
© Stephan Limberg / Stine Photography

TEXT: ALEXANDER GRAU

Das Porträt: **Thomas-Gabriel Rüdiger**

Dr. Thomas-Gabriel Rüdiger war Polizist. Heute ist er Leiter des Instituts für Cyberkriminologie an der Hochschule der Polizei des Landes Brandenburg in Oranienburg. In seinen Untersuchungen befasst er sich intensiv mit Cybergrooming, Cybermobbing, Sexting, Sextortion, digitaler Hasskriminalität und der Rolle einer digitalen Polizei. Sein besonderes Anliegen ist es, den häufig sehr sozialwissenschaftlichen Blick auf Internetkriminalität um eine kriminologische und polizeiliche Perspektive zu ergänzen.

Thomas-Gabriel Rüdiger liebt seinen Beruf – und er hat eine Botschaft. Das spürt man sofort. „Wenn Sie eine Veranstaltung zu Sicherheit von Kindern im Straßenverkehr machen, denken Sie vermutlich sofort an die Polizei. Wenn hingegen eine Tagung zur Sicherheit im Internet organisiert wird, wird zuerst an Medienpädagogen gedacht, an Psychologen oder Jugendmedienschützer, aber ganz selten an die Polizei." Das will Thomas-Gabriel Rüdiger ändern. „Der Grund dafür ist, dass sich die Polizei tatsächlich mit diesen Fragen zu wenig beschäftigt. Zugleich hat man aber den Eindruck, dass viele Jugendmedienschützer mit der Situation auch ganz zufrieden sind." Auch das möchte Thomas-Gabriel Rüdiger ändern.

„Entscheidend", so Rüdiger, „ist die Mischung. Polizisten werden nicht unbedingt ein Verständnis für Medienpädagogik haben, im Gegenzug haben Medienpädagogen aber wenig Kenntnisse von Polizeiarbeit, deren rechtlichen Grundlagen wie dem Legalitätsprinzip und dem Strafrecht. Wichtig ist die Zusammenarbeit. Daher habe ich mich immer versucht dagegenzustemmen, dass bei Vorträgen, Kongressen oder ähnlichen Veranstaltungen die Polizei kaum eine Rolle spielt." Der ehemalige Polizist sieht sich daher ausdrücklich als Bindeglied zwischen Polizei und Medienschutz und versucht, die Polizeiarbeit in diese Richtung zu öffnen. Medienkompetenz sei letztlich eine Form der Kriminalprävention. Es sei daher im Interesse der Gesamtgesellschaft, nicht nur Kinder und Jugendliche, sondern alle Altersstufen fit für die Risiken und Möglichkeiten der Digitalisierung zu machen.

Kriminologie und Cyberkriminologie

Aufgewachsen ist Thomas-Gabriel Rüdiger in Berlin. Nach seinem Abitur ging er zur Polizei in Brandenburg und begann ein Studium an der Fachhochschule der Polizei in Basdorf. „Das war damals noch ein Diplomstudiengang Verwaltungswirt (FH) Polizei", erinnert sich Rüdiger. Umwege haben ihn dann vom Polizeidienst in das Innenministerium des Landes Brandenburg geführt, wo er zunächst für internationale Polizeizusammenarbeit und später auch für Gnadengesuche und Petitionen zuständig war.

Zunehmend beschäftigte sich Rüdiger aber auch mit weiterführenden Problemen: „Als klassischer Polizist ist es deine primäre Aufgabe, Straftäter zu überführen", erläutert er. „Allerdings fragt man nach wie vor zu wenig nach den Ursachen. Weshalb ist jemand zum Straftäter geworden? Hätte man das verhindern können? Was sagen Kriminalstatistiken aus? Wie schauen wir als Gesellschaft auf Kriminalität als soziales Phänomen?" Um Antworten auf seine Fragen zu finden, begann er neben seiner Arbeit ein Studium der Kriminologie an der Universität Hamburg. Insbesondere der interdisziplinäre Zugriff auf Kriminalität begeisterte ihn. In den Seminaren saßen Soziologen, Juristen, Psychologen und Pädagogen. „Das war für mein Leben ein entscheidender Einschnitt, der mich auch gedanklich noch mal weitergebracht hat."

Zugleich, erzählt Rüdiger, habe er schon damals häufig Onlinespiele gespielt, wobei ihm zahlreiche Normenbrüche aufgefallen seien, angefangen von der Beleidigung über Betrugsdelikte bis zur sexuellen Belästigung. Zusammen mit einer Kollegin habe er daher vorgeschlagen, eine Arbeit über Kriminalität im Umfeld von Onlinespielen zu schreiben. „Heute ist das mehr in der öffentlichen Wahrnehmung. Damals jedoch war das relativ neu. Zugleich war *Second Life* sehr aktuell und wir haben *Second Life*-Plattformen und Onlinespiele untersucht, inwiefern dort sexuelle Übergriffe stattfinden, Betrugsdelikte begangen werden oder sich Extremisten äußern." Veröffentlicht wurde die Arbeit unter dem Titel *Gamecrime und Metacrime. Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Welten*.

Aufgrund seiner Veröffentlichungen und seiner wissenschaftlichen Qualifikation wechselte Thomas-Gabriel Rüdiger schließlich vom Innenministerium zum Institut für Polizeiwissenschaft der Hochschule der Polizei des Landes Brandenburg (HPol) mit den Forschungsschwerpunkten Cyberkriminologie, Cyberkriminalität, digitale Polizeiarbeit und digitaler Kinderschutz. 2020 wurde er dann mit einer rechtswissenschaftlichen Arbeit über Cybergrooming am juristischen Institut der Universität Potsdam promoviert. Seit letztem Jahr leitet er das neu gegründete Institut für Cyberkriminologie an der HPol Brandenburg.

„Der Grund für die Einrichtung des Instituts war, dass die Mechanismen von Cyberkriminalität anders funktionieren als Kriminalität im physischen Raum und daher andere Ansätze benötigen." Rüdiger illustriert diese These mit einem Beispiel: In der analogen Welt seien wir in der Regel selten mit Kriminalität konfrontiert. Allenfalls Vandalismus falle hier und dort im Straßenbild auf. Anders im Internet. „Allein wenn Sie heute in Ihren Spamordner schauen, werden Sie vermutlich eine Vielzahl an Phishingmails sehen. Dahinter stehen meistens versuchte Betrugsdelikte. Schon auf dieser Ebene sind Sie also vermutlich täglich von Kriminalität umgeben, auch wenn man sich das häufig gar nicht klarmacht."

Diese hohe digitale Kriminalitätstransparenz, so Rüdiger, könne Folgen für unsere Gesamtgesellschaft haben. So sei schon jetzt erkennbar, dass die Allgegenwart von Kriminalität im Netz, von Betrugsversuchen, Hass oder Datendiebstahl zu einem Absenken der Hemmschwelle und des Problembewusstseins gerade bei Jüngeren geführt habe. Anders als im physischen Raum werde seitens der Polizei diesen Tendenzen aber nicht vergleichbar entgegengetreten. Hierfür ein Bewusstsein zu schaffen, sieht Rüdiger als einen wichtigen Teil seiner Arbeit und der des Instituts für Cyberkriminologie. Zu diesem Zweck unterhält Rüdiger auch privat Aufklärungskanäle, etwa bei Instagram.[1]

Die Broken-Web-These

Für den Cyberkriminologen ist das auch deshalb von Bedeutung, weil er die Gefahr sieht, dass digitale Kriminalität den analogen Raum entsprechend kontaminiert. Er wendet sich damit gegen den „digitalen Dualismus", wonach digitale und analoge Sphäre zwei getrennte Welten sind. Menschen würden im digitalen Raum Dinge begehen, die sie im physischen Raum nie begehen würden. Vertreten wurde diese Theorie etwa von Karuppannan Jaishankar, Doyen der Cyberkriminologie und Professor für Kriminologie am International Institute of Crime & Security Sciences in Bengaluru.

„Hass im Netz kann zur Senkung der Hemmschwelle und damit auch zu Hass auf der Straße führen."

Rüdiger hält dem entgegen, dass es zwar im digitalen Raum andere Deliktmöglichkeiten gebe, aber dennoch Einstellungen und Verhaltensmuster vom digitalen in den analogen Raum hinüberfluten und die Gesellschaft negativ verändern könnten. „Die Kriminalität in den jeweiligen Sphären beeinflusst sich gegenseitig. Hass im Netz kann zur Senkung der Hemmschwelle und damit auch zu Hass auf der Straße führen, insbesondere wenn der jeweilige Akteur den Eindruck bekommt, seine Straftaten würden nicht sanktioniert."

Jeder Mensch, betont der Kriminologe, werde in seinem Leben irgendwann auch rechtliche Normen brechen, auch wenn uns das häufig nicht bewusst sei. Anders als im analogen Raum, wo Gesetzesverstöße häufig gar nicht wahrgenommen würden, seien sie uns im digitalen Bereich sehr viel näher und präsenter. Hier würden wir permanent mit Kriminalität konfrontiert. Dadurch bestehe die Gefahr einer gewissen Abstumpfung und zudem der Eindruck, dass das Internet ein rechtsfreier Raum sei.

Rüdiger verweist in diesem Zusammenhang auf den Soziologen Heinrich Popitz, der schon in den 1960er-Jahren darauf aufmerksam gemacht hat, dass das Nichtwissen über die tatsächliche Präsenz von Kriminalität eine Präventionswirkung hat, da die Menschen sich so an die – allerdings nur scheinbar – funktionierenden Regeln halten. „Im Netz", erklärt Rüdiger, „ist diese Prävention durch Nichtwissen jedoch durchbrochen. Das Dunkelfeld an Kriminalität wird sichtbar. Da der durchschnittliche Deutsche heutzutage mehr Zeit im Netz als auf der Straße verbringt, besteht somit die Gefahr, dass die Kriminalitätserfahrung im Internet auf die analoge Realität übertragen wird und hier zunehmend Tabus fallen."

So habe das Landeskriminalamt von Nordrhein-Westfalen schon 2013 in einem Lagebericht zu Cybercrime betont, dass Kinder und Jugendliche sexuelle Übergriffe im Netz als so normal empfinden, dass sie es nicht mehr als strafbar ansehen. „Auch der derbe und eben teilweise auch strafbare Sprachgebrauch bei Onlinespielen gehört für viele Jugendliche einfach zur Normalität – und das hat Folgen für den Umgang in der analogen Welt." Angelehnt an die Broken-Windows-Theorie spricht Rüdiger in diesem Zusammenhang von der Broken-Web-These. „Verstärkt wird dieser Effekt noch dadurch, dass es im Netz keine sichtbare Normkontrolle gibt. In der Realität begegnen Sie hin und wieder Polizeistreifen. Im Netz hingegen gibt es kaum bis keine sichtbaren Ordnungshüter. Das ist wie in einem Straßenverkehr, wo jeder weiß, dass es keine Polizeistreifen gibt und keine Geschwindigkeitskontrollen. Die Einhaltung der Regeln wäre vermutlich wesentlich laxer, als es schon jetzt mit diesen Formen der Normenkontrolle ist." Die Sichtbarkeit der Polizei unterstreiche letztlich die Bereitschaft und auch die Möglichkeit, das Gewaltmonopol des Staates durchzusetzen. Im Netz fehle so etwas. „Meiner Meinung nach brauchen wir daher analoge Formen sichtbarer und ansprechbarer Polizeistreifen im Netz."

Medien- und Strafrechtskompetenz stärken

Eine Klarnamenpflicht hält der Kriminologe hingegen in diesem Zusammenhang für weniger sinnvoll. Verschiedene Studien würden zeigen, dass eine Klarnamenpflicht beispielsweise nicht per se zu einer Absenkung der Hasskriminalität führe. Und bei Cybergrooming oder anderen Sexualdelikten sei die Identifizierung der Täter keine große Herausforderung: „Bei Cybergrooming hatten wir eine Aufklärungsquote von knapp 84 % in der Polizeilichen Kriminalstatistik (PKS) 2021. Das Problem liegt aber darin, dass die allermeisten Delikte nicht zur Anzeige kommen." Bei Ladendiebstählen liege das Verhältnis von begangenen und angezeigten Fällen bei etwa eins zu zehn und sei damit für die analoge Welt vergleichsweise hoch. Im Netz hingegen lägen die Quoten bei digitalen Delikten deutlich im dreistelligen Bereich. Allerdings, gibt Rüdiger zu bedenken, habe auch die Politik nicht immer ein Interesse an einer höheren Anzeigenquote, denn das habe eine massiv steigende Kriminalitätsrate zur Folge. „Die insgesamt sinkenden Kriminalitätszahlen der letzten Jahre zeigen u.a. lediglich, dass sich Kriminalität von der Straße in das Netz verlagert und dort aber kaum zur Anzeige kommt."

Die niedrige Anzeigenquote im Netz hat eine Reihe organisatorischer und praktischer Gründe. So gibt es keine einheitlichen und zentralen Internetwachen, die Zuständigkeit ist, anders als bei Kriminalität auf der Straße, häufig unklar – und die vorhandenen Portale bei der Polizei sind nicht immer nutzerfreundlich. „Im Grunde", fasst Rüdiger zusammen, „fehlt es der Polizei in Deutschland an entsprechenden Strukturen und einer grundlegenden digitalen Strategie. Die Hälfte der Polizeiarbeit besteht beispielsweise in der sogenannten polizeilichen Gefahrenabwehr. Die erfordert aber eine örtliche Zuständigkeit. Dafür ist die jeweilige Landespolizei in ihrem Bundesland zuständig. Wo aber verläuft die Landesgrenze von Bremen, Bayern oder Brandenburg im Netz? Das Ergebnis: Die Hälfte der Polizeiarbeit findet im Netz kaum bis gar nicht statt."

Gewaltprävention ist allerdings nicht nur Aufgabe der Polizei, sondern jedes Bürgers. Das fängt schon beim klassischen Mobbing an. Zu diesem Zweck unterscheidet der Kriminologe zwei Formen von Mobbing. Das schulische Mobbing in sozialen Netzwerken sei eine Fortsetzung von Schulmobbing und müsse daher primär auf der Schulebene gelöst werden. Interessanter aus Sicht des Cyberkriminologen ist es, wenn Menschen aufgrund ihrer Selbstdarstellung auf sozialen Plattformen aus der Anonymität des Netzes heraus angegriffen werden. „Wir alle neigen zu einem gewissen digitalen Narzissmus. Also dazu, uns im Netz zu inszenieren, um Aufmerksamkeit zu erzeugen. Das lernen schon Kinder und Jugendliche gerade durch die Mechanismen sozialer Medien."

„Aufgrund der Rechtslage rate ich dazu, auch im privaten Bereich sensibel zu agieren. Selbst ein Bikini-Bild der 12-jährigen Tochter könnte den Anfangsverdacht von Kinderpornografie auslösen."

Das führe allerdings dazu, dass relativ ungesteuert Informationen von den Menschen preisgegeben würden. Hinzu komme, dass selbst viele Erwachsene nicht erkennen würden, wo die Probleme in ihrer Selbstdarstellung liegen. „Bei Schulmobbing sind die Verantwortlichen zumeist leicht zu identifizieren. Bei Shitstorms in sozialen Medien – und Shitstorms kann man auch als Form von Cybermobbing erfassen – geht aber meist irgendein Post anonym viral. Das bekommen Sie nicht mehr in den Griff. Das lässt sich nur präventiv eingrenzen. Hier braucht es bei den Nutzern selbst das nötige Problembewusstsein und die entsprechende Medienkompetenz."

Eine Schlüsselfunktion bei der Erziehung kommt für Rüdiger den Schulen zu, da es immer Eltern gebe, die entweder keine Zeit hätten, kein Problembewusstsein oder keine Lust, ihren Kindern die Regeln des Internets zu vermitteln. „Im Straßenverkehr würden sich Eltern ja auch nicht von ihren Kindern die Verkehrsregeln erklären lassen. Im Internet aber werden die Kinder aus vielerlei Gründen häufig alleingelassen und übernehmen dann die Regeln, die sie dort lernen, die aber mit unseren gesellschaftlichen Vorstellungen und Gesetzen nicht immer übereinstimmen."

Allerdings weist Thomas-Gabriel Rüdiger auch darauf hin, dass Medienkompetenz keine Einbahnstraße ist. Nicht nur Nutzer, unabhängig vom Alter, müssten lernen, dass das Internet kein rechtsfreier Raum ist, auch der Gesetzgeber müsse realisieren, dass das Netz mitunter anders funktioniert als die analoge Realität. Ein klassisches Beispiel dafür sei das Thema „Verbreitung von Kinderpornografie". „Noch vor wenigen Jahren hätten wir uns den durchschnittlichen Täter als einen erwachsenen Mann vorgestellt, der einsam vor seinem Rechner sitzt. Und das war vor wenigen Jahren auch berechtigt. Seit vier Jahren haben wir aber jährlich fast eine Verdopplung der Fallzahlen bei Kindern und Jugendlichen als Tatverdächtige bei der Begehung über das Tatmittel Internet. Inzwischen sind wir bei 54 % minderjähriger Tatverdächtiger angelangt."

Ursache für diesen rapiden Anstieg sei auch die Gesetzeslage. Wenn etwa ein 13-jähriges Mädchen ihrem Freund ein Nacktfoto schicke, sei das Kinderpornografie. Wenn das Mädchen 14 werde und das Foto noch immer auf ihrem Smartphone hätte, könnte sie sich aufgrund ihres eigenen Bildes ebenfalls der Kinderpornografie schuldig machen. Ein weiteres Problem seien jugendliche Chatgruppen, in denen aus vermeintlich harmlosem Spaß heraus Fotos mit entsprechendem Inhalt weitergegeben würden. Über automatische Download-Funktionen hätten dann unter Umständen ganze Klassen unbeabsichtigt kinderpornografische Inhalte auf den Handys. Wenn aufgrund polizeilicher Arbeit auch die Eltern in die Ermittlungen einbezogen würden, könnte das, auch wenn der Sachverhalt selbst harmlos sei, gravierende Folgen für alle Beteiligten haben.

„Das Problem ist, dass die Polizei das nicht gewichten darf, sondern gezwungen ist, auch harmlosen oder auf Unkenntnis beruhenden Delikten in vollem Umfang nachzugehen. Das blockiert die eigentliche Polizeiarbeit und kann für die Betroffenen unangenehme Folgen haben." In diesem Bereich sei auch die Medien- und Rechtskompetenz von Erwachsenen oft unterentwickelt. So warnt Rüdiger etwa Lehrer ausdrücklich davor, zur Beweissicherung Screenshots einschlägiger Fotos von Schülerhandys anzufertigen. Auch das sei Besitz oder die Anfertigung von sogenannter Kinderpornografie und ein Verbrechenstatbestand. Solche Beweissicherung dürfe erst nach ausdrücklicher Rücksprache mit der Polizei erfolgen.

„Aufgrund der Rechtslage rate ich dazu, auch im privaten Bereich sensibel zu agieren. Selbst ein Bikini-Bild der 12-jährigen Tochter könnte den Anfangsverdacht von Kinderpornografie auslösen." Das Problem sei dabei weniger eine tatsächliche Verurteilung, sondern der individuelle soziale Schaden. „Die Polizei hat selbst keine Einstellungsmöglichkeiten. Sobald ein Sachverhalt als Kinderpornografie gekennzeichnet ist, muss die Polizei, bedingt durch das sogenannte Legalitätsprinzip, handeln. Das kann im Ergebnis bedeuten, dass die Polizei im schlechtesten Fall frühmorgens eine Hausdurchsuchung macht und die Nachbarn das mitbekommen. Dagegen hilft vor allem Aufklärung." Hier fehle in der Bevölkerung die Strafrechts- und Medienkompetenz. „Früher gab es im Fernsehen das Verkehrserziehungsformat *Der 7. Sinn*. So etwas bräuchten wir im Grunde genommen für Medienthemen."

Anmerkung:

1 Vgl. https://www.instagram.com/cyberkriminologe

Dr. Alexander Grau arbeitet als freier Kultur- und Wissenschaftsjournalist u.a. für „Cicero", „NZZ" und den Deutschlandfunk.