifikation
BH13	„Black Hat / "shadow spoofer".“ (Z. 39) „Vulnerability exploitation and Social Engineering“ (Z. 44)	Realistisches Selbstbild: Taten im Einklang mit Selbstidentifikation
BH14	„I'm a Black Hat Hacker actually, but I'm also in the field of doing jobs that a grey hat hacker can do and also in the field of doing jobs that a White Hat would do.“ (Z. 48-49) „I receive jobs from people. I do jobs for people and I also pick targets myself sometimes, to keep myself busy.“ (Z. 53-54) „Well, actually, I'm on the dark web. And yes, I do have a chat room on the dark web. Yes, I've been doing a lot of jobs on my website has been taken down a lot of times by Interpol. So it's kind of... I come back stronger, you understand?“ (Z. 63-65)	Erfüllt Aufträge aller Art, egal ob legal oder nicht

ID	Textstelle Interview	Code/ Interpretation
BH14	„Yes, I was into ethical hacking then and I watched the movie and I got like the rush to get, into the business, like know more about hacking and I started to write my own malware and exploits and software and mixing machines for money laundering and a lot of things.“ (Z. 82-85)	Seiten gewechselt motiviert durch einen Film

Kategorie: Motive

ID	Textstelle Interview	Code/ Interpretation
BH01	„But life turned into despair, and to survive I had to become something else, I had to create a persona that would help me get my life back.“ (Z. 39-40)	Finanzielle Notwendigkeit als Motiv
BH01	„I don't even know where to start, it's more than 20 years of work. Yes, motivation changes over time, for the simple fact that we grow as people and our necessity changes [...]“ (Z. 63-65)	Motive haben sich verändert im Zeitverlauf
BH01	„When I was younger it was everything about exploring the internet world, trying writing code, it was a constant excitement“ (Z.66-67)	Beginn aus Neugierde/ Excitement
BH01	„[...] but then it changes into a job and then you have to start making money“ (Z. 67-68) „The road never been easy btw.“ (Z. 68-69) „Of course, there is financial interests (I find "financial needs" more appropriate)“ (Z. 70) „[...] but I never been proud when I have done something "bad".“ (Z. 72-73) „I'm just someone who went to hell and came back.“ (Z. 106-107)	Betont finanzielle Notwendigkeit
BH01	„Also, especially in my prime years, excitement, yes.“ (Z. 71)	Excitement als Kernmotiv
BH01	„Rebellion? Yes, since forever, it's part of my nature.“ (Z. 74)	Rebellion als Kernmotiv
BH01	„Never felt powerful, never felt addicted.“ (Z. 72)	Sucht und Macht spielen keine Rolle
BH01	„I did what I did for many different reasons.“ (Z. 72)	Motivbündel
BH01	„I never had respect for the system, for its people, politicians or else“ (Z. 75)	Disrespect für das System
BH01	„Maybe it's more like a statement: "Don't fuck with me, I never give up, you can be smarter, you can have resources, but I'm persistent, you are just training, no matter what it costs me, in the end I will always find a way to win.““ (z. 78-81)	Rache/ Challenge/ Herausforderung
BH02	Zur Liste der Motive: „I guess a bit of all hahaha.“ (Z. 68)	Motivbündel
BH02	Hack companies? -> „Yes, If I get an opportunity.“ (Z. 84) „No, I wouldn't commit any financial crimes.“ (Z. 82)	Hacking aus nicht- finanziellen Motiven
BH03	„At first, it was curiosity and wanting to outsmart systems. Now it's more about the challenge, learning, and sometimes making bread.“ (Z. 62-63)	Motive gewandelt: Neugierde, Herausforderung, Lebensunterhalt
BH03	„making bread“ (Z. 63)	Betont finanzielle Notwendigkeit
BH04	„Can I say all of them? Because I feel like that's all of the reasons that motivate and discipline me each time I go on this path?“ (Z. 65-66)	Motivbündel
BH04	Hauptmotiv: „Then I would say it's "testing your skills, peer recognition.“ „And to respect and honor the death of a well-known hacker in the world [...] Kevin Mitnick.“ (Z. 68-71)	Selbstwirksamkeit und Anerkennung
BH05	„I do phishing and bank scams. Well, I'm Involved in any job that is financially motivated“ (Z. 44-45)	Finanzielle Motive
BH05	„Well, it has always been for financial gain, status and control.“ (Z. 62) „My motivation is money and status. Just like a trophy cabinet, that shows how far I've gone in the game.“ (Z. 65-66)	Motivbündel: Geld, Macht, Status

ID	Textstelle Interview	Code/ Interpretation
BH06	„I love the thrill, it's fun watching systems collapse and I like to see things burn, it's not always about the money.“ (Z. 60-61)	Freude an Zerstörung
BH07	„For me personally, I enjoy breaking into systems and researching to increase skills more. Nothing motivates me, the more challenge I see, the more I want to grow stronger and break it.“ (Z. 70-72)	Motiv Herausforderung
BH07	„There is no one thing that motivates me; you cannot ask why a biker loves to ride. It is simple: because it is fun.“ (Z. 78-79)	Hacking wie Motorradfahren (intrinsisch motivierte Leidenschaft)
BH07	„We wish for fun, money, and other things too.“ (Z. 101-102)	Motivbündel: Geld, Spaß und Sonstiges
BH08	„Now it's business, not fun. Moving into banking sectors and more.“ (Z. 44) „I was motivated by money at first, but I love it when I break into something big, cracking stuff to prove I could. My status mattered then.“ (Z. 61-62)	Motivbündel: Status und Geld
BH09	„When I started, it was mostly enjoyment of challenge, technical problem-solving, and testing your skills, but as you get more involved and communicate with others doing the same thing, it quickly became peer recognition and an addiction, with a little bit of fun, entertainment, or trolling being a motivator. But then you grow up and have to pay the bills, now it's mostly financial interests.“ (Z. 60-64)	Wandel der Motive im Zeitverlauf
BH09	„Do not get me wrong, even if it's mainly for financial interest, I always enjoy a challenge, and developing my skills and being respected by my peers is a side effect of the skills that come with that.“ (Z. 65-67)	Motiv hinter dem Motiv „Geld“
BH10	„My motivation behind my actions always has been, and always will be, money. Sure, there are other reasons which I suppose would add fuel to the fire, so to speak, but money is by far my biggest priority. I would also say that there is some degree of addiction involved in such actions, as I, along with most people I know, feel a thrill of some kind from pulling off said actions.“ (Z. 66-70)	Motivbündel: Geld und Sucht (Thrill)
BH10	„One thing that I do not care for is recognition or notoriety, and I do not have a permanent online identity for such reasons.“ (Z. 70-71)	Status spielt absolut keine Rolle
BH10	„I hope my actions help spark a flame of distrust for banks, as I personally hate them.“ (Z. 88-89)	Anti-Autorität und Anti- Kapitalismus
BH10	„Yes, I would, and do, hack companies online for both my own financial gain as well as the financial loss of the targeted business. I typically go for bigger corporations as I despise capitalism and believe those in the 'best' positions deserve the worst. I will not bore you with the details.“ (Z. 95-98)	Anti-Autorität und Anti- Kapitalismus
BH11	„Financial gains = yes. I also love puzzles built by arrogant engineers.“ (Z. 61)	Motivbündel: Geld + Herausforderung
BH12	„It's just that I sometimes lose track of whether it's day or night while I'm working, it doesn't matter to me.“ (Z. 48-49)	Flowzustand / Sucht
BH12	„My motivation for hacking the most is financial interest, I want financial stability.“ (Z. 65) „Second, I enjoy it. It is like I can't leave it, like I am addicted to it. I pass hours and hours sitting in one place. While working, I forget all the things which make me scared, as well as it stops my overthinking, that's also a reason.“ (Z. 67-70) „But seriously, I don't drink, nor use any drugs, or have any other addiction, except hacking.“ (Z. 78)	Motivbündel: Geld und Sucht
BH12	„The only inspiration for me was: if everything is unfair, then why should I be fair and suffer a lot? No, I shouldn't. I should do what I like, what I want, no matter what happens.“ (Z. 137-138) „I don't believe in God and I am also influenced by nihilism and Charvak philosophy.“ (Z. 75) „[...] but life is not fair, nature is not fair, even in my country they are unfair“ (Z. 83-84)	Nihilistische Einstellung der Sinnlosigkeit

ID	Textstelle Interview	Code/ Interpretation
	„I was a very, very religious person. I even decided to become a monk, but after that, I tried to find the science (now we call it pseudo-science) in my religion, then after that I came to know the truth that no God exists and the world is meaningless.“ (Z. 200-202)	
BH13	„It started as curiosity, but shifted toward reputation building.“ (Z. 44-45)	Motive gewandelt
BH13	„Mostly challenge, skill-testing, and peer recognition; less about money now.“ (Z. 61) „I enjoy the process more than the output. Money is just a tool to access more.“ (Z. 163)	Motivbündel: Herausforderung, Anerkennung, Geld
BH13	„As a hacker building a reputation matters. The total of completed jobs / total of failed jobs. A good win rate specifies a good reputation.“ (Z.151-152) „To those who know.“ (Z. 154)	Anerkennung vor peer group
BH14	„Most of my work is for the money and also the skill.“ (Z. 77)	Motivbündel: Geld und Herausforderung

Kategorie: Schuldexternalisierung

ID	Textstelle Interview	Code/ Interpretation
BH01	„Many people have zero knowledge in terms of internet security, especially at a certain age. They trust the system. They are easy targets. Also, there is no education about it. Their fault? They can learn more, yes, but this applies to many other things in life.“ (Z. 85-88)	Teilschuld bei Opfern
BH02	„Totally agree, I think it's important to care for your digital assets, like you do for your physical assets. If you wouldn't use a weak lock for your gold, why would you for your accounts?“ (Z. 72-73)	Schlechter Schutz = Opfer selbst schuld
BH03	„Blame should fall more on tech companies, that don't design secure defaults.“ (Z. 67-68)	Teilschuld bei Techkonzernen
BH04	„[...] it's their fault for not listening, and that's one of the main reasons in this world, that those reckless people get hacked easily.“ (Z. 75-76)	Opfer selbst Schuld
BH05	„If you have a bad door in a bad neighborhood, you should expect a visit.“ (Z. 70)	Teilschuld bei Opfern
BH06	„Hell yeah, because we are in a jungle, don't act like a prey.“ (Z. 65)	Teilschuld bei Opfern
BH07	„True, actually. Weak passwords are bad“ (Z. 83)	Teilschuld bei Opfern
BH08	„Having weak passwords is the victim's fault.“ (Z. 66)	Opfer selbst Schuld
BH09	„The dummies on the internet should be happy that we, who keep everything running, let them online in the first place. If they don't want to put in the work of keeping themselves safe, it's on them for getting hacked.“ (Z. 71-73) „It's like walking into the wrong side of town, known for robberies and danger, flaunting cash and not having any form of protection, and being surprised when you get robbed.“ (Z. 74-75)	Völlige Schuldumkehr
BH10	„In a sense, I hope that people learn from their mistakes and do not allow people like myself to take advantage of them in the future. However, weak security is no different from an open door.“ (Z. 76-78)	Zynisches Bild: Hoff das Opfer aus seinen Taten lernen + Metapher
BH10	„Although I just mentioned that individuals are responsible for their own security, I believe that the banks hold the majority of that responsibility when they are trusted by the aforementioned individual. If they cannot reasonably secure funds, they should not be in possession of them.“ (Z. 85-88)	Teilschuld bei Banken
BH11	„Partially true, but the system is also to blame, because they don't enforce better security.“ (Z. 65)	Teilschuld beim System
BH12	„[...] people want to be fools.“ (Z. 88)	Menschen wollen getäuscht werden
BH13	„Agree, users bear the responsibility of their personal information.“ (Z. 66)	Teilschuld bei Opfern
BH14	„[...] but if you are not OpSec-wise, I would say it's entirely your fault. So it's more like a 50-50.“ (Z. 100-101)	Teilschuld bei Opfern

Kategorie: Online- vs. Offline Persona

ID	Textstelle Interview	Code/ Interpretation
BH01	„This doesn't mean I'm willing to physically steal from someone on the street, that's a very different kind of criminal." (Z. 102-103)	Reales Stehlen sei was ganz anderes
BH01	„Yes, I would hack companies online, but here too there must be a reason. And no, I don't see myself stealing from companies in real life. I'm not a thief." (Z. 105-106)	„Ich bin ja kein Dieb“
BH01	„I can't be just one person." (Z. 110)	Differenz Online vs. Offline Identität
BH01	„Also, I do charity work, so I guess that I don't lack empathy." (Z. 150-151)	Online Hacker, Offline engagiert für Charity
BH02	„No, I have never stolen anything in real life, not even candy from an aisle." (Z. 83)	Würde nicht mal Kaugummi stehlen
BH02	„Offline, I'm open with my friends and family about everything, except my online presence, I'm an open book and love socializing. But online, I stay anonymous on some aliases, while not on some other." (Z. 88-90)	Differenz Online vs. Offline Identität
BH03	„The internet creates emotional distance." (Z. 80) „Online feels abstract. It's easier to justify digital intrusion than physical actions. But impact is impact, so it's something I stay mindful of." (Z. 83-84)	Online-Verhalten fühlt sich nicht real an
BH04	„I'm only skilled in digital stealing, that's why I don't interfere physically, because I'm not physically strong." (Z. 84-85)	Stiehlt „nur“ digital
BH04	„Theres actually not any difference between me in online or offline, because even my own friends know that I'm a hacker, I even work with them as a free hire-a-hacker." (Z. 89-90)	Kein Doppelleben
BH05	„I'm emotional with physical victims, but online, it's a mask." (Z. 81) „It means, I can't steal from people physically, but online it's a free world." (Z. 83)	Online ist es wie eine Maske
BH06	„In real life consequences are immediate. I don't want to mess with that. I could hack a bank but not rob it, also I won't hurt people in real life just web work where it's secured." (Z. 73-74)	Stiehlt „nur“ digital
BH06	„In the real world I'm just a dude. I'm not taking risks I can't walk away from." (Z. 77)	Differenz Online vs. Offline Identität
BH07	„We don't work in real; what we do stays here. In the real world, we are the same as others." (Z. 96) „In real, I would just love to have a coffee." (Z. 98)	Differenz Online vs. Offline Identität
BH08	„I won't rob someone on the streets. Too many people watching, robbing online is fair game." (Z. 74)	Real Gefahr zu groß, Online = Freiwild
BH08	„I feel invisible online, plus the thrill to stay behind the keyboard." (Z. 77)	Online-Verhalten fühlt sich nicht real an
BH09	„[...] petty theft IRL is high risk, low reward, when you can do it online for low risk, high reward." (Z. 83-84)	Cybercrime = Low risk, high reward
BH09	„[...] or sometimes I volunteer IRL to help homeless people." (Z. 143)	Hilft Obdachlosen in der Realität
BH10	„Yes, I would, and at one point in my life greatly considered, stealing from people in real life, as I see that as no different from my online activity. There is an added risk of being caught and confronted, but that is all." (Z. 91-93)	Kein Unterschied, außer Risiko
BH10	„Yes, I absolutely would, and once did (many times), steal from companies in real life. As I mentioned in Point 2, I was once into carding, and a 'skill' I picked up from those days involved receiving products from companies without paying a single penny, and instead leaving that debt on their own tab. I believe in the end I accumulated ~\$40,000 worth of merchandise from a very wide array of companies, in fact, every single appliance in my home was acquired through these means." (Z. 100-105)	Stiehlt auch real, ganze Einrichtung gestohlen

ID	Textstelle Interview	Code/ Interpretation
BH10	„Hack and steal from everyone and everything I can when I am online. I work a rather mundane and low-paying job in real life. I actively despise capitalism and attempt to ruin companies that benefit from the evils of it when I am online. I actively contribute to a capitalist society in real life. My online and offline identities are essentially polar opposites. The reason for the difference is mostly for my privacy and for some level of plausible deniability if, for some reason, my two identities are ever connected.“ (Z.115-120)	Normaler Job als Alibi. Hasst Kapitalismus, aber ist Teil davon in analogen Leben
BH11	„Digital crimes are like a hit-and-run, but offline is something I won't want to go into.“ (Z. 76)	Würde offline nicht stehlen
BH12	„Yes, I would hack companies if their main motive is to make much profit, then I should be behind that. I will also make profit from that.“ (Z. 102-103) „No, I would not steal in real life from companies.“ (Z. 105)	Stiehlt „nur“ digital
BH12	„Like I never use any bad words because I haven't felt the need to use them (Never means never). I become, how I am, in the Cyber World.“ (Z. 113-114)	Würde real nicht mal fluchen
BH13	„Would hack an individual bank accounts [...] and would hack companies. There is no difference, it's a game.“ (Z. 74-75) „To me it's just a game sometimes you win, sometimes you lose. That's the mindset I have for them.“ (Z. 159-160)	Online ist wie ein Spiel
BH13	„Online feels more anonymous and theatrical; offline has real, immediate consequences.“ (Z. 78)	Online ist wie Theater
BH14	„I don't think stealing in reality is a wise thing to do.“ (Z. 108) „Because I would say it's not safe. I would just say it's not safe.“ (z. 110)	Würde nicht real stehlen
BH14	„I'll say one thing for sure. I'm a movie guy. If you watched Batman Last Knights, someone said something: "Nobody cares about me or who I am, until I put on the mask.“ (Z. 163-164)	Online andere Persönlichkeit (wie Batman)

Kategorie: Entdeckungswahrscheinlichkeit und OpSec

ID	Textstelle Interview	Code/ Interpretation
BH01	„Newton's Third law, "you can't go ahead without leaving something behind".“ (Z. 107)	Man hinterlässt immer Spuren
BH01	„Everybody can get caught. It doesn't matter how simple a task may seem, you can't lower your guard just because you are in hurry or something. You must keep following your system, your method, your routine. You must be a machine. You need discipline, or you are fucked.“ (Z. 114-117)	Man muss eine disziplinierte Maschine sein und immer wachsam (Machiavellismus)
BH02	„No, there's a high chance, almost always because of OpSec problems. I had one case, where I was caught dumping a website's database online publicly for no profit“ (Z. 94-95)	Hohe Entdeckungswahrscheinlichkeit
BH03	„If you know what you're doing and keep your OpSec tight, the odds are low.“ (Z. 88)	Niedrige WK, wenn OpSec gut
BH04	„Yes, because I've been doing this same thing for 5 years, and neither me, my friends, nor my dealers got caught, and the reason is because I stayed true to myself without breaking any of my own rules or protocols“ (Z. 94-96)	Niedrige WK, wenn OpSec gut
BH05	„Yes, that's true, if you know what you are doing.“ (Z. 87)	Niedrige WK, wenn OpSec gut
BH06	„If you are good, it's very low. Most people get caught working with idiots.“ (Z. 81)	Niedrige WK, wenn OpSec gut
BH07	„See, the thing is simple: no system is safe.“ (Z. 86-88)	Alles ist angreifbar
BH07	„It all comes down to how cautious one stays; the moment you lose your cool, you are done. It is all about how much calm you maintain; the moment you start to believe you are the best, everything ends.“ (Z. 110-113)	Impulsivität und Narzissmus als OpSec Gefahr
BH07	„It depends. Hacking small things or not crossing paths with the NSA is good“ (Z. 107)	Entdeckungswahrscheinlichkeit abhängig von Relevanz
BH08	„Low chance of getting caught, because I don't brag or work with dumb people.“ (Z. 81)	Narzissmus als OpSec Gefahr

ID	Textstelle Interview	Code/ Interpretation
BH09	„I am very confident that I won't be caught." (Z. 97)	Niedrige WK, wenn OpSec gut
BH10	„I do believe there is a low chance of being caught. If you know what you are doing, take basic precautions, and do not allow greed or ego to cloud your OpSec, the chances of actual legal consequences are slim to none" (Z. 124-126)	Niedrige WK, wenn OpSec gut, Narzissmus als Gefahr
BH10	„I act as though I am already under surveillance from them as a habit." (135-136)	Agiert gewohnheitsmäßig wie unter Beobachtung
BH11	„Yes, if you practice good OpSec." (Z. 80)	Niedrige WK, wenn OpSec gut
BH12	„Yes, I believe that there's a very low chance to be caught when engaging in hacking activities. I follow a full anonymous structure. I make sure to do White Hat activities in a different environment, and for Black Hat hacking, I use a separate environment." (Z. 119-121)	Niedrige WK, wenn OpSec gut
BH13	„Disagree. The risk of being caught is real and often underestimated." (Z. 82)	Hohe Entdeckungswahrscheinlichkeit
BH14	„Well, and I'll say in the hacking space, there's no guarantee you don't get caught. Your OpSec matters" (Z. 113-114)	Niedrige WK, wenn OpSec gut

Kategorie: Kompetenz der Polizei

BH01	„No. The Police is not incompetent, and in the scenario where you believe that the police is your adversary, then you should never, never, underestimate your opponent." (Z. 121-122)	Nicht inkompetent
BH02	„They are incompetent, at the least where I live, they are." (Z. 100)	Inkompetent
BH03	„Most law enforcement are years behind and rely on third parties to do the actual work. Exceptions exist, but they're rare." (Z. 92-93)	Inkompetent
BH04	„Yes, totally, because even after many years, they still use old-school methods." (Z. 101)	Inkompetent
BH05	„No, they are becoming more advanced." (Z. 91)	Werden kompetenter
BH06	„Completely, they're busy raiding people, torrenting movies, while ignoring the actual crime." (Z. 85)	Inkompetent, falscher Fokus
BH07	„Yes, a bit; though the real issue is about this too: many people don't report it to them. It depends on the level of cops you mean. Even German FEDs took down breachforms and their team recently." (Z. 117-119)	Hohes Dunkelfeld, unterschiedlich kompetent
BH08	„I don't think they have the skill set to deal with people like me or my team." (Z. 85)	Inkompetent
BH09	„The police are incompetent in cyberspace, the only ones who get caught are skids and dummies. The police need private-sector partnerships to even do that." (Z. 88-89)	Inkompetent
BH10	„Truthfully, my knowledge of the police is limited. However, from what I have heard, I believe it is fair to say that they are not only incompetent but a joke. Their approach is reactive, not proactive, and they rely on third parties and private-sector actors to do the real work." (Z. 131-133)	Nicht nur inkompetent, sondern ein Witz
BH10	„That said, three-letter agencies are a different story. They are not incompetent. They are extremely patient, extremely quiet, and, unfortunately, extremely effective." (Z. 133-135)	Three Letter Agencies sind sehr effektiv
BH11	„Yes, unless they are in the top-5 jurisdictions globally, they rely on external intelligence or on leaks." (Z. 84-85)	Inkompetent, je nach Nation
BH12	„But they forget that it doesn't matter how many cases there are, their duty is to solve every case, not just saying this or that, blah blah. They work if the party is big [...]" (Z. 130-132)	Polizei untätig bei kleineren Fällen
BH13	„Mixed. Some police units are skilled, others under-resourced." (Z. 86)	Unterschiedliche Kompetenz
BH14	„The police are doing a good job" (Z. 115)	Kompetent

Kategorie: Quelle der Hackingfähigkeiten/ Hacker-Karriere

ID	Textstelle Interview	Code/ Interpretation
BH01	„I started around 16. Hacking forums, coding, hardware to test. It's been more than 2 decades ago, that was the game back then. I have always studied and practiced by myself.“ (Z. 126-127)	Beginn mit 16: Hacking-Foren, Herumprobieren, Selbststudium
BH01	„Keep studying and practicing, years of it.“ (Z. 131)	Jahre des Selbststudiums
BH02	„Initially, it was purely to get a lot of Minecraft accounts to cheat in-game and evade bans.“ (Z. 51)	Beginn über Computerspiele
BH02	„Over time, it became somewhat fun to manipulate social media. In college, I was a cybersec major, worked mostly on TLS based fingerprinting research.“ (Z. 52-53)	Selbststudium und College
BH02	„Around 14 years, there used to be a popular YouTube channel on Minecraft hacking, which inspired me to cheat, which inspired me to crack Minecraft accounts. Website security used to be very low those days, they didn't even hash passwords! I think the power I felt made me continue for all these years.“ (Z. 104-107)	Beginn als Teenager über Computerspiele
BH02	„There used to be a couple forums I frequented named Nulled & Cracked. I had high reputation profiles there, I learnt from there (Skidding), moved on, and developed my own tools and shared there.“ (Z. 111-113)	Selbststudium + Foren
BH02	„In my time there, I came across some very talented individuals, collaborating with whom I learnt my current skill set; we all evolved together. I think being surrounded by such people and witnessing new hacks and ideas everyday was a very good learning point.“ (Z. 113-116)	Lerntheorie/ Subkulturtheorie
BH03	„Started with basic exploits in games, then moved into web-app vulnerabilities and OSINT. Lately more into Social Engineering, with mastery of 7 program languages.“ (Z. 44-45) „Around 13. I was modding games, stumbled onto cheat forums, and it spiraled into scripting, exploits, and IRC culture. Never stopped learning and creating projects since.“ (Z. 97-98)	Beginn als Teenager über Computerspiele
BH03	„90% self-study. Books, forums, CTFs, exploit DBs, reverse-engineering old malware. Occasionally, I learned from older hackers on Discord and Darknet forums.“ (Z. 102-103)	Primär Selbststudium + Foren
BH04	„During the first two years, it was self-teaching; third year, a little bit on the Darknet, forums, videos, websites, blogs, and studying with my friends who are also interested in both hacking and cyber security; fourth and fifth year, diploma, HND, and online-classes. But even after all those years, still the self-teaching was the main method.“ (Z. 113-116)	Primär Selbststudium + Foren
BH05	„When I was 18, I started with online forums.“ (Z. 95) „Black Hat Chat , Red Hat Chat forums.“ (Z. 97) „I learnt most by myself from programming up to where I'm at now.“ (Z. 101)	Primär Selbststudium + Foren
BH06	„Found a leaked keylogger on a hacking forum, sent it to classmates and watched chaos unfold LOL 😂.“ (Z. 89-90) „I learnt from RIP forums, ChatGPT styled code and Darknet-tutorials.“ (Z. 94)	Primär Selbststudium + Foren
BH07	„For me, "research and break" was the rule. I find a challenge in any deep research on how it works and operates, try some tools, find some new ways of bypassing and breaking it, it was fun.“ (Z. 122-124)	Trial & Error
BH07	„On the web, you could find so much info on how it works, I gather it, increase my knowledge, and build a way to break it.“ (Z. 129-130)	Primär Selbststudium + Foren
BH08	„Started with dumb shit like stealing Wi-Fi passwords, modding games, and defacing school sites over time.“ (Z. 43-44) „I was like 14, stumbled on information from the Darkweb, from forums and sites, then started testing stuff on neighbors and school networks.“ (Z. 89-90)	Beginn mit 14 durch Computerspiele und Hacking von WiFi und Schule
BH08	„Everything I know today is self-taught. I picked it up from old hackers in the game.“ (Z. 94)	Primär Selbststudium + Foren
BH09	„As you will find, if you ask enough hackers, it is often video games, and this applies to me as well. I started hacking in video games when I was 12, probably 13. It very quickly escalated to hacking others' online accounts to continue playing in the game after they were caught. Then I began developing my own cheat software, which I used to infect other game cheaters who didn't know much about computer security.“ (Z. 104-108)	Beginn mit 12/13 durch Computerspiele

ID	Textstelle Interview	Code/ Interpretation
BH09	„Everything I know about computers is self-taught. I learned from forums and chatrooms, the same ones you publish your own research on to gain respect and teach others later, when you are more skilled.“ (Z. 112-114)	Primär Selbststudium + Foren
BH10	„When I was starting out, I focused more on fraud and was active in the carding scene for a number of years. Yes, my actions have changed over time“ (Z. 47-49)	Begonnen mit Carding
BH10	„When I was around 11, I used to play a LOT of mobile games, which were riddled with ads and microtransactions, and got fed up with dealing with those. I came across the online modded APK/IPA scene and fell in love. The whole idea of changing something to work in the way which I want, completely took me by storm and is what kick-started my entire life. From there, I began learning to code, creating my own cheats for random games, and then it turned less legal 😊.“ (Z. 139-144)	Beginn im Alter von 11 durch Modding in Computerspielen
Bh10	„I began messing with mods and scripts when I was a teenager and taught myself to code by following YouTube tutorials and reading books (unfortunately, I cannot remember what those were). From there, I fell down a rabbit hole of reading Stack Overflow and joining IRC channels, and then joining some random forums where people actually explained how certain systems work. CTFs were huge for me; platforms like Hack The Box, TryHackMe, and some other invite-only private ones taught me to understand the mindset and workflow of actually working on a project. I began meeting people on bug bounty Discords and other chatrooms, which led to me being mentored by someone. I took computer science in college and went from there.“ (Z. 148-156)	Primär Selbststudium + Foren
BH11	„Started at 16, watching how robots work and discovered how much data can be accessed.“ (Z. 89)	Startete mit 16 mit Interesse an Technik/ Robotik
BH11	„I learnt most of what I know by myself and long hours of work.“ (z. 93)	Primär Selbststudium
BH12	„I started my hacking journey in the first phase of COVID-19, or slightly before (in 2020).“ (z. 136-137)	Beginn während Covid
BH12	„I have initially learned about hacking from YouTube, then came to forums and got the truth, and using that, I firstly started cracking RDPs and sold them and earned money. And like that, after, I purchased courses and taught myself, and after that learned in depth from various sources and came to this stage.“ (Z. 146-149)	Primär Selbststudium + Foren
BH13	„Early teenager years. Video games, modding and curiosity.“ (Z. 89)	Beginn in Teenagerjahren durch Videospiele
BH13	„Self-study, write-ups, CTFs, mentors, hands-on sandboxes.“ (Z. 93)	Primär Selbststudium
BH14	„There's a movie that came out some years back a hacking team, about the Dark Web.“ (Z. 78) „I had to get to watch the movie and I got like the rush to get into the business like know more about hacking and I started to write my own malware and exploits“ (Z. 83-84) „When I was around i'll say during my 17s yeah my teenage 17, I guess yes. I like, I love computers, I love checking things out, writing programs and a lot of things which got me into ethical hacking. And then as I told you, I watched the movie and then I had to change the game.“ (Z. 119-122)	Beginn in Teenager Jahren, Interesse für Ethical Hacking, Durch Film zum Black Hat geworden
BH14	„Telegram was a good place, you find a lot of information on Telegram even right now. I have some groups I'm into.“ (Z. 126-127)	Selbststudium Telegram App

Kategorie: Rolle von Social Engineering

ID	Textstelle Interview	Code/ Interpretation
BH01	Zur Rolle des Social Engineering:	Wichtige Rolle von SE

ID	Textstelle Interview	Code/ Interpretation
	„I would say a very good role, considering that when a system fails is because of human error. Studying human behavior and mind, and actions, is how we learn how to exploit them.“ (Z. 139-140)	
BH02	„Social Engineering plays a very big role. In a lot of my hacks, information has come from employees of organizations, which is how they got targeted.“ (Z. 128-129)	Wichtige Rolle von SE
BH03	„You can bypass the best firewalls, if you understand how people think. Manipulation, persuasion, timing - more effective than code in many cases.“ (Z. 112-113)	Wichtige Rolle von SE
BH04	„Both Social Engineering and Psychology are great weapons with their own specialties. You can social-engineer to make people do something they are not supposed to do, like make them give personal and private usernames, passwords, phone numbers, or even their exact location.“ (Z. 126-129)	Wichtige Rolle von SE
BH05	„Social Engineering is the base, especially for phishing.“ (Z. 112)	Wichtige Rolle von SE
BH06	„I use Social Engineering to trick people into opening the door, instead of smashing through the wall.“ (Z. 102-103)	Wichtige Rolle von SE
BH07	„It plays a major role. Hacking is not just about systems, but people themselves. Making them get what we want, manipulating them, or making them play well is a good way. Systems can be complex, though humans can't be, unless they have a well-developed mindset. Hacking is not just exploiting the device, but people themselves.“ (Z. 141-144)	Wichtige Rolle von SE
BH08	„Social Engineering is 85 percent of the game. You can buy zero days but you can't patch stupidity. People are weak“ (Z. 103-104)	Wichtige Rolle von SE
BH09	„Human error is all there is to hacking. If it's not due to Social Engineering, it's due to a bug in the code, a mistake made by a human.“ (Z. 131-132)	Auch technische Fehler indirekt menschliche Fehler
BH10	„Psychology is by far more important than code. The ability to predict and steer someone's behavior is one for which I am most grateful to have learned. I've done more with a convincing email than I've ever done with any brute force. Humans are, and always will be, the weakest link, and are so easily manipulated.“ (Z. 167-170)	Wichtige Rolle von SE
BH11	„Based on psychology, humans are predictable, if you understand their emotional triggers.“ (Z. 102)	Wichtige Rolle von SE
BH13	„Psychology often opens doors, technical tools can't.“ (Z.101)	Wichtige Rolle von SE
BH14	„You don't hack your victims for their passwords. You have to manipulate them to get their passwords.“ (Z. 94-95)	Wichtige Rolle von SE
BH14	„Social Engineering is like 80%, let me say 70 to 80% for any hacker. It's important because you have to think like a victim.“ (Z. 144-145)	Wichtige Rolle von SE

Kategorie: Rolle von KI

ID	Textstelle Interview	Code/ Interpretation
BH02	„I think websites, especially Cloudflare, are doing a good job of using AI in detecting botnet clients.“ (Z. 122-123)	KI als Chance für Cybersicherheit
BH03	„AI is a double-edged sword. Great for automating tasks like recon or phishing templates. I've used it to generate fake personas and emails, but not for exploits. Yet.“ (Z. 107-108)	KI als zweiseitiges Schwert
BH04	„Good, not bad, but at the end of the day, it all matters the way and the reason you use them.“ (Z. 120)	KI als zweiseitiges Schwert
BH05	„Well AI does a lot and helps at times.“ (Z. 105) „and one day will be used to pull off one of the biggest moves in the game.“ (Z. 107-108)	KI als Chance für Cyberkriminalität
BH06	„AI is the future and helps me a lot.“ (Z. 98)	KI als Chance für Cyberkriminalität
BH07	„For advanced hacking, AI has no way yet. It has many restrictions and flaws; what it gives is unrealistic, not the truth. One cannot learn by becoming its slave. AI is good for researching,	KI gut für Recherche, aber nicht für Code

ID	Textstelle Interview	Code/ Interpretation
	asking it to fetch links for articles, or our plans and things. For coding and finding ways, no.“ (Z. 134-137)	
BH08	„AI is a game changer. You could literally spin up phishing scams and scripts, and it cuts down time.“ (Z. 98-99)	KI als Chance primär für Phishing
BH09	„It's currently shitting on the scene, all these skids come in with AI-coded malware. It's really sad to see. I have not used it much myself, but I have seen it used for fraud, bypassing KYC, and such things to sign up under fake IDs on websites like crypto exchanges and banks.“ (Z. 118-120)	KI senkt die intellektuelle Einstiegshürde
BH10	„AI is genuinely changing everything. I've used it for automated phishing kits, voice cloning, fake documents, and bypassing certain filters. It is insane for Social Engineering. I've barely even scratched the surface of what's possible“ (Z. 160-162)	KI als Gamechanger
BH11	„AI changes everything, especially with hacking and automation, but I guess it's just getting started.“ (Z. 97-98)	KI als Chance für Cyberkriminalität
BH12	„So doing bad work will be easier [...]“ (Z. 155)	KI als Chance für Cyberkriminalität
BH13	„AI/deepfakes are game-changers; useful for research but risky if abused.“ (Z. 97)	KI als Chance für Cyberkriminalität
BH14	„It's good in the hacking space, but it's also limited. It's also limited. I have some new AIs which I have created that are unlimited“ (Z. 132-133)	KI als Chance für Cyberkriminalität, er umgeht Restriktionen

Kategorie: Narzissmus

ID	Textstelle Interview	Code/ Interpretation
BH01	„No, I don't recognize myself in any of those traits. I do what I do in silence, nobody knows who I am. I avoid point of failures. I need no admiration, no recognition.“ (Z. 149-151)	Niedriger Narzissmus, keine Suche nach Anerkennung
BH02	„I don't feel I'm anything special; I just might have been in the right places at the right times.“ (Z. 139-140)	Niedriger Narzissmus
BH03	„I like recognition, and I've definitely felt "smarter than the system" before. But I'm not attention-obsessed.“ (Z. 122-123), NARC-Score: 2.89	Moderater Narzissmus
BH04	„I would say no, because even though I do hack stuff, both legally and illegally, as both - Black Hat Hacker and Gray Hat Hacker -, I don't share them with other people for money; the main reason is to sharpen my own skills for my future job.“ (Z. 142-144)	Niedriger Narzissmus, tut es für sich, nicht für Anerkennung von anderen
BH05	„My motivation is money and status. Just like a trophy cabinet, that shows how far I've gone in the game.“ (Z. 65-66), NARC-Score: 3.0	Moderater Narzissmus: Status bedeutsam, aber her für sich selbst
BH06	„Yes, I love feeling superior to the people I exploit.“ (Z.112), NARC-Score: 4.56	Hoher Narzissmus
BH08	„I love recognition when it's deserved but I'm self-aware constantly.“ (Z. 113), NARC-Score: 4.11	Liebt Anerkennung
BH09	„Sure, I recognize myself in that. I think everyone is a bit narcissistic at times, but I also very much enjoy helping people, and everything does not always have to be about me.“ (Z. 141-142)	Moderater Narzissmus
BH10	„One thing that I do not care for is recognition or notoriety, and I do not have a permanent online identity for such reasons. Those who do focus on achieving such things are, in my eyes, pathetic.“ (Z. 70-72)	Verachtung von narzisstischer Suche nach Anerkennung
BH10	„I do believe there is a low chance of being caught. If you know what you are doing, take basic precautions, and do not allow greed or ego to cloud your OpSec, the chances of actual legal consequences are slim to none. 90% of the people who get caught are too loud or too trusting.“ (Z. 124-127)	Narzissmus ("greed or ego") als OpSec Gefahr
BH10	„Perhaps. I don't crave admiration, but I do believe I'm better than most people. Not because I need validation, but because I know how the majority of people think. There's a certain detachment that comes from seeing through the illusions of society. I would also say I do lack empathy. So yes, most likely I have some narcissistic traits.“ (Z. 179-182)	Sucht keine Anerkennung, aber fühlt sich überlegen

ID	Textstelle Interview	Code/ Interpretation
BH11	„I don't seek validation, but I know my value.“ (Z. 111)	Sucht keine Anerkennung, aber fühlt sich überlegen
BH13	„Some narcissistic traits (I enjoy recognition), but not extreme.“ (Z. 110) NARC-Score: 4.22	Hoher Narzissmus
BH14	„I do it for myself, not for the, um, validation online“ (Z. 156) NARC-Score: 3.22	Moderater Narzissmus

Kategorie: Psychopathie

ID	Textstelle Interview	Code/ Interpretation
BH01	„Also, I do charity work, so I guess that I don't lack empathy.“ (Z. 150-151)	Charity Arbeit kein „Beleg“ gegen Psychoathie, aber eher Kontraindikator
BH01	„I plan and I execute with method, any risk I take is calculated. I don't lack guilt or remorse, I feel them very sharp. Consequences are real, that's why you must be careful, not considering consequences is not an option.“ (Z. 158-160)	Primäre Psychopathie/ Machiavellismus
BH02	„Maybe a little bit, because I've taken several stupid decisions, which has gotten me into some trouble. But I do feel guilt, trust me lot of it.“ (Z. 147-148)	Impulsivität, aber Schuldempfinden (nach eigenen Angaben)
BH03	„I can detach emotionally from my targets. But I do feel guilt and have lines I don't cross.“ (Z. 130), PSYCH-Score: 2.33	Emotional kalt, aber gewisse Schuldgefühle
BH05	„No, I meant I know the consequences of my actions.“ (Z. 133)	Nicht impulsiv, strategisch
BH06	„I don't feel bad that much.“ (Z. 119), PSYCH-Score: 3.78	Recht Gewissenlos
BH06	„I love the thrill, it's fun watching systems collapse and I like to see things burn, it's not always about the money.“ (Z. 60-61)	Thrill Seeking, Freude an Zerstörung
BH08	„Guilt rarely factors in my work, I weigh risk logically not emotionally.“ (Z. 123), PSYCH-Score: 2.78	Recht Gewissenlos
BH09	„Yes, I used to have a lot of this, but as I have grown as a person, I have learned how others might feel when you hurt them (something I did not know for many years).“ (Z. 150-152)	Hat kalte Empathie gelernt
BH09	„I have also started acting less impulsively and am more calculating now (a big reason why I believe I won't be caught).“ (Z. 151-153)	Impulsivität als OpSec Gefahr
BH10	„If something can be exploited, it should be. Why should I not do something that benefits me if doing so is both easy and has no consequences for myself?“ (Z. 79-81)	Skrupellos opportunistisch
BH10	„I do feel some varying levels of guilt (not actual guilt, but the closest thing to it), depending on who I steal from. Individuals could potentially be in a tough financial spot and could suffer greatly from my actions, and for that, I do genuinely apologize, but I do not care enough to refrain from stealing from them. Companies do not deserve that same mindset. Quite frankly, there is nothing I would not do that results in a loss of any kind for any company, especially a larger corporation.“ (Z. 107-112)	Keine echte Empathie
BH10	„Empathy is conditional for me, and I don't feel guilt. I understand emotion much more than I feel it. I analyze people the same way I analyze systems by ways of vulnerabilities, triggers, behavioral loops, etc. I don't necessarily seek chaos, but if it's profitable, I wouldn't flinch either. Emotionally, I am cold. This is not a trait I hide or am ashamed of.“ (Z. 189-193)	Kalt, empathielos, rücksichtslos und sieht es nicht als Schwäche
BH10	„I don't act out of impulse unless impulse serves the plan, as doing so is OpSec suicide.“ (Z. 202)	Impulsivität ist OpSec Suizid
BH11	„No, I'm calculated, but not reckless.“ (Z. 118)	Sieht sich als berechnend, aber nicht rücksichtslos
BH12	„I don't care if people suffer or not.“ (Z. 185)	Empathielos
BH13	Sagt selbst: „Low on psychopathy, not cold or remorseless.“ (Z. 117) PSYCH-Score: 3.33	Moderate Psychopathie

ID	Textstelle Interview	Code/ Interpretation
BH14	„I'm a Black Hat Hacker actually, but I'm also in the field of doing jobs that a grey hat hacker can do and also in the field of doing jobs that a White Hat would do." (Z. 48-49) PSYCH-Score: 3.78	Führt Aufträge aus, wie Söldner (ohne Moral)

Kategorie: Machiavellismus

ID	Textstelle Interview	Code/ Interpretation
BH01	„I plan and I execute with method, any risk I take is calculated." (Z. 158)	Primäre Psychopathie/ Machiavellismus
BH01	„Well, yes, but only if that kind of behavior is needed to achieve the task. Hacking some system may involve deception, manipulation, that's social engineering. So, in this case, I can recognize myself, but only when needed for professional meaning, I don't do that with my friends." (Z. 168-171)	Nur instrumentelle Manipulation, wenn sie „notwendig" sei
BH02	„I don't feel this." (Z. 157) (MACH Score: 3.67)	Machiavellismus hoch, Selbsteinschätzung niedrig
BH03	„My ethics are situational." (Z. 40)	Moralisch flexibel
BH03	„Yes. I can be strategic, manipulative, and patient when I need to be, especially in long-term Operations or Social Engineering." (Z. 138-139)	Strategisch und manipulativ
BH05	„I'm well organized and always think ahead." (Z. 141) „Most importantly, I avoid issues by thinking ahead" (Z. 143) „I'm confident in my strategy, that's what decides how effective I am." (Z. 123-124) „It's all about the strategy" (Z. 121)	Strategisch, kontrolliert, OpSec
BH06	„Completely, I adapt, manipulate and move on. It's a game." (Z. 127), MACH-Score: 4.00	Hoher Machiavellismus
BH07	„Well, I trust myself most, so if the whole world goes against me, I would still watch with burning eyes and strength, the world is where I belong and I own it myself not for others. You see, hackers are not AI or robots, they are humans, same as others. I follow discipline, no I have no such traits." (Z. 168-171)	Agiert und manipuliert als Black Hat Auftraghacker, sieht dies aber nur als „diszipliniert"
BH08	„Yes, a strategy is my best shot plus long-term planning. I'm kind of pragmatic." (Z. 131)	Hoher Machiavellismus
BH09	„[...] petty theft IRL is high risk, low reward, when you can do it online for low risk, high reward." (Z. 83-84)	Reine Kosten-Nutzen Kalkulation
BH09	Zur Machiavellismus-Definition: „Yes, this is me currently." (Z. 161)	Hoher Machiavellismus
BH10	„I do not necessarily act based on morals or the law, for that matter, but rather financial gain." (Z. 40-41) „Yes, my actions have changed over time, but I believe that is only due to the difference in present opportunities at both times in my life, as I still have the exact same goal in mind all these years later: money." (Z. 48-50)	Finanzieller Gewinn, egal wie
BH10	„If something can be exploited, it should be. Why should I not do something that benefits me if doing so is both easy and has no consequences for myself?" (Z. 79-81) „Hack and steal from everyone and everything I can when I am online." (Z. 115)	Skrupellos opportunistisch
BH10	„Absolutely. Everything I do is calculated, and for me, I see people as tools and not constants. I don't act out of impulse unless impulse serves the plan, as doing so is OpSec suicide. I'm sure you may have also picked up on certain Machiavellian traits throughout my answers." (Z. 201-203)	Hoher Machiavellismus
BH11	„Yes, I think long term, I act based on utility, not morality." (Z. 126)	Hoher Machiavellismus
BH12	„And if I have to go up at the cost of someone, I will go." (Z. 190-191)	Skrupellose Nutzenmaximierung

ID	Textstelle Interview	Code/ Interpretation
	„If manipulation gives me benefit, then of course I will. People suffer because of the system and their fault, not because of mine.“ (Z. 192-193) MACH-Score: 4.44	
BH13	„I am strategic and pragmatic.“ MACH Score: 4.22	Hoher Machiavellismus
BH14	Antwort zur Definition von Machiavellismus: „That is exactly me!“ (Z. 171) MACH-Score: 4.00	Hoher Machiavellismus

Anhang 9: Codebogen White Hat Hacker

Deduktive Kategorienanwendung

Thematisches Codieren nach Flick (2025)

- Jede Textstelle wird zusammen mit der Quelle (Interview ID) in die passende Kategorie eingefügt.
- Code/ Interpretation: Fassen die Kernaussage oder Bedeutung in eigenen Worten zusammen.

Kategorie: Selbstidentifikation

ID	Textstelle Interview	Code/ Interpretation
WH01	„Gray Hat vermutlich. In meiner Kindheit/Jugend war ich definitiv Black Hat, jetzt arbeite ich aber professionell und legal.“ (Z. 36-37) „In Kindheit/Jugend war da leider auch Carding und Faking dabei (d. h. z. B. Kreditkartenbetrug, vor >15 Jahren). Als Erwachsener interessiere ich mich vor allem für sicherheitsrelevante Themen (z. B. Schutz von Web-Anwendungen), aber auch für das Aushebeln sonstiger Schutzmechanismen wie Kopierschutz etc.“ (Z. 46-49)	Früher Black Hat, Heute White Hat. Teils Gray Hat
WH01	„Dabei ist zu bedenken, dass meine Selbstbezeichnung als "Hacker" eher der Oldschool-Definition entspricht. Wikipedia formuliert es so schön: "A hacker is a person skilled in information technology who achieves goals and solves problems by non-standard means." (Z. 40-42) „Damals wie heute war und ist ein großes Interessengebiet das „Hacking“ im Sinne des Oldschool-Maker-Gedankens, d. h. das Erschaffen von „verrückten“ Erfindungen auf technisch-kreative Arten. Mein letztes „Hacking-Projekt“ in dieser Hinsicht war das Upgrade meiner Gastherme von 1990 auf eine smarte Steuerung.“ (Z. 50-54)	Hält an ursprünglicher Hacker-Definition fest
WH02	„Also, ich würde mittlerweile tatsächlich eher zu White Hat tendieren. Aber ich hab schon eine graue, oder sagen wir mal, dunkle Vergangenheit. Die ist aber schon 30 oder über 30 Jahre her. Das waren ja noch die Anfänge des Internets, wo man sich rumprobiert hat, BTX-Geschichten gemacht hat und so weiter, also so richtig Oldschool-Geschichten. Da wäre ich wahrscheinlich eher der „böse“ gewesen. Aber heute ist das halt nicht mehr so.“ (Z. 33-37) „Genau deswegen hatte ich dir ja auch geschrieben, ich kenne beide Seiten ganz gut. Ich kenne auch die Motivation, weil ich die selber im Grunde genommen ja habe, ein Stück weit, nur habe ich mich halt irgendwann von der illegalen Seite sage ich mal abgewandt und habe das in einen legalen Kontext gebracht. Oder auf eine legale Schiene gebracht. Aber früher also, in den Anfängen in den Neunzigerjahren, war ich zum Beispiel schon in großen Chemiekonzernen habe Zugriffskontrollen überwunden und so weiter.“ (Z. 40-45)	Früher Black Hat, Heute White Hat.
WH03	„Ich würde mich als Defense Spezialist bezeichnen, ich habe nicht das Gefühl, dass Kunden oder Unternehmen eigenes Security Personal haben und mag diese "Kriegs-/ Kampf" Begriffe.“ (Z. 37-39) „Mit 10 ist mein Interesse gewachsen. Viel Videospiele, viel YouTube, erste Linux Server (für TeamSpeak etc.)... wollte immer mehr wissen. 4chan. Angriffe auf Mastercard und Visa, selbst als Teen viel geddoSt. [Anmerkung: DDoS-Angriffe durchgeführt]“ (Z. 95-97) „Ich bin als SOC-Analyst an keiner Hacking Aktivität beteiligt.“ (Z. 43)	Früher als Kind Black Hat Aktivitäten (DDoS), heute White Hat (SOC Analyst)

ID	Textstelle Interview	Code/ Interpretation
WH04	„Da ich ja kein klassischer Hacker bin, sondern mich als ethischer Social Engineering Pentester wahrnehme, der immer nur im Auftrag des Kunden agiert, gibt es ja für mich diese Art der Unterscheidung nicht. Das ist für mich eh schon sehr ungreifbar. Also ich bin dann auf jeden Fall eher der White Hat.“ (Z. 31-34) „Denn wir suchen ja keine technischen Lücken, sondern bei uns geht es immer um den Faktor Mensch.“ (Z. 47-48) „Also wir machen von dem klassischen, also in meiner Welt, klassischen Social Engineering Pentesting über jeden Kommunikationskanal, am Telefon, per SMS, über QR-Codes, die irgendwo hingeklebt oder verschickt werden, Phishing, Spearphishing und eben analog.“ (Z. 64-67) „Ich habe Behördenbackground und habe dort entweder muss ich es jetzt rausstreichen, dann kann ich dir nicht helfen. Ich habe halt HUMINT gemacht, also Human Intelligence gemacht“ (Z. 86-88) „Das war militärisches Nachrichtendienstwesen.“ (Z. 106)	Ex-Militär/ Nachrichtendienst (HUMINT), heute White Hat/ Social Engineering Pentester, aber kein klassischer Hacker

Kategorie: Motive

ID	Textstelle Interview	Code/ Interpretation
WH01	„In Kindheit/Jugend standen auf jeden Fall Anerkennung und finanzielle Interessen im Vordergrund. Heute ist es eine nicht zu bändigende Faszination für technische Herausforderungen („Das ist nicht möglich“ ist mein Triggerwort) und anschließend das großartige Gefühl, diese Herausforderung gemeistert zu haben.“ (Z. 72-75)	Motive gewandelt
WH01	„Politisch/ideologisch bin ich ein extremer Verfechter von „Digital Sovereignty“ und dem „Right to Ownership“, d. h. ein gekauftes Gerät soll dem Kunden gehören, und diesem soll es freistehen, damit zu tun, was er will. Viele meiner heutigen „Hacking-Projekte“ sind privater Natur und haben damit zu tun, Endverbraucher-Hardware mit eigener Software zu versehen. „Also eine Mischung aus Spaß + Faszination + Herausforderung + Ideologie.“ (Z. 76-80)	Motivbündel: Spaß, Faszination, Herausforderung, Ideologie
WH02	„Also der Punkt war bei mir ziemlich spät, das war viel jugendlicher Leichtsinn. Also, ich hab in frühester Jugend in meiner Kindheit mit elf meinen ersten Computer gekriegt. Das war noch vor der 64er Zeit. Es war einfach Neugierde und was geht.“ (Z. 54-56)	Früher jugendliche Neugier/ Leichtsinn
WH02	„Aber die Qualität und der Antrieb waren ein anderer. Ich hab das nie gemacht, um finanzielle Vorteile zu erlangen oder kapital daraus zu schlagen, sondern eher aus dem Antrieb: Ich möchte Unternehmen oder einfach Schwachstellen aufzeigen.“ (Z. 69-72)	Auch unautorisiertes Hacking war ohne finanzielle Motive
WH02	„Ich hab mal einen eBay-Hack gemacht, wo ich gesagt hab: „Hier, eBay, ihr habt da offene Stellen.“ Damals gab es noch keine Bug-Bounty-Programme, und eBay fand es damals gar nicht so cool, darauf aufmerksam gemacht zu werden, und hat mich angezeigt.“ (Z. 72-75)	Früher wurde White Hat Hacking noch eher kriminalisiert
WH02	„Ja, am Anfang war es tatsächlich ein bisschen Spaß, um zu gucken, was möglich ist.“ (Z. 83-84) „Ich hatte nie die Idee... natürlich habe ich Ideen, wie man daraus Geld machen oder es auf eine schwarze, illegale Schiene bringen kann, aber das war nie meine Intention oder mein Antrieb. Ich habe nie wirklich darüber nachgedacht.“ (Z. 91-93) „Tatsächlich ist es eher sowas wie ein Revolutionsgedanke, so nach dem Motto: „Ich zeig euch jetzt mal, was geht“ oder „Ich probier mal aus, was möglich ist.“ Das ist für mich die	Motiv: Herausforderung, kein finanzieller Gewinn

ID	Textstelle Interview	Code/ Interpretation
	Kernintention. „Gar nicht finanziell, keine persönliche Bevorteilung, sondern eher zu gucken: Was ist möglich? Was ist schaffbar? Wie kann ich Systeme knacken? Schaff ich das oder nicht? Am Ende wie ein Sportler.“ (Z. 112-116)	
WH03	„Als White Hat liegt meine Motivation in dem Schutz betroffener Unternehmen. Ich finde es nicht in Ordnung, wenn Kunden Opfer werden, damit jemand sein Machtgefühl ausleben kann. Ich habe ein sehr starkes Gerechtigkeitsbedürfnis und setze mich auch privat für Schwächere und Minderheiten ein.“ (Z. 47-50)	Motiv: Gerechtigkeitssinn
WH04	„Keine der von dir genannten Motive, tatsächlich keine, nicht mal das Finanzielle. Es ist tatsächlich eher altruistisch“ (Z.116-117) „Ich habe mich bewusst für den Weg Behörde, Militär, in meinem ersten Arbeitsleben entschieden, um zu dienen und ich wechsele jetzt einfach nur den Bedarfsträger. Und ich diene, mit dem was ich tue, habe ich die Möglichkeit, die deutsche Wirtschaft sicherer zu machen und vor allem unsere deutsche KRITIS sicherer zu machen und das ist tatsächlich mein primärer Antrieb. (Z. 118-122) „Aber wenn es um die Arbeit selber geht, dann ist es eher, dass ich die Möglichkeit habe, der deutschen Gesellschaft etwas zu geben, was es auf dem deutschen Sicherheitsmarkt nicht oft gibt, aber ein unglaublich großes Risiko in sich birgt.“ (Z. 127-130)	Motiv: Altruismus. Früher Deutschland gedient (Militär), heute Wirtschaft „dienen“ sicherer zu werden
WH04	„Dahinter gelagert ist dann das Finanzielle, weil ich als Unternehmer viel mehr Spielraum habe als noch als Soldat.“ (Z. 122-123) „Und natürlich ist mein Motiv, ich möchte es mir selber beweisen, dass ich es zivil schaffe und definitiv mehr Geld verdienen kann als damals noch als Soldat. Das ist so ein bisschen Ego.“ (125-127)	Sekundäre Motive: Geld, Ego, Selbstwirksamkeit
WH04	„Ich würde sagen, die Hälfte von meinem Team sieht die Challenge tatsächlich als Mitmotiv, zu sagen, du stehst vor einer gut gesicherten kritischen Infrastruktur und zwei Wochen später stehst du trotzdem in einem Rechenzentrum, in einer Netzleitstelle und hast es geschafft.“ (Z. 133-136)	Im Team ist „Herausforderung“ ein häufiges Motiv

Kategorie: Schuldexternalisierung

ID	Textstelle Interview	Code/ Interpretation
WH01	„Eine schwierige Frage, die sich nahtlos in die „Victim Blaming“-Debatte einreicht. Das ist vereinfacht ein elitärer Gedanke, dem ich so nicht vorbehaltlos zustimmen kann. Es liegt in der Verantwortung der (oft gierigen und inkompetenten) Plattformbetreiber, welche persönliche Daten verarbeiten oder Geld verwalten wollen, die Daten ihrer Nutzer zu schützen. Wer einen Massenmarkt anstrebt, muss seine Produkte so gestalten, dass sie intrinsisch sicher sind und darf diese Verantwortung nicht auf Kunden abwälzen. Gleichzeitig muss ein souveräner digitaler Bürger die Eigenverantwortung mitbringen, sich sicher im Internet bewegen zu können. Eine Teilschuld ist vielleicht also gegeben, was in keinem Fall die Schuld des Täters mindert. Passend wäre hier die Analogie eines Autofahrers, der bei einem nicht selbst verursachten Auffahrunfall verletzt wird, aber nicht angeschnallt war.“ (Z. 85-95)	Differenzierte Sichtweise einer Teilverantwortung
WH02	„Ja, sind sie selbst schuld. Weil ich glaube gerade die Passwortdiskussion heute eigentlich obsolet ist. Da gibt's ja technische Lösungen sozusagen.“ (Z. 141-142)	Opfer selbst Schuld, wenn schlechtes Passwort
WH02	„Wenn die Firma halt schlecht vorbereitet ist oder schlecht aufgestellt ist, darf man sich nicht wundern. Und dann ist das auch fahrlässig. Wenn da was passiert und wenn das Arbeitsplätze kostet, dann ist das total traurig, aber dann ist das 'n Problem der Geschäftsführung, die dann	Unternehmen selbst schuld

ID	Textstelle Interview	Code/ Interpretation
	nicht drauf geachtet hat oder das so ein bisschen im Blick hatte. Und da fehlt mir tatsächlich auch das Mitleid dann. Und genau, dann sind sie halt selbst schuld.“	
WH03	„Ja. Wir haben 2025 und ein grundlegendes Sicherheitsverständnis erwarte ich. Shared Passwörter, kein MFA ist ähnlich wie kein Backup, - selbst schuld.“ (Z. 55-56)	Opfer selbst schuld
WH04	„Ne, das wäre zu einfach. Also ich stimme dem so nicht zu. Ich würde das nach, wenn ich das darf, nach Bundeswehrmanier mal bewerten wollen. Ich würde jetzt unterscheiden wollen, haben wir es hier mit einem Ausbildungsmangel zu tun oder mit einem erzieherischen Mangel.“ (Z. 149-152) „Dann ist er nicht selber schuld, wenn was passiert. Wenn man es ihm schon dreimal erklärt hat und er macht es aber nicht, aus welcher Motivation auch immer, dann ist es ein Erziehungsmangel und dann hat er am Ende selber schuld, wenn was passiert.“ (Z. 154-157)	Opfer selbst schuld, wenn sie es eigentlich besser wissen, aber nicht umsetzen

Kategorie: Online- vs. Offline Persona

ID	Textstelle Interview	Code/ Interpretation
WH01	„Anonymität wäre ein großer Faktor.“ (Z. 120)	Anonymität ist wichtig
WH03	„Offline bin ich viel ängstlicher als online. Ich habe eine diagnostizierte Angststörung. Online habe ich keine Angriffsfläche.“ (Z. 77-78)	Online andere Persönlichkeits-Merkmale (weniger ängstlich)

Kategorie: Entdeckungswahrscheinlichkeit und OpSec

ID	Textstelle Interview	Code/ Interpretation
WH01	„Das kommt sehr darauf an, wer was macht. Mit perfekter Vorkehrung ist die Wahrscheinlichkeit de facto bei 0%. Allerdings ist niemand perfekt, und der Krug geht zu Brunnen, bis er bricht. (Z. 124-126)	Geringe WK bei guter OpSec
WH02	„Ja, ich würde sagen, die ist verschwindend gering, ja.“ (Z. 171)	Geringe Entdeckungs-WK
WH04	„Ja. Ich glaube, ja, wenn man seinen Job kann.“	Geringe WK bei guter OpSec

Kategorie: Kompetenz der Polizei

WH01	„Ja, die normale Polizei auf jeden Fall. Es gibt spezialisierte SOKOs, die schon etwas leisten können, meistens aber nur in Verbindung mit ausländischen Kollegen. Die deutschen Kollegen kämpfen aber auch nicht nur mit miserablen Gehältern, sondern vor allem mit einem unfassbaren Gewirr an bürokratischen Hürden..“ (Z. 134-137)	Inkompetent, außer SOKO mit int. Kooperationen
WH02	„Inkompetent finde ich ist nicht das richtige Wort. Ich glaube, sie sind einfach noch ein bisschen hinter der Zeit. Ich glaube, sie sind noch nicht soweit, wie sie sein müssten oder wie andere... Sie sind noch nicht so weit, um dem guten Black Hat wirklich das Wasser reichen zu können oder wirksam zu machen.“ (Z. 181-184)	Nicht inkompetent, aber rückständig
WH03	„Definitiv. Unsere Sicherheitsbehörden sind eine Lachnummer. Informationen zu Angriffen vom Verfassungsschutz oder vom Staat sind enorm veraltet oder die Vertrauenswürdigkeit schränkt aktiv das verteidigen ein.“ (Z. 82-84)	Inkompetent

	„Ja. Egal, ob Hate Speech, Cybercrime oder Identitätsdiebstahl. Besonders schlimm finde ich das nicht löschen von Kinderpornografie im Darknet und nur das Entfernen der Posts.“ (Z. 90-91)	
WH04	„Ich finde inkompetent ein bisschen hart. Wenn ich das abstimmen könnte von 1 bis 10 und 1 ist inkompetent und 10 wäre sehr kompetent, würde ich das, was ich über die deutschen Ermittlungsbehörden im Bereich Cybercrime weiß, würde ich die auf so 3, 4 setzen ungefähr. Von einer 10er Skala? Von einer 10er Skala. Wenn ich nur inkompetent Ja oder Nein sagen würde, würde ich sagen, wahrscheinlich eher Ja.“ (Z.183-187)	Eher inkompetent

Kategorie: Quelle der Hackingfähigkeiten/ Hacker-Karriere

ID	Textstelle Interview	Code/ Interpretation
WH01	„Ich fand Videospiele super und hatte durch „Modding“ den Einstieg gefunden. :-“ (Z. 140)	Beginn durch Computerspiele
WH01	„Selbststudium. Dazu zählen eben auch Foren, in denen man still mitlesen kann, CTFs zum Ausprobieren, und extrem viel Google. Das Darknet hat eine extrem untergeordnete Bedeutung und ich würde es nicht als Ort zum Lernen ansehen.“ (Z. 145-147)	Primär Selbststudium + Foren
WH02	„Also der Punkt war bei mir ziemlich spät, das war viel jugendlicher Leichtsinn. Also, ich hab in frühester Jugend in meiner Kindheit mit elf meinen ersten Computer gekriegt. Das war noch vor der 64er Zeit. Es war einfach Neugierde und was geht.“ (Z. 54-56) „Aber ich hab schon eine graue, oder sagen wir mal, dunkle Vergangenheit. Die ist aber schon 30 oder über 30 Jahre her. Das waren ja noch die Anfänge des Internets, wo man sich rumprobiert hat, BTX-Geschichten gemacht hat und so weiter, also so richtig Oldschool-Geschichten.“ (Z. 33-36) „Also hab ich Informatik studiert und dann war naheliegend, dass ich Security mache, weil es aus dieser Schiene herauskam.“ (Z. 64-65) „Also das war ein richtiger Freak. Und da hab ich das natürlich als kleiner Bruder übernommen, ein Stück weit, und dann haben wir halt angefangen.“ (Z. 196-197)	Früher Black Hat aus jugendlicher Neugier, dann Informatikstudium und White Hat
WH02	„[...] und dann natürlich mit Spielen da so Cheats-Geschichten zu machen oder im Kaufhaus mal alle Computer sperren. Damals konnte man ja am Computer noch rumspielen in den Kaufhäusern und solche Geschichten. Und dadurch ist das tatsächlich entstanden, weil das natürlich mega cool war. Ja, ich war da irgendwie 11, 12, 13... und da war das natürlich total mega cool, weil du auch so ein Freak warst irgendwie, ne. Und ja, so ist es auch dann historisch gewachsen, sozusagen.“ (Z. 200-205)	Beginn mit 11-13 über Tüftelerei und Cheats in Computerspielen
WH02	„Ja, Bücher, das meiste Bücher. Also Netz kam ja erst und BTX-Sachen zu Amiga-Zeiten, das war 64er-Zeiten. Da haben wir halt viel rumprogrammiert und gemacht und getan, und da gab's halt... also, weiß ich noch, Data Becker.“ (Z. 212-214)	Selbststudium damals über Bücher und Trial and Error
WH03	„Mit 10 ist mein Interesse gewachsen. Viel Videospiele, viel YouTube, erste Linux Server (für TeamSpeak etc.) wollte immer mehr wissen. 4chan. Angriffe auf Mastercard und Visa, selbst als Teen viel geddoSt.“ [Anmerkung: DDoS-Angriffe durchgeführt] Z. 95-97) „Natürliches Talent. Ich lese logs und erkenne sofort die Gefahren und für die graue Seite viel HackTheBox und Exploitdb.“ (Z. 101-102)	Beginn mit 10 über Computerspiele, dann Selbststudium, YouTube
WH04	„Hatte ich nicht. Ich hatte mich mit dem Thema auch Faktor Mensch und Kommunikation mit allem, was da dranhängt, überhaupt nicht auseinandergesetzt. Bin mit 20 zur Armee gekommen und bin mit 25 ins militärische Nachrichtenwesen gewechselt und bin dann 15 Jahre da drin geblieben.“ (Z. 194-197)	Über militärischen Nachrichtendienst (HUMINT) zum Social Engineering

ID	Textstelle Interview	Code/ Interpretation
		gekommen. Keine klassische Hacker-Karriere
WH04	„Als ich in das Thema gekommen bin, habe ich durch die Armee viele Lehrgänge bekommen, also sei es HUMINT, sei es Interrogation, sei es diese ganze Intel-Analyst und OSINT Geschichte und habe dann angefangen, das für mich als Hobby noch zu erkennen und habe mich dann mit allem, was möglich ist, weitergebildet. Also ich habe viele Bücher gelesen, ich war viel in den Auslandseinsätzen“ (Z. 210-215) „YouTube ist ein starker Kanal geworden, wo ich mir immer wieder kleine Schlüsselinformationen ziehen kann, Podcasts und der Austausch mit anderen SE-lem vor allem.“ (Z. 221-223)	Fähigkeiten über Berufliche Ausbildung, Praxis, Bücher, YouTube, Austausch

Kategorie: Rolle von Social Engineering

ID	Textstelle Interview	Code/ Interpretation
WH01	„Die meisten Formen von kriminellem Hacking können durch "Social Engineering" verbessert werden. Angreifer müssen ihre Opfer einschätzen können, um überzeugende Phishing-Mails zu verfassen.“ (Z. 158-160)	Wichtige Rolle von SE
WH01	„'Social Engineering' wird in der Szene geme von Narzissten hervorgehoben, die auf technischer Ebene keine Skills haben, aber gut labern können und unbedingt Anerkennung brauchen.“ (Z. 164-166)	Übertriebene Hervorhebung von SE
WH02	„Eine ziemlich große, oder eigentlich die Kernrolle würde ich sogar sagen, denn ich glaube, dass wir technisch gar nicht so 'n großes Problem haben.“ (Z. 246-247) „Wenn ich Adminrechte irgendwo habe, dann ist es völlig egal, welche technischen Sachen da dranhängen, ob da 'ne Firewall gut oder schlecht konfiguriert ist. Wenn ich es schaffe, jemanden dazu zu bringen, mir Adminzugang oder Rechte zu geben, ist das nicht mehr relevant. Deswegen glaube ich, ist das das Thema, das Kernthema.“ (Z. 250-254)	Wichtige Rolle von SE
WH03	„Ist das Hauptthema. Kaum ein Angriff klappt ohne Social Engineering. Wer weiß Menschen zu manipulieren, bekommt alles was er will.“ (Z. 112-113)	Wichtige Rolle von SE
WH04	„[...] aus der Perspektive heraus würde ich sagen, Social Engineering ist mit die größte Gefahr, die man zurzeit haben kann. Egal, ob du eine Multifaktor-Authentifizierung für was auch immer hast, der richtige Anruf sorgt am Ende dafür, dass du am Ende nicht nur die Credentials bekommst, sondern eben auch die PIN oder die TAN.“ (Z. 259-262) „Ich glaube, aus Marketing- und Vertriebsicht wird es oft noch ein bisschen, werden die Zahlen ein bisschen größer gemacht, als sie sind. Weil mir ist schon bewusst, dass die Angriffe grundsätzlich erstmal digital sind und dass die Unternehmen erst einmal technisch ihre Hausaufgaben machen müssen.“ (Z. 250-253)	Wichtige Rolle von SE, aber teilweise auch übertrieben

Kategorie: Rolle von KI

ID	Textstelle Interview	Code/ Interpretation
WH01	„Deepfakes könnten eine neue Masche für Einzeltrickbetrüger ermöglichen. KI ist ein nützliches Werkzeug, das ich schon häufiger zum Lernen und auch Reverse-Engineering	Gefahren durch Deepfakes, KI nützlich aber kein

ID	Textstelle Interview	Code/ Interpretation
	genutzt habe. Es ist aber derzeit keine Silver-Bullet, die ein neues Zeitalter einläuten wird. Wer ohne KI kein "Hacker" ist, ist auch mit KI kein Hacker." (Z. 151-154)	Wundermittel, das Hacking-Skills ersetzt
WH02	„Ich glaub, dass sich das auf beiden Seiten extrem, also ähnlich wie du das auch mal im Vortrag gesagt hast, extrem potenzieren wird, sag ich jetzt mal, vom Tempo her und von der Flexibilität her. Das ist so 'n bisschen: Für die Bösen sind es Chancen, aber für die Guten natürlich auch, weil sie auch, also auch wir im Unternehmen, machen ja jetzt auch schon Analysen mit KI, die dann wesentlich schneller gehen, als wenn man es von Hand und zu Fuß macht.“ (Z.224-229)	KI als Chance für Cybersicherheit und Cyberkriminalität
WH03	„Auf der weißen Seite ist es ohne KI und Algorithmen nicht mehr möglich. Menschliche Expertise kann sie nicht ersetzen. Bei Phishing zum Beispiel habe ich große Angst vor einer erhöhten Qualität durch KI.“ (Z. 106-108)	KI als Chance für Cybersicherheit und Cyberkriminalität
WH04	„Also ja, wir nutzen natürlich auch für die Recherche KI, aber gerade im Bereich SE ist KI ein unglaublicher Multiplikator. Also wir nutzen jetzt schon KI, wenn es darum geht, Vishing-Angriffe zu simulieren.“ (Z. 227-229)	KI für Recherche und Deepfake-Stimmsimulation
WH04	„Aber ich glaube, KI wird im Bereich Social Engineering uns noch, wenn ich es flapsig sagen darf, um die Ohren fliegen, weil das wirklich den Täter völlig andere Möglichkeiten gibt.“ (Z. 234-236)	KI als Chance für Cyberkriminalität

Kategorie: Narzissmus

ID	Textstelle Interview	Code/ Interpretation
WH01	„Jeder Mensch hat narzisstische Züge. Ich habe vermutlich stärker ausgeprägte narzisstische Züge als manch andere Menschen, bin aber kein klinischer Narzisst (ausdrücklich kein F60.8).“ (Z. 176-177) NARC-Score: 2.22	Hält sich für überdurchschnittlich narzisstisch, aber in Wahrheit niedriger Narzissmus-Score
WH02	„Nein, gar nicht. Das muss man vielleicht korrigieren: Früher eher... vielleicht ist mein Lebenslauf dafür auch zu hakelig, sozusagen. Also früher waren mir solche Sachen wichtig, tatsächlich, und da waren mir auch andere Menschen relativ egal und mir war Status wichtig. Ich musste dickes Auto haben und und und. Das hat sich aber quasi bei mir... ich hab ja vier Jahre in Nepal gelebt, und in der Zeit hat sich das einmal komplett um 180° gedreht, quasi. Ich hab das jetzt gar nicht mehr. Also deswegen mach ich ja auch diese Vereinsarbeit und bin jetzt genau das Gegenteil von dem, was du gerade beschrieben hast.“ (Z. 263-269) NARC-Score: 2.33	Geringer Narzissmus, Anerkennung war früher wichtiger
WH03	„Nein. Mir ist die Meinung von anderen eher egal.“ (Z. 123) NARC-Score: 3.89	Meinung anderer egal, aber eher hoher Narzissmus
WH04	„Somit hoffe ich nein. Ich hoffe, dass ich da nicht viel von habe. Ich glaube trotzdem, ich weiß nicht, ob das dann Narzissmus ist, sondern ein gesundes Selbstverständnis und Selbstbewusstsein. Kenne ich jetzt da die Schwelle nicht.“ (Z. 276-278)	Kein Narzissmus, aber gesundes Selbstbewusstsein

Kategorie: Psychopathie

ID	Textstelle Interview	Code/ Interpretation
WH01	„Ich lebe legal, um nachts ruhig schlafen zu können.“ (Z. 105-106) PSYCH-Score: 2.22	Keine Psychopathie; Gewissen/ Angst vor Strafe
WH02	Ist White Hat, engagiert sich sozial, nie das Motiv gehabt anderen zu schaden. PSYCH-Score: 2,44	Keine Psychopathie
WH03	„Nein. Privatpersonen zu bestehlen finde ich nicht in Ordnung.“ (Z. 63) „Je nach Lücke, wenn ein Unternehmen kritische Sicherheitsupdates nicht einspielt und ich mit einfachen Tests Zugriff bekommen würde, würde ich mich nicht zurück halten sollte ich diese Information haben.“ (Z. 65-67) „Ja. Unternehmen haben in der Regel genug Geld. Insbesondere aber auch in der online Welt, Lizenzen, Cracks etc.“ (Z. 69-70)	Empathie gegenüber Einzelpersonen, aber nicht bei Konzernen
WH03	„Empathie ist nicht meine Stärke. Häufig sind Menschen selber schuld.“ (Z. 132) PSYCH-Score: 3.22	Leicht erhöhte Psychopathie- Scores, wenig Empathie
WH04	„Also gemäß der Definition, die du genannt hast, wäre ich sehr schlecht in meinem Job, wenn ich nicht ein vielleicht sogar etwas höheres Maß an sozialer Kompetenz und Empathie hätte.“ (Z. 274-276) „Und denke aber, dass ich manchmal eher zu viel Empathie habe und zu viel soziale Kompetenz habe.“ (Z. 279-281)	(Zu) viel Empathie, keine Psychopathie

Kategorie: Machiavellismus

ID	Textstelle Interview	Code/ Interpretation
WH01	„Bei einem gehackten Bankkonto mit Geldabfluss ist der Geschädigte die Privatperson. Der Unterschied ist meiner Erfahrung nach den meisten Cyberkriminellen bewusst, und einigen ist er tatsächlich auch wichtig.“ (Z. 110-112) „Ich denke, in einer Notsituation wäre ich durchaus in der Lage, einen Großkonzern wie z. B. Amazon zu bestehlen, ohne Gewissensbisse zu haben.“ (Z. 113-114)	Kriminalität zu rechtfertigen in Notsituation, aber nur gegen Konzerne
WH01	„In meinem Jobtitel steht "Strategist", und ich liebe es, mein Leben sehr organisiert anzugehen. Ich versuche emotionale Handlungen und Kurzschlussreaktionen zu vermeiden, und ich versuche auch, mit jedem Menschen "auf Augenhöhe" zu sprechen. Ich habe allerdings kein "Streben nach gewissen Zielen".“ (Z. 195-198) MACH-Score: 2.44	Niedriger Machiavellismus
WH02	MACH-Score: 2.67	Niedriger Machiavellismus
WH03	„Total, mir ist egal was andere von mir halten. Ich würde über Leichen gehen meine Ziele zu erreichen. Ich habe ein sehr starkes schwarz / weiß denken und unterscheide sehr schnell zwischen Freund und Feind.“ (Z. 141-143)	Hoher Machiavellismus, Opportunismus und Einteilung in Freund vs. Feind