Fachhochschule
Polizei Brandenburg

ORANIENBURGER SCHRIFTEN

Beiträge aus der Fachhochschule der Polizei des Landes Brandenburg

Sonderausgabe 2013

AUS DEM INHALT

Inhalt

Editorial

Sehr geehrte Damen und Herren,

für einen Präsidenten einer Hochschuleinrichtung der Polizei ist es immer eine besondere Freude, eine wissenschaftliche Publikation seines Hauses in den Händen zu halten. Bereits seit dem Jahr 2007 veröffentlicht die Fachhochschule der Polizei des Landes Brandenburg regelmäßig ein deutschsprachiges Wissenschaftsheft, die Oranienburger Schriften. Diese widmen sich im Rahmen von jeweiligen Themenschwerpunkten aktuellen, für die Polizei relevanten Phänomenlagen.

Hin und wieder kann dabei aber die Erkenntnis reifen, dass ein Themenfeld aufgeworfen wird, dessen Bedeutung von einer größeren, einer internationaleren Dimension ist, als es eine deutschsprachige Publikation abspiegeln kann. Aus unserer Sicht behandelt die vorliegende Ausgabe wissenschaftlich gesehen genau ein solches, bisher weitestgehend unbekanntes Thema.

Mit Unterstützung unseres Innenministers, Herrn Dr. Dietmar Woidke, haben wir uns daher entschieden, diese Ausgabe erstmalig auch auf Englisch zu publizieren, um einem möglichst breiten Publikum die Erkenntnisse zur Viktimisierung von Minderjährigen in virtuellen Welten durch Sexualtäter näher zu bringen.

Ich hoffe, dass der eine oder andere Leser diese Publikation zum Anlass nimmt, um mit uns in einen wissenschaftlichen Austausch zu treten. Ich würde mich darüber sehr freuen.

Ihr

Rainer Grieger
Präsident der Fachhochschule der Polizei
des Landes Brandenburg

Vorwort
Minister des Innern des Landes Brandenburg

Sehr geehrte Damen und Herren,

am 19. September 2012 richtete das Innenministerium in der Vertretung des Landes Brandenburg in Brüssel eine Tagung zu den Risiken virtueller Welten aus. Mit dieser Tagung sollten sowohl die Europäische Kommission, als auch das Europäische Parlament und weitere an dieser Thematik Interessierte für die Gefahren, die bei der Nutzung von sog. Online-Spielen – u.a. durch Sexualtäter – Minderjährigen drohen, sensibilisiert werden. Ich hielt die Durchführung dieser Tagung für geboten, da es auch die ureigenste Aufgabe der Politik ist, sich bei offensichtlichen Missständen für eine Besserung einzusetzen. Die vielen positiven nationalen wie internationalen Reaktionen und das Medienecho bestätigten mich in meiner Annahme, dass die Durchführung einer solchen Veranstaltung notwendig und sinnvoll war.

Umso erstaunter war ich, dass bisher kaum jemand ernsthaft die Gefahren der Nutzung von virtuellen Welten durch Sexualtäter und den damit einhergehenden mangelnden Kinder- und Jugendschutz thematisiert hat. Trotz dem für viele Kinder und Jugendliche die Nutzung von Online-Spielen die Medienrealität darstellt und diese je nach Altersstufe teilweise beliebter sind als Chat-Räume, fehlt nach wie vor eine noch intensive Auseinandersetzung mit den Risiken. Dabei sprechen wir nicht darüber, ob diese Spiele gewalthaltige oder pornografische Inhalte haben, wir sprechen darüber, dass sich damit auseinander gesetzt werden muss, wer mit wem in solchen Welten spielt, interagiert und kommuniziert. Es ist daher notwendig, die bisherigen Sicherheitsmechanismen in solchen Spielen kritisch zu hinterfragen und in einen internationalen – einen europäischen - Kontext zu setzen. Hierbei müssen sowohl die Betreiber als auch die zuständigen Einrichtungen im Bereich des Kinder- und Jugendschutzes in die Pflicht genommen werden, ihre bisherigen Sicherheitsvorkehrungen zu überdenken. Neben diesen technischen und politischen Maßnahmen müssen die Nutzer und insbesondere auch Eltern und Erziehungsberechtigte für diese Risiken sensibilisiert werden. Dies ist aus meiner Sicht notwendig, damit sich Eltern mit ihren Kindern dem verantwortungsvollen Umgang mit dem Internet stellen können.

Diese Publikation kann einen Teil dazu beitragen, dass wir einerseits Minderjährigen einen möglichst gefahrfreien Umgang mit dem Internet ermöglichen und andererseits neue Ideen für das Tätigwerden von Sicherheitsbehörden in den Bereichen der Strafverfolgung aber insbesondere der Prävention aufzeigen können. Ich hoffe, dass diese Sonderausgabe der Oranienburger Schriften dabei helfen wird, eine Sensibilisierung für diese Risiken zu bewirken.

Ihr
Dr. Dietmar Woidke

Minister des Innern
des Landes Brandenburg

Sexualtäter in virtuellen Welten

Thomas-Gabriel Rüdiger, M.A.

Abstract
Virtuelle Welten und insbesondere Online-Spiele werden jedes Jahr von immer mehr Menschen gespielt. Allein das bekannte Online-Spiel World of Warcraft konnte zu Hochzeiten 12 Millionen Menschen zum Spielen animieren. In Deutschland spielen bereits 16 Millionen Menschen online. In virtuellen Welten treffen Menschen jeglichen Alters und Geschlechts in einer spielerischen Interaktion aufeinander, ohne stets genau zu wissen, wer tatsächlich der jeweilige Mitspieler ist. Ein Bruchteil nutzt diese Anonymität und das intime Interaktionserlebnis aus, um dabei sexuelle Kontakte mit Minderjährigen anzubahnen. Dabei können primär zwei Tätertypen unterschieden werden. Einen offen agierenden Erpresser-Typus und einen konspirativ vorgehenden Guten-Freund-Typus. Beide Tätertypen nutzen aber die Besonderheiten virtueller Welten aus, um z.B. durch das Anbieten von virtuellen Gütern Kinder zu sexuellen Handlungen zu verleiten. Diese Vorgehensweise wird durch Jugendschutzgesetze ermöglicht, die noch nicht an die Interaktions- und Kommunikationsrisiken von Spielen angepasst sind und durch mangelndes Wissen von Eltern und der gesellschaftlichen Institutionen über das Medium.

"In online games where you can get some bonus points. When a child meets someone unknown in such game and that person offers him or her buying those points if the child sends him some naked photos."

1. Einleitung

"In online games where you can get some bonus points. When a child meets someone unknown in such game and that person offers him or her buying those points if the child sends him some naked photos."

Die Eingangsaussage dieses Artikels stammt von einem 12jährigen Jungen aus der Tschechischen Republik und kann einem offiziellen Bericht des Forschungs-Projektes „EU Kids Online" entnommen werden (Livingstone et.al, 2011-1).

In nur zwei Sätzen beschreibt der Junge eindrucksvoll seine Erfahrungen mit dem Phänomen des sogenannten Cybergrooming während der Nutzung von Online-Spielen. Dabei sind dies nicht die einzigen Schilderungen von Sexualtätern in virtuellen Welten, die offiziellen EU-Berichten entnommen werden können. Bereits in demselben Report berichtet ein elfjähriger Junge aus Belgien: "I was playing a game with [my friend] online and we bumped into something like sex and it was all over the screen" (ebd.). In einem Folgebericht desselben Forschungsprojektes beschreibt ein 15jähriges Mädchen aus der Türkei ihre Erfahrungen wie folgt: "When I am playing games with my older sister on the internet, naked people pop up and it is very bad" (Livingstone et. al, 2011-2).

Obwohl diese Schilderungen eindrucksvoll die Risiken der sexuellen Belästigungen in virtuellen Welten insbesondere für Minderjährige darlegen, erfolgte bisher noch keine weitergehende politische oder wissenschaftliche Auseinandersetzung mit diesem Phänomen. Der nachfolgende Artikel soll sich daher dieser besonderen onlinebasierten Vorgehensweise von Sexualtätern annehmen und virtuelle Welten als Rahmen für Sexualdelikte problematisieren. In einem ersten Schritt werden zunächst die für ein Verständnis der Gesamtthematik notwendigen sozialen, ökonomischen und technischen Mechanismen virtueller Welten beschrieben, um diese im nächsten Schritt mit grundlegenden Erkenntnissen zu Cybergrooming-Prozessen zu verknüpfen. Auf diese Aus-

gangslage zurückgreifend sollen in einem abschließenden Schritt begünstigende oder hemmende Faktoren herausgearbeitet und erste Forderungen zu einem besseren Kinder- und Jugendschutz im Internet formuliert werden.

2. Virtuelle Welten

Die Nutzung des Internets ist aus der Lebensgestaltung von weltweit bereits mehr als zwei Milliarden Menschen nicht mehr wegzudenken (Pingdom, 2012). Das Internet durchdringt dabei fast jeden Aspekt menschlichen Handelns und zwischenmenschlicher Interaktionen. Die Menschen nutzen die Möglichkeiten, die ihnen durch das Internet eröffnet werden in mannigfaltigster Form – vom Online-Shopping über virtuelle Kontakttreffs bis hin zur Hintergrundrecherche. Ein ganz entscheidender wirtschaftlicher und kultureller Einflussfaktor ist dabei aber die Ausgestaltung des Freizeitverhaltens. Dieses wird immer stärker von der Nutzung Sozialer Medien geprägt, zu denen nicht nur die klassischen Sozialen Netzwerke wie Facebook, Xing und Google Plus sowie Videoplattformen wie YouTube und MyVideo, sondern auch sogenannte virtuelle Welten zu zählen sind.

Das wirklich besondere an virtuellen Welten ist, dass Millionen von Menschen weltweit mit und über ihre Spielfiguren interagieren und kommunizieren, was tagtäglich Myriaden von sozialen Prozessen generiert.

Virtuelle Welten stellen eine Form von programmierten gedanklichen (Fantasie-) Welten dar, in denen eine große Anzahl von Menschen miteinander interagieren können (z.B. kommunizieren, handeln, spielen, kämpfen, singen, tanzen). Zur Verbildlichung dieser Interaktion bewegen sich die Nutzer in der Mehrzahl der virtuellen Welten mit verbildlichten und interaktiv steuerbaren Abbildern ihrer selbst – den sogenannten Avataren[1]. Eine verbindliche wissenschaftliche Definition für virtuelle Welten konnte sich bisher noch nicht etablieren, jedoch werden zur Abgrenzung üblicherweise die Merkmale Immersion – das emotionale Einsinken in der Umgebung welches zumeist durch den Avatar realisiert wird –, Persistenz – die Weiterentwicklung der Welt unabhängig von der Frage, ob der Nutzer online ist – sowie Konsistenz – alle Nutzer können dasselbe wahrnehmen – genutzt (Meyfarth, 2007). Das wirklich besondere an virtuellen Welten ist, dass Millionen von Menschen weltweit mit und über ihre Spielfiguren interagieren und kommunizieren, was tagtäglich Myriaden von sozialen Prozessen generiert. Wie jede andere zwischenmenschliche Interaktion auch, können diese Prozesse sowohl positive als auch negative Auswirkungen haben.

Gegenwärtig unterteilt die Wissenschaft virtuelle Welten in Metaversen und Onlinegames. Metaversen, die auch als Lebenssimulationen (Lifesimulations) bezeichnet werden, kennzeichnet, dass diese dem Nutzer kein direktes Spielziel vorgeben oder bieten möchte. Vielmehr stehen die sozialen Interaktionsprozesse – wie bei den klassischen sozialen Netzwerken – der Nutzer im Mittelpunkt des Erlebens. Eine der bekanntesten Metaversen ist Second Life, das insbesondere 2007 für einen regelrechten Internethype gesorgt hat. Second Life versucht das Leben in all seinen Facetten virtuell nachzubilden (Krebs & Rüdiger, 2010). Linden Labs, der Betreiber von Second Life, konnte aber auch noch für das Jahr 2012 bekanntgeben, dass täglich immerhin 80.000 Menschen online sind und insgesamt bereits 32 Millionen Avatare – sog. Residents – erstellt worden sind (Dwell, 2012). Das Besondere an Second Life ist aber, dass die Nutzer Inhalte (sog. Usercontent) selbst erstellen und diese in die Welt integrieren, nutzen und sogar verkaufen können. Dies hat auch dazu geführt, dass schwerste Gewalt- und Sexualhandlungen (u.a. das sog. „Dolcett Plays“) in Second Life durch einige Nutzer programmiert und interaktiv erlebbar gemacht wurden (Rüdiger, 2013-1). Neben Second Life gibt es noch mehrere Vertreter dieser Sparte wie There, Secret City oder das für Facebook programmierte Cloud

1 Der Begriff „Avatar“ stammt aus dem hinduistischen Sanskrit und bedeutet in etwa ein auf Erden wandelnder Gott (Erenli 2008, S.4).

Party. Zu dem Bereich der Metaversen kann man auch sogenannte 2D- und 3D-Communitys zählen wie Habbo Hotel, Smeet, Freggers oder Club Coee. Diese Welten versuchen, die Erfahrung von Sozialen Netzwerken mit interaktiven grafischen Oberflächen und unter Nutzung von Avataren vor allem für Minderjährige erlebbar zu machen.

Onlinegames hingegen setzen klar auf das spielerische Element. Das bedeutet, dass den Nutzern – egal in welcher Form – Ziele und Aufgaben vorgegeben werden, die sie alleine oder gemeinsam erfüllen müssen oder können. Um diese Spiele für eine möglichst große Zielgruppe attraktiv zu gestalten, gibt es unterschiedlichste Spielkonzepte und grafische Ausgestaltungen. Die wohl bekanntesten Vertreter von Onlinegames sind sogenannte Massively Multiplayer Online Role Playing Games (MMORPGS). In diesen spielen teilweise Millionen von Menschen in einer zumeist mittelalterlich anmutenden Fantasywelt[2] mit ihren optisch individuell anpassbaren Avataren miteinander. Blizzard, der Betreiber des kommerziell und sicherlich medial auch erfolgreichsten MMORPG´s World of Warcraft, konnte in einer Pressemitteilung bereits am 7. Oktober 2010 verlautbaren, mittlerweile mehr als zwölf Millionen zahlende Nutzer verbuchen zu können (Blizzard, 2010). Im Zusammenhang mit dem Siegeszug mobiler internetfähiger Endgeräte haben sich auf dem Markt zudem sogenannte Browser- und Socialgames etablieren können. Diese sind meistens im Bereich der Strategiespiele anzutreffen, bei denen entweder ein Land, eine Stadt oder ähnliches aufgebaut und gepflegt werden muss oder auch im Rahmen einer Variation, bei der die Weiterentwicklung des Avatars im Mittelpunkt steht. Von Socialgames spricht man dann, wenn entweder das Spiel direkt in einem sozialen Netzwerk integriert ist – ein bekanntes Beispiel hierfür ist das in Facebook integrierte Farmeville – und oder das Spielkonzept darauf aufbaut, dass man möglichst immer wieder seine eigenen Kontakte in den sozialen Netzwerken zum Mitspielen animiert. Knapp 15 Prozent des Milliardenumsatzes von Facebook soll durch Spiele der Firma Zynga, die auf dieses Konzept setzen, generiert werden (Tagesspiegel, 2012). Ein weiteres wichtiges Genre sind onlinebasierte Multiplayerparts von Computer- und Videospielen. Gegenwärtig erscheint fast kein klassisches datenträgerbasiertes Spiel mehr ohne die Möglichkeit, per Internet gegen oder mit anderen zu spielen. Für viele Spieler ist dieser Aspekt mittlerweile der eigentliche Kaufgrund. Beliebt sind in diesem Zusammenhang insbesondere die sogenannten First Person Shooter – wie die Call of Duty oder Battlefield Reihe – oder Sportspiele – wie die FIFA und PES Fußballreihen.

Den Einfluss, den solche virtuelle Welten auf die gegenwärtige Medienlandschaft und -nutzung tatsächlich ausüben, kann am ehesten an den aktuellen Nutzerzahlen abgelesen werden. Demnach spielen allein in Deutschland bereits ca. 24 Millionen Menschen Computerspiele (Bitkom, 2012). Etwa jeder fünfte Deutsche – insgesamt also ca. 16,5 Millionen Menschen – spielt online (BIU, 2012). Eine für Deutschland repräsentative Studie hat zudem ergeben, dass im Jahr 2012 66 Prozent der 6-9jährigen und 75 Prozent der 10-13jährigen ihre Freizeit mit Online-Spielen verbrachten (KidsVA, 2012). Hingegen nutzten der KIM Studie 2010 zu Folge in Deutschland nur 15 Prozent der 6-9jährigen und 50 Prozent der 10-13jährigen regelmäßig Chat-Räume (KIM, 2010). Die aktuelle technische Entwicklung wird dabei die Anzahl der aktiven Computerspieler vermutlich nochmals in den nächsten Jahren erhöhen. Insbesondere die Verbreitung von Smartphones und Pads – die letztlich ja mobile Minicomputer darstellen – tragen diesen Trend. Bereits im ersten Quartal 2012 war jedes dritte Mobilfunkgerät in

Eine für Deutschland repräsentative Studie hat zudem ergeben, dass im Jahr 2012 66 Prozent der 6-9jährigen und 75 Prozent der 10-13jährigen ihre Freizeit mit Online-Spielen verbrachten (KidsVA, 2012).

2 MMORPGs können eine Vielzahl von Settings aufweisen, von Sciencefiction- über Horror- bis zu Agentenszenarien.

Deutschland ein Smartphone (Pakalski, 2012). Smartphones sind dabei nicht nur für Erwachsene als Zielgruppe relevant, denn immerhin 63 Prozent aller Kinder besitzen ein eigenes Handy und jedes fünfte ein internetfähiges Smartphone (YouGov, 2012). Diese Zahlen berücksichtigen dabei jedoch noch nicht die Anzahl der Minderjährigen, die z.B. bei Fahrten im öffentlichen Nahverkehr oder bei Familienfeiern Smartphones oder Tablets von Verwandten oder Bekannten zum Zeitvertreib nutzen dürfen. Die gegenwärtige Verbreitung von Smartphones geht einher mit einem Angebot an immer preisgünstigeren Internet-Flatrate-Tarifen. Betreiber von virtuellen Welten haben diesen Trend erkannt und setzen immer stärker auf Produkte, die ein gemeinsames Spielen auf mobilen Endgeräten ermöglichen. Dies spricht wiederum besonders Gelegenheitsspieler – sog. Casual Gamer – und Kinder an (Bitkom, 2012-1). Eine Studie stellte für das Jahr 2012 fest, dass bereits 73 Prozent aller Kinder in Deutschland auf einem Handy oder Smartphone spielen (ebd.). Eine andere europäische Studie kommt zu dem Schluss, dass die ersten Erfahrungen die die gegenwärtige Generation von Kindern mit dem Internet macht, überwiegend auch über das Medium der Online-Spiele erfolgen (Livingstone et.al, 2011-2, S. 14).

Eine andere europäische Studie kommt zu dem Schluss, dass die ersten Erfahrungen die die gegenwärtige Generation von Kindern mit dem Internet macht, überwiegend auch über das Medium der Online-Spiele erfolgen (Livingstone et.al, 2011-2, S. 14).

3. Ökonomische Betrachtung

Die Hersteller von virtuellen Welten haben vornehmlich das Ziel, einen möglichst großen Umsatz mit ihren Produkten zu erwirtschaften. Traditionell setzten die Betreiber in der Vergangenheit auf ein Finanzierungskonzept, das sich über etwaige Anschaffungskosten sowie eine fixe monatliche Grundgebühr refinanzierte. Insbesondere diese Grundgebühr versprach bei erfolgreichen Spielen einen immensen Gewinn. Annähernd eine Milliarde US–Dollar erwirtschaftete beispielsweise Blizzard im Jahr 2010 mit der ungefähr 12 Euro teuren monatlichen Grundgebühr von World of Warcraft (PCGames, 2012). Der Gedanke hinter der monatlichen Grundgebühr und diesem als „Pay to Play (P2P)“ bezeichneten Finanzierungsmodell ist, dass der Nutzer regelmäßig für die eigentliche Nutzung bezahlt und dem Betreiber somit planbare Einnahmen beschert. Teilweise wird diese monatliche Grundgebühr noch dadurch erhöht, dass der Nutzer für virtuelle Gegenstände (sog. Items) oder spezielle Zusatzleistungen Geld bezahlen kann.

Gerade der Verkauf von Items hat sich in den letzten Jahren zu einem eigenen hoch rentablen Finanzierungsmodell entwickelt. Dieses Modell wird in der Werbung immer wieder als „gratis“ oder auch „free“ bezeichnet. Von daher leitet sich auch die Modell-Bezeichnung „Free to Play (F2P)“ ab. Bei diesem Prinzip wird das eigentliche Spielen für den Nutzer tatsächlich kostenlos ermöglicht. Der Umsatz wird dann durch den Verkauf von Items (z.B. Schwerter, Möbel, Haustiere, Rüstungen) oder speziellen Zusatzleistungen erwirtschaftet. Die Spiele werden dabei so programmiert, dass der Spieler zu Beginn sehr schnell in das Spielgeschehen einsteigen kann, erste Erfolgserlebnisse verzeichnet und so zum Weiterspielen animiert wird. Konkret könnte ein F2P-Browsergame mit einer strategischen Ausrichtung so strukturiert sein, dass der Nutzer eine mittelalterliche Stadt und eine zugehörige Armee aufbauen soll. Zu Beginn dauert die Bauzeit von Häusern zur Erhöhung der Einwohnerzahl nur wenige Sekunden, mit fortlaufender Spieldauer kann sich diese Zeit schon einmal auf mehrere Tage verlängern. Im Gegenzug wird dem Spieler aber angeboten, diese Zeitdauer durch die Bezahlung von Geld zu verkürzen. Dieses Geld wird wiederum kundenfreundlich mit mystischen Begriffen wie z.B. „Zaubermünzen“ oder „Edelkristalle“ umschrieben. Der Nutzer muss diese virtuellen Währungen aber vor dem Einsatz über echtes Geld erkaufen. Hierfür stehen zumeist Bezahlmethoden wie Kreditkarte, Paypal oder Paysafecard zur Verfügung. Viele Spiele setzen aber auch auf ein telefonisches Bezahlmodell. Hierbei

kann der Nutzer im Spiel angeben für wieviel Geld er virtuelle Währungen kaufen möchte, wobei einige Spiele diesen Wert zeitweise in der Höhe und der Häufigkeit beschränkt haben. Im nächsten Schritt bekommt er eine individuelle mehrstellige Nummer zugeschrieben und muss bei einer meist kostenpflichtigen Service-Hotline (0900 Nummer) anrufen oder eine SMS zu einer solchen senden. Nach Eingabe dieser Nummer wird der vorher festgelegte Betrag von der Telefonrechnung des Anschlussinhabers abgebucht[3] . Auf ähnliche Weise funktioniert auch der Kauf von Items in F2P-MMORPG. Der Hintergrund hierbei ist, dass bei MMORPGs die Nutzer durch das Besiegen von Gegnern (zumeist Monstern) und dem Lösen von Herausforderungen stetig stärker werden und ihnen quasi als Belohnung Ausrüstungsgegenstände, die sie wiederum auch stärker machen, geschenkt bekommen. Üblicherweise unterliegen die Items, die die besiegten Monster hinterlassen (sog. droppen), einem Zufallsfaktor. Zu Beginn des Spiels, also in der Erfolgsphase, können Items noch häufiger gefunden werden und haben auch einen der Spielstufe angemessenen Mehrwert. Je länger ein Spieler jedoch spielt, umso seltener werden insbesondere starke und leistungsfähige Items gedroppt. Items wie Waffen oder Rüstungen sind, wenn sie getragen werden, an dem jeweiligen Avatar sichtbar. Somit werden der Status, der Erfolg und vor allem die im Spiel verbrachte Zeit anderen Mitspielern durch das Tragen entsprechender Items angezeigt. Je länger sich daher ein Spieler auch mit dem Spiel beschäftigt, umso länger kann auch die Zeit dauern, die er für einen konkreten Erfolg benötigt. Einige Spieler sind – wie aufgezeigt – daher bereit, sich solche Vorteile zu erkaufen oder zu tauschen, um das zeitintensive Erspielen zu umgehen. Viele virtuelle Welten sehen zudem die Möglichkeit vor, dass Nutzer Items und virtuelle Währungen untereinander handeln und tauschen, bzw. sich diese auch schenken können.

Dabei geht die Wirtschaft davon aus, dass gegenwärtig im Schnitt nur jeder zehnte Nutzer bereit ist, für solche virtuellen Güter Geld zu bezahlen. In der nachwachsenden Spielergeneration der 18 – 29jährigen hat jedoch bereits jeder fünfte einmal Geld für virtuellen Spielecontent ausgegeben (Bitkom, 2012-2). In Deutschland wurden alleine im Jahr 2011 insgesamt 233 Millionen Euro durch Item-Handel und virtuelle Zusatzleistungen umgesetzt (BIU, 2011). Marktanalysten gehen sogar davon aus, dass bereits im Jahr 2015 fast 12 Milliarden US-Dollar mit virtuellen Spielegütern umgesetzt werden (InStat, 2011). Die im Verhältnis zu der absoluten Nutzerzahl geringe Anzahl an zahlungsbereiten Nutzern verdeutlicht, dass es Spielebetreibern daran gelegen sein muss, den Zugang zum Spiel attraktiv und einfach zu gestalten, um möglichst viele Nutzer für das eigene Spiel zu gewinnen. Die Anmeldung zu virtuellen Welten wird daher möglichst einfach gestaltet. Überwiegend gibt der Nutzer eine Emailadresse, einen Nutzernamen, ein Passwort und hin und wieder auch ein Alter an. Eine Verifikation der sich anmeldenden Person oder deren wirkliches Alter findet – wenn überhaupt – überwiegend nur durch eine einfache Verifikationsemail statt. Dieses einfache, aber vor allem aus Kinder- und Jugendschutzaspekten heraus unbefriedigende Anmeldeverfahren, ermöglicht dem Nutzer hingegen ein barrierefreies und vor allem schnelles Einfinden in das jeweilige Spiel. Aus denselben Gründen kann es auch im Interesse von Betreibern liegen möglichst nicht in Konflikt mit den gesetzlichen Regelungen zum Kinder- und Jugendschutz

In der nachwachsenden Spielergeneration der 18 – 29jährigen hat jedoch bereits jeder fünfte einmal Geld für virtuellen Spielecontent ausgegeben (Bitkom, 2012-2).

3 Im Rahmen dieses Bezahlmodells kommt es immer wieder vor, dass Minderjährige ohne Wissen und Erlaubnis der Eltern in Einzelfällen bis zu 10.000 Euro im Monat für virtuelle Güter über die heimische Telefonrechnung bezahlen. Überwiegend wurden die Eltern in Gerichtsprozessen, insbesondere mit dem Hinweis darauf, dass Sondernummern hätten gesperrt werden können, zur Begleichung dieser Summe verurteilt. Eine Ausnahme von dieser Praxis bildete jedoch ein Gerichtsurteil aus Saarbrücken, bei dem der Richter u.a. den mangelnden Kinder- und Jugendschutz in Online-Spielen kritisierte (LG Saarbrücken, 2011).

Kritisch gesehen könnte eine solche Grafik in Verbindung mit der Aussage, dass ein Spiel „gratis“ sei, auch die Sensibilität von Eltern für die innewohnenden Interaktionsrisiken, aber auch für das Vorhandensein entsprechender Bezahlmodelle, senken.

zu kommen und damit ggf. eine möglichst geringe Altersfreigabe zu erhalten. Unter anderem deshalb vermeiden eine Vielzahl von heutigen Onlinegames pornografische und gewalthaltige Inhalte und setzen auf eine kinderbunte und kindgerechte Spielegrafik. Kritisch gesehen könnte eine solche Grafik in Verbindung mit der Aussage, dass ein Spiel „gratis“ sei, auch die Sensibilität von Eltern für die innewohnenden Interaktionsrisiken, aber auch für das Vorhandensein entsprechender Bezahlmodelle, senken.

Unabhängig davon, welches Finanzierungsmodell konkret durch die virtuelle Welt genutzt wird, kann es irgendwann dazu kommen, dass die Nutzer – insbesondere wenn es sich um Minderjährige handelt – nicht mehr das Geld haben, um dieser Spielleidenschaft in der von ihnen gewünschten Form nachzukommen. In diesem Rahmen gab es weltweit, aber auch in Deutschland, in den letzten Jahren vermehrt die Diskussion, ob exzessives Online-Spielen zur Sucht oder suchtartigen Erscheinungsformen bei den Nutzern führen kann. Zu dieser Frage gab es einige relevante deutsche Untersuchungen, die sich letztlich nur in der Höhe der Betroffenen und nicht in dem Vorhandensein der Erscheinungsform unterschieden (Pfeiffer et al., 2009; Fritz et al., 2011; Rumpf et al., 2011).

In einem Zwischenfazit kann also festgehalten werden, dass virtuelle Welten für eine Vielzahl von Menschen und insbesondere für Minderjährige höchst attraktiv erscheinen, da diese die Möglichkeiten der Interaktion und Kommunikation beinhalten. Im Gegenzug findet jedoch in den meisten Fällen keine Überprüfung der Identität oder des Alters der anmeldenden Person statt.

4. Cybergrooming

Minderjährige sind traditionell eine wichtige Zielgruppe für virtuelle Welten. Dies kann unter anderem daran erkennt werden, dass eine Vielzahl von Spielen sich zumindest optisch direkt an dieser Gruppe ausrichtet. Als ein Beispiel soll hier das Metaversum Habbo Hotel dienen, welches nach eigenen Angaben ca. 14 Millionen aktive Nutzer und ca. 250 Millionen Zugriffe weltweit verzeichnet (Sulake, 2012). Das Alter von 90 Prozent der Nutzer soll sich zudem zwischen 13 – 19 Jahren bewegen (ebd.). Eine fehlende effektive Altersüberprüfung lässt diese Zahlen jedoch prinzipiell fraglich erscheinen, da das tatsächliche Alter des Anmeldenden nicht sicher festgestellt wird. Obwohl diese Form der Anonymisierung in virtuellen Welten von vielen Menschen positiv genutzt wird, indem diese in ein anderes Geschlecht oder einen anderen Charakter schlüpfen und sich eine virtuelle Identität aufbauen (Cole; Griffith 2007), gibt es auch Personen, die gezielt ihr Alter und Geschlecht verschleiern, um sich unter dieser vorgegebenen Identität das Vertrauen von minderjährigen Nutzern zu erschleichen. Das Ziel dieses Vorgehens ist die Einleitung von sexuellen Interaktionen mit Minderjährigen – dem sogenannten Cybergrooming (Rüdiger, 2012).

Der Begriff Grooming wurde durch den niederländischen Psychologen Ruud Bullens im Jahr 1995, als die Planungsphase, die einem sexuellen Übergriff durch einen Erwachsenen auf ein Kind vorausgeht, definiert (Bullens, 1995, S.55). Nachvollziehbarerweise bezogen sich die Erörterungen von Bullens noch nicht auf das Internet als Phänomenträger, sodass die Komponente des „Cyber“ bei ihm noch nicht von Relevanz war. In der Kombination beider Begriffe ergibt sich das Kunstwort „Cybergrooming“. Letztlich steht Cybergrooming in etwa für „Pflege“ oder „Streicheln“. Übersetzt würde Cybergrooming also Internetpflege /-streicheln bedeuten (Choo, 2009). Unter Beachtung des von Bullens gewählten Definitionsansatzes erscheint es aber naheliegend, Cybergrooming als „das Anbahnen von sexuellen Handlungen mit Minderjährigen durch Ausnutzung der Anonymität und der Kommunikationsmöglichkeiten des Internets als Vorbereitungsphase einer

sexuellen Interaktion“ zu bezeichnen. Im englischen Sprachgebrauch hat sich für die Täter die Bezeichnung „(Cyber)groomer“ (ebd, S. 92) und im US-amerikanischen „Onlinepredator“ herausgebildet (Finkelhor et. al., 2008). Finkelhor kommt in Auswertung von 6.594 registrierten Vergewaltigungen in den USA bereits 2008 zu dem Ergebnis, dass von diesen sieben Prozent durch das Internet angebahnt wurden (ebd.). Bisherige Untersuchungen zu Cybergrooming beziehen sich fast gänzlich auf Handlungen in typischen Chat-Foren ohne eine entsprechende grafische Umgebung und Interaktion durch einen Avatar oder eine Spieleumgebung einzubeziehen (Choo, 2009; Finkelhor et. al., 2008; Ybarra; Mitchell, 2005). Im deutschsprachigen Raum hat Katzer im Jahr 2007 eine erste Untersuchung zur Viktimisierung von Jugendlichen in Chat-Räumen durch sexuelle Gewalt vorgelegt (Katzer, 2007). Katzer kommt dabei zu dem Schluss, dass sexuelle Viktimisierungen von Minderjährigen – insbesondere Mädchen – in Chat-Räumen aufgrund der dort herrschenden Anonymität sogar noch häufiger stattfindet, als in der physischen Realität (ebd, S. 79). Auch hat sie festgestellt, dass vor allem Mädchen in der Adoleszenz dazu neigen, sich sexuell orientierte Nicknames in Chat-Foren zu geben, was wiederum die Wahrscheinlichkeit einer Viktimisierung erhöht. In Auswertung dieser Erhebung haben bereits 48 Prozent der unter 14jährigen Mädchen ungewünschte sexuelle Kommunikationen im Internet erlebt, 26 Prozent gaben an, ungewollt nach sexuellen Erlebnissen gefragt worden zu sein, 24 Prozent wurden aufgefordert, entsprechende Erlebnisse aktiv zu schildern, elf Prozent gaben zudem an, bereits mindestens einmal zu einem realen Treffen eingeladen worden zu sein (ebd, S. 88).

Vor dem Hintergrund der stetig steigenden Verbreitung von Internetzugängen, die bei Minderjährigen in Deutschland eine annähernd hundertprozentige Abdeckung erreicht hat, erscheint es aber im Bereich des Wahrscheinlichen, dass sich die Viktimisierungsrate weltweit eher erhöht als verringert hat.

5. Tätertypologien

Gegenwärtig können zwei primäre Täterypologien von Cybergroomern festgestellt werden. Dem relativ offen agierenden „Erpresser“ oder „direkten“ Typus und den eher konspirativ vorgehenden „Guten-Freund-Typus“. Beide Tätertypologien sollen in diesem Artikel vornehmlich an dem Beispiel des deutschsprachigen Habbo Hotels, aber auch unter Heranziehung weiterer virtueller Welten, erläutert werden.

Zum Grundverständnis der Vorgehensweise von beiden Tätertypologien wird zunächst dargestellt, wie die Interaktion und Kommunikation in virtuellen Welten allgemein funktioniert.

Eine Anmeldung in Habbo Hotel erfordert die Eingabe eines Nutzernamens, die Festlegung eines Passwortes und die Angabe einer Email-Adresse. Dabei findet im deutschsprachigen Habbo Hotel keine tatsächliche Überprüfung der Gültigkeit der Email-Adresse statt, beispielsweise in Form einer zugesendeten Verifikationsemail. Nachdem sich ein Nutzer angemeldet hat, befindet er sich in einem virtuellen Hotelraum. Durch den Verkauf virtueller Möbel (furnitures), Bekleidung und Haustiere an die Nutzer finanziert sich Habbo Hotel. Gerade auf Minderjährige stellt zudem der Verkauf von virtuellen Haustieren (u.a. Ponys, Katzen und Hasen) ab. Aber nicht nur die Haustiere müssen mit sogenannten Habbo Talern (der virtuellen Währung in Habbo Hotel) bezahlt werden, sondern auch das zugehörige Haustierfutter muss regelmäßig erneut gekauft werden. In dem zugehörigen Shop heißt es hierzu *„Haustiere brauchen Essen, Wasser und Belohnungen. Du findest alles Nötige bei der Haustierverpflegung“*. In Habbo Hotel ist dabei die Möglichkeit vorgesehen, dass Nutzer diese Items unter einander tauschen bzw. einander schenken können.

In Auswertung dieser Erhebung haben bereits 48 Prozent der unter 14jährigen Mädchen ungewünschte sexuelle Kommunikationen im Internet erlebt, 26 Prozent gaben an, ungewollt nach sexuellen Erlebnissen gefragt worden zu sein, 24 Prozent wurden aufgefordert, entsprechende Erlebnisse aktiv zu schildern, elf Prozent gaben zudem an, bereits mindestens einmal zu einem realen Treffen eingeladen worden zu sein (ebd, S. 88).

Die Nutzer können in Habbo – dies geschieht in den meisten anderen virtuellen Welten ähnlich – prinzipiell in zwei Formen in Kontakt zueinander treten. In den Lobby- und Themenräume kommt eine Vielzahl von Nutzern mit ihren Avataren zusammen und schreibt in einem für alle im Raum einsehbaren öffentlichen Chat miteinander. Wenn zwei Nutzer nur direkt miteinander und ohne andere Mitleser kommunizieren wollen, nutzen sie eine interne Chat- und Nachrichtenfunktion. Hierfür müssen sich die Nutzer aber vorher erst miteinander verbinden, was durch die Versendung und Annahme einer Freundschaftsanfrage (FS) geschieht. Zudem können sich die Nutzer dann auch in die privaten individuellen Hotelräume zurückziehen, bei denen auch ein weiteres Mitlesen von anderen Nutzern ausgeschlossen werden kann. Während der Kommunikation können die Avatare auch in eine Interaktion treten, indem diese beispielsweise zusammen tanzen, im selben Bett liegen oder sich an denselben Tisch setzen. Sexualtätern bietet sich daher eine Vielzahl an verbalen und nonverbalen Kontaktmöglichkeiten zu potentiellen minderjährigen Opfern.

In einem solchen Sachverhalt bezahlte 2010 ein 28jähriger Däne 25 Jungen im Alter von 12 – 16 Jahren mit Gold für World of Warcraft für die Übersendung von Nacktfotos und Videos, auf denen die Jungen masturbierten (Chalk, 2010).

Erpresser-Typus

Der Erpresser-Typus agiert bei der Anbahnung sexueller Kontakte zumeist direkt und offen. Ihm geht es im Kern darum, eine schnelle sexuell orientierte Kontaktaufnahme mit Minderjährigen herzustellen. Sobald er dies erreicht hat, kann er diesen Kontakt ausnutzen, indem er das Opfer animiert, immer mehr Medien – wie Fotos und Videos - von sich anzufertigen oder anfertigen zu lassen. Wenn ein Opfer dies nicht mehr möchte oder den Kontakt einstellt, kann der Täter auf unterschiedlichste Weise reagieren. Im besten Fall bricht er den Kontakt zum Opfer ebenfalls ab. Im schlimmsten Fall – und wie das Beispiel von Amanda Todd gezeigt hat – droht er damit den Eltern oder Freunden Fotos oder Videos zu senden oder im Netz zu veröffentlichen, wenn das Opfer nicht weitere sexuelle Interaktionen zulässt.

Um einen solchen Kontakt mit einem Minderjährigen überhaupt zu initiieren, setzen Täter dabei zwei primäre Anbahnungsmethoden ein. Die offensichtlichste Variante ist, wenn der Täter im öffentlich einsehbaren Chat konkret nach Opfern sucht. Das kann dann z.B. wie folgt aussehen: *„Welches Mädchen mit Skype, MSN oder ICQ hat Lust auf Camen,?“* (Rüdiger, 2012). Andere in Habbo Hotel festgestellte Anfragen lauteten z.B. *„wer möchte eine MOLA sehen* [Anm. des Autors *„Morgenlatte“*]“ oder *„wer möchte ihn da unten sehen?“*. Obwohl solche Anfragen aus Sicht eines Erwachsenen als offensichtlich problematisch angesehen werden können, kann nicht ausgeschlossen werden, dass gerade Minderjährige in der Adoleszenz-Phase durchaus aus einfacher Neugier auf solche Anfragen eingehen.

Eine andere Taktik besteht darin, Minderjährigen Items und virtuelle Währungen als Gegenleistung für das Übersenden von Bildern (Pics) oder dem Camen anzubieten. Beispielhaft können in öffentlichen Hotelräumen in Habbo Hotel immer wieder Anfragen registriert werden wie *„welches Mädchen mit einer Webcam, möchte sich 70 – 100 Taler (ca. 12 Euro) verdienen, bitte FS“* (ebd.). In anderen bekannten Fällen wurden z.B. minderjährige Opfer in World of Warcraft mit virtuellem Gold für das Anfertigen und Übersenden von Nacktfotos bezahlt. In einem solchen Sachverhalt bezahlte 2010 ein 28jähriger Däne 25 Jungen im Alter von 12 – 16 Jahren mit Gold für World of Warcraft für die Übersendung von Nacktfotos und Videos, auf denen die Jungen masturbierten (Chalk, 2010).

Um diese Bilder und Fotos auch zu bekommen oder sogar einen Live-Video-Chat mit den Opfern zu erreichen, versucht der Erpresser-Typus üblicherweise, eine schnelle Überleitung der Kommunikation auf einen Instant-Messenger, wie ICQ und insbesondere Skype zu forcieren. Um beispielsweise in Kontakt mit einem Minderjährigen bei Skype zu treten, muss

der Täter nur den Nutzernamen der Person kennen. Diesen Nutzernamen versucht der Täter wiederum in Habbo Hotel oder einem anderen Online-Spiel oder Chat-Portal zu erfahren, daher erfolgt auch häufig die Frage *„welches Mädchen mit Skype […]“*. Sobald ein Opfer diesen Skype-Namen herausgegeben hat, fügt ihn der Täter zu seiner eigenen Kontaktliste hinzu. Hier kommt ihm zu Gute, dass Skype so voreingestellt ist, dass bei einem eingehenden Videoanruf automatisch die Live-Übertragung des Anrufers erscheint – unabhängig davon, ob die Nutzer diesen auch annehmen möchten und ob überhaupt eine Web-Kamera angeschlossen ist. Kommt es zu einer Videoübertragung, kann der Täter das gesamte Video mitzeichnen oder auch einzelne Screenshots von dem Geschehen machen. Zudem bietet Skype auch die Möglichkeit einer Dateiübertragung über den integrierten Chatbereich, über den relativ unkompliziert Bild- und Videodateien ausgetauscht werden können. Dies bedeutet, dass ein Opfer z. B. unkompliziert Nacktbilder, die es von sich per Web-Cam gemacht hat, an den Täter übersenden kann. Wenn ein Opfer entsprechende Videos und Fotos von sich anfertigt, die einen pornografischen Charakter haben, handelt es sich letztlich um die Anfertigung und den Besitz von strafbarer Kinder- und Jugendpornografie.

Das tragische Beispiel der 15jährigen Kanadierin Amanda Todd zeigt, wie der Erpresser-Typus weiter vorgeht. Amanda Todd wurde mit 12 Jahren im Internet durch Männer dazu gebracht, ihre Brüste vor einer laufenden Web-Kamera zu entblößen. Wie bereits dargestellt, wurden dabei von Amanda Fotos (Screenshots) angefertigt. Im Nachgang schrieb einer der Männer Amanda über Facebook an und verlangte immer weitere Nacktfotos von ihr und drohte bei einer Verweigerung mit der Veröffentlichung der bisherigen Fotos im Internet. Amanda verweigerte weitere sexuelle Kontakte mit dem Täter, woraufhin dieser die Fotos bei Facebook als Profilbilder eines Fake-Accounts verwendete und eine Rundmail an den Email-Verteiler versendete. In der Folge wurde Amanda durch ihr soziales Umfeld gemobbt und litt unter ständigen Cybermobbing-Angriffen. Vermutlich bedingt durch diese ständigen Angriffe brachte sie sich am 10. Oktober 2012 um (Shaw, 2012). Das Beispiel von Amanda veranschaulicht sehr eindringlich das beschriebene Vorgehen von Tätern. Dem Erpressertypus kommt bei der Opfersuche in virtuellen Welten insbesondere zu Gute, dass viele Minderjährige ihren Avataren Nutzernamen geben, durch die Rückschlüsse auf das Alter gezogen werden können. So liefern Zahlen hinter den Namen häufig einen Hinweis auf ein vermeintliches Alter – beispielsweise „Sonnenblume12“ (12 Jahre) oder „Sonnenblume99“ (Jahrgang 1999 - demnach 12 Jahre). Namen wie z.B. „Checker15“ (Junge, 15 Jahre alt) können zudem Auskunft über das Geschlecht geben. Nebenbei können Nicknames auch bereits sexuelle Botschaften vermitteln wie, „gro.ßer.sch.wanz19“ oder „sexybitch13“ (Breichler et.al, 2009, S.9). Viele Nutzer haben zudem die Angewohnheit, ihren Avataren das eigene Geschlecht zu geben, sodass der Täter – bedingt durch das Geschlecht des Avatars und den Nutzernamen – bereits eine Opferauswahl treffen kann.

Dem Erpressertypus kommt bei der Opfersuche in virtuellen Welten insbesondere zu Gute, dass viele Minderjährige ihren Avataren Nutzernamen geben, durch die Rückschlüsse auf das Alter gezogen werden können.

Teilweise beginnen Täter die Kommunikation auch mit der direkten Anfrage nach Cybersex (CS). Cybersex steht für eine Form von interaktiver Schrifterotik, die sich in der Intensität noch am ehesten mit Verbalerotik – wie Telefonsex – vergleichen lässt. Bei dieser schreiben sich die Nutzer gegenseitig entweder ihre sexuellen Fantasien oder reagieren jeweils auf die Anmerkungen des Gegenübers. So entsteht eine intime Kommunikation, die häufig pornografische Züge aufweist. Teilweise können solche Gespräche auch völlig unverfänglich begonnen werden. In MMORPG können Einleitungen beispielsweise darin bestehen, dass auf die grafische Gestaltung des – üblicherweise weiblichen – Avatars Bezug genommen

wird. Je nach Erfolg dieser Einstiegsphase, aber auch nach Motivation des Täters, wird das Gespräch weitergeführt und kann in der Folge auch auf die IRCs übergeleitet werden. Die Täter setzen dabei darauf, dass Minderjährige aus Neugier und durch das Fehlen von Video- oder Bildübertragungen eher dazu bereit sind, sich etwaigen sexuellen Gesprächen zu öffnen.

Dass Täter in dieser Form vorgehen, konnte im Rahmen einer teilnehmenden Beobachtung und Verwendung einer kindlichen Legendierung in Online-Spielen und Kinder-Chaträumen beobachtet werden. Beispielhaft wurde eine solche im deutschsprachigen Habbo Hotel vom 28. Februar 2013 von 13:00 – 16:00 Uhr vorgenommen. Zum Zwecke der Beobachtung wurden die zu diesem Zeitpunkt beiden höchst frequentierten öffentlichen Chaträume aufgesucht. Insgesamt konnten dabei 25 relevante Kommunikationsversuche festgestellt werden (Rüdiger, 2013-2). Diese teilten sich wiederum auf in 15 Äußerungen, in denen direkt nach sexuellen Handlungen (bsp. camsex) oder in denen nach Skype oder ICQ gefragt wurde. Beispielhaft fielen unter diese Kategorie folgende Aussagen von unterschiedlichen Avataren *„Welches Girl hat Lust auf Bildertausch? FS schicken☺“ „Suche Boy mit Langem für Real Treff PSL[please] Melden“ „Suche percverses girl mit skyxpe (sic!)“*[4]. Zudem wurden fünf direkte Kommunikationsanbahnungen dem legendierten Avatar gegenüber festgestellt, von denen zwei hier dargestellt werden sollen. Dabei wurde sich passiv und nicht aktiv fördernd verhalten. Im ersten Fall wurde im öffentlichen Chat folgende Anfrage geschrieben *„Du bist weiblich und willst dir 140 Taler [ca. 20 Euro] verdienen? ← FS anbieten ←…☺“*. In der Folge schrieb derselbe Nutzer den legendierten Avataren an *„Hi wie xalt?* 13 aber bald 14! *Hast xcam?* Meinst skip? *Und eine xwebxcam am notebook.* Was soll ich machen? *Kannst dir 140 Taler verdienen indem du mir ein bisschen was per xcam xzeigst!* Was denn? *Xmehr von dir.* Muss aba noch warten mama ist da. *Wie lang denn* (Abbruch der Kommunikation)“. Im zweiten Fall wurde erneut der legendierte Avatar ohne aktives Tun durch einen Nutzer angeschrieben *„Hi srry komme jetzt dumm an aber brauche wirklich hilfe voll peinlich aber mein hand tuht voll weh“*? was meinst? *Ja hole mir einen runter komme nicht zum schluss wie peinlich ;(((* Wie soll ich helfen? *Kannst du mir nicht dabei zu sehen?* Und wie ? *Ja über xxcamxx ?* wie alt? *17 und hilfst du mir?* Ich bin aber jünger! *Wie alt bist du den?* 13. *Egal helf mir bitte las xcamenxx bitte“*. Die übrigen drei Kontaktanbahnungen liefen in derselben Vorgehensweise ab. Innerhalb von nur drei Stunden hätte es also im schlimmsten Fall zu mindestens fünf sexuellen Viktimisierungen von Minderjährigen kommen können (ebd.).

Auffallend im Rahmen der teilnehmenden Beobachtung war zudem die Feststellung, dass vereinzelt auch bereits direkt nach dem beliebten Smartphone Messenger WhatsApp zum Bildertausch gefragt wurde, beispielhaft „bochk auf skyipe oder xwhattsapp und xbilder schicken oder habbo sxx?“.

In einem wiederholenden Versuch am 2. März 2013 konnten im Zeitraum von 12:00 – 12:40 Uhr in einer Lobby in Habbo Hotel insgesamt 26 entsprechende Äußerungen von 22 Avataren festgestellt werden. Diese teilten sich auf in 18 offene Anfragen beispielhaft „Ich will xcamsexx ;☺“,“Welches mädchen will mir zugicken ☺ ?:) fs ☺“ oder „Welches Girl ist xpervers? FS schicken“. Sechs Äußerungen waren sonstiger Natur mit sexuellem Inhalt oder Wiederholungen und zwei waren direkte Anfragen an den legendierten Avatar bezüglich einer Gesprächsüberleitung auf Skype (ebd)[5]. Auffallend im Rahmen der teilnehmenden Beobachtung war zudem die Feststellung, dass vereinzelt auch bereits direkt nach dem beliebten Smartphone Messenger WhatsApp zum Bildertausch gefragt wurde, beispielhaft „bochk auf skyipe oder xwhattsapp und xbilder schicken oder habbo sxx?“. Eine erfolgreiche Überleitung auf WhatsApp hätte für

4 Die bewusst falsche Schreibweise in den Kommunikationen, soll – wie bereits dargestellt – die Wort-Filterung in Habbo Hotel umgehen. Im Rahmen des Artikels erfolgt eine wortgetreue Wiedergabe.

5 Zur Legendierung wurde ein weiblicher Avatar mit einen Nickname, der auf ein Mädchen im Alter von 13 Jahren hindeutete, erstellt.

den Täter mehrere Vorteile. Einerseits muss für eine Kommunikation über dieses Programm zwingend eine Handynummer ausgetauscht werden, was weitere Formen der Belästigung und Annäherung ermöglicht und andererseits können über WhatsApp unkompliziert Mediendateien, also auch selbstgemachte Bilder, ausgetauscht werden.

Das Vorgehen des Erpresser-Typus ist in vielen internationalen Beispielen belegt. Im Jahr 2011 wurde in New York ein 19jähriger Mann festgenommen, der über die Spiele-Konsole Xbox einen 13jährigen Jungen angegroomt und sexuell missbraucht hatte (Fahey, 2011). Der Täter bezeichnete sich im sog. Gamertag (für andere Spieler ersichtlicher Nickname und Profil des Nutzers und seine bisherigen Spielerfolge) für alle Mitspieler ersichtlich als „homosexuelles Pelztier" (homosexual furry). Der Täter hat hier ausgenutzt, dass in Millionen Wohn- und Kinderzimmern weltweit Spielekonsolen wie die Xbox und Playstation vorhanden sind und mit diesen in einem großen Umfang online gespielt wird. Sowohl die Xbox als auch die Playstation konnten bereits 2012 jeweils 70 Millionen verkaufte Spielekonsolen vermelden (Leschni, 2012). Beide Systeme sehen zudem die Möglichkeit vor, mit Mitspielern auch nach einem Spiel in Kontakt zu treten und sich mit diesen über eine Freundschaftsanfrage enger zu verbinden. Auch haben beide Systeme die Möglichkeit, durch die Playstation Eye oder die Xbox Kinect eine Live-Videoübertragung nachzurüsten. Aber auch mit Habbo Hotel als Anbahnungsplattform ist eine Vielzahl von Sachverhalten bekannt. Im September 2012 wurde ein 25jähriger ehemaliger Polizeiangestellter in England zu einer dreieinhalbjährigen Haftstrafe verurteilt. Der Täter hat Habbo Hotel genutzt, um gezielt minderjährige Jungen anzusprechen und dazu zu bringen, ihn vor der Web-Kamera über Skype oder MSN bei sexuellen Handlungen zu betrachten (Phagura, 2012).

Variationen dieses Tätertypus gibt es unzählige, indem diese sich beispielweise als Mitarbeiter einer Jugendzeitschrift oder einer Modelagentur ausgeben und ein minderjähriges Opfer um Probefotos bittet.

Indirekte Tätertypus

Während der Erpresser direkt und offen agierend auftritt, so geht der zweite primäre Typus eher verdeckt und konspirativ vor. Dieser auch als „indirekte" oder „Buddy" bezeichnete Typus meldet sich zunächst in virtuellen Welten mit falschen Anmeldedaten an. Da ein Teil der virtuellen Welten keinen Abgleich der sich anmeldenden IP-(InternetProtocol)Adressen vornimmt, ist es ihnen möglich, gleichzeitig mehrere Nutzer-Accounts zu gestalten und zu betreiben. So kann ein Täter mit mehreren Avataren mit differenten Ausgestaltungen (Junge/Mädchen/Alter/Hintergrund) in einer virtuellen Welt vertreten sein. Insofern spricht man auch von „Multiboxing". Teilweise können die Täter auch den öffentlichen Chat verfolgen, um Ansatzpunkte für den Einstieg in das Gespräch mit einem potentiell ausgewählten Opfer zu finden. Hierbei kann sich der Täter dann über seine differenten Avatare entsprechend unterschiedlich bei dem Opfer ausgeben. Zumeist versuchen die Täter im Gespräch, das Alter des Opfers herauszufinden, um ihr eigenes potentielles Alter anzupassen. Dieses gibt er dann meist auch als gleichaltrig oder nur geringfügig älter an. Im Rahmen der Anbahnungsphase versucht der Täter dann, einen emotionalen Einstiegspunkt zu dem Opfer zu finden. Das ist insbesondere in der Pubertät vielversprechend, wenn der Täter Verständnis und Interesse für das Opfer zeigt. Während dieser Phase versucht sich der Täter bereits unauffällig über das Aussehen des Opfers und etwaige erste sexuelle Erfahrungen zu erkundigen. Sofern er dabei eine Überleitung auf andere Medien zur Kommunikation versucht, achtet er in der Anbahnungsphase noch darauf, dass sein Alter oder sein Geschlecht, sollte er sich als andersgeschlechtlich ausgegeben haben,

Der Täter hat Habbo Hotel genutzt, um gezielt minderjährige Jungen anzusprechen und dazu zu bringen, ihn vor der Web-Kamera über Skype oder MSN bei sexuellen Handlungen zu betrachten (Phagura, 2012).

nicht enttarnt wird. So würde er z.B. bei Skype angeben, dass seine Videokamera nicht mehr funktioniert usw.. Sobald der Täter davon ausgehen kann, dass er das Vertrauen des Opfers hat, leitet er die sogenannte Geheimnisphase ein. In dieser offenbart er dem Opfer ein gemeinsames Geheimnis, was nur diese beiden teilen, beispielsweise sein wahres Alter oder Geschlecht. Wenn das Opfer hier nicht den Kontakt abbricht, verfestigt sich die Verbindung mit dem Opfer und eine Überleitung z.B. zu einem physischen Treffen wird ermöglicht.

Insgesamt muss davon ausgegangen werden, dass beiden Täter-Typologien die Besonderheiten virtueller Welten, wie die Möglichkeit der Offerierung virtueller Güter als „Bezahlung", der Annäherung durch spielerische Interaktionen, die grafische Ausgestaltung sowie der relativ unbewachten Kommunikation entgegenkommen.

Konkrete Beispiele für solche Vorgehensweisen sind international bereits für eine Vielzahl von virtuellen Welten bekannt. Im Jahr 2010 näherte sich ein 28jähriger unter Vorgabe, ein 12jähriger zu sein, einem elfjährigem Mädchen im niederländischen Habbo Hotel. Er fing eine Interaktion mit ihr an, verband sich im Rahmen der Freundschaftsanfragen und zusammen statteten sie ein gemeinsames Hotelzimmer aus. In der Folge verbrachten beide viel Zeit im gemeinsamen Hotelraum und führten eine Art virtuelles Familienleben. Hierbei konnte der Täter ausnutzen, dass er ganz andere monetäre Möglichkeiten hatte, virtuelle Möbel zu kaufen. Nach einiger Zeit leitete der Täter in die beschriebene Geheimnisphase über. In dieser offenbarte er sein wahres Alter und verabredete sich mit dem Kind in einem Hotelraum. Hier kam es zu sexuellen Handlungen. Überführt wurde der Täter, da die Mutter SMS des Täters mit sexuellem Inhalt auf dem Handy des Kindes fand (Middelburg, 2010).

Ein anderes Beispiel hat in den USA im Jahr 2011 für einige Diskussionen gesorgt. Im MMORPG Runescape spielte ein 54jähriger Mann mit einer dreizehnjährigen Nutzerin zusammen. Es ging soweit, dass in dem Spiel eine virtuelle Hochzeit zwischen beiden gefeiert wurde. In der Folge kam es zu realen direkten Treffen zwischen Täter und Opfer und in deren Rahmen auch zu sexuellen Handlungen. Überführt wurde der Täter, da er dem Opfer bei einem Treffen zur besseren Kommunikation ein Mobilfunktelefon gegeben hatte. Dieses wurde von der Mutter – die ihrer Tochter den Besitz von Handys verboten hatte – gefunden und die gespeicherten Nachrichten mit entsprechend sexuellem Bezug entdeckt (Parrish, 2011).

Besonders auffällig ist, dass bei bekannt gewordenen Sachverhalten auch Frauen als Täterinnen in Erscheinung getreten sind. So wurde bereits im Jahr 2009 eine 42jährige englische Schullehrerin verhaftet, nachdem sie einen 14 Jahre alten Jungen über World of Warcraft angegroomt hatte (DailyMail, 2009). In einem anderen Fall wurde im Jahr 2011 eine 36jährige Amerikanerin verhaftet, nachdem sie einen 13jährigen Jungen sexuell missbraucht hatte. Den sexuellen Missbrauch leitete die Täterin über die Chat-Möglichkeiten (Xbox-Live) der Spielekonsole Xbox ein (Kornhaber, 2011).

Insgesamt muss davon ausgegangen werden, dass beiden Täter-Typologien die Besonderheiten virtueller Welten, wie die Möglichkeit der Offerierung virtueller Güter als „Bezahlung", der Annäherung durch spielerische Interaktionen, die grafische Ausgestaltung sowie der relativ unbewachten Kommunikation entgegenkommen.

6. Umfang des Phänomens

Eine konkrete wissenschaftliche und auf anerkannten empirischen Methoden basierende Aufarbeitung des Umfangs der sexuellen Viktimisierung von Minderjährigen, die ihren Ursprung in virtuellen Welten, Kinder-Chaträumen oder Spiele-Umgebungen (Spielekonsolen) genommen haben, ist bisher noch nicht erfolgt. Aussagen zu dem Umfang können seriös betrachtet nicht vorgenommen werden. Dies gilt umso mehr, da es sich bei Cybergrooming – ähnlich wie bei anderen Missbrauchsdelikten – überwiegend um ein sog. Kontrolldelikt handelt. Also ein Delikt, das selten von Opfern angezeigt wird und

vornehmlich nur durch proaktive Ermittlungshandlungen der Polizei ins Hellfeld gezogen werden kann. Wenn die Strafverfolgungsbehörden also nicht selbstständig im Internet den Versuch unternehmen die Täter zu ermitteln und zu überführen, wird die Zahl der Anzeigen und damit auch der Verurteilungen gering bleiben. Trotzdem die Polizeiliche Kriminalstatistik (PKS) in Deutschland im Hellfeld eine Steigerung der Anzeigen von entsprechenden Straftatbeständen von 934 im Jahr 2011 um annähernd 50 Prozent auf 1.406 im Jahr 2012 aufweist (BMI, 2013)[6], erscheinen diese Zahlen vor dem Hintergrund, dass Millionen von Kindern täglich in Online-Spielen, Sozialen Netzwerken und Kinder-Chaträumen aktiv sind, relativ gering. Eine Annäherung an den gesamten Umfang kann, bedingt durch das Vorgenannte, daher nur über Indizien erfolgen. Neben den in diesem Artikel genannten Gerichtsurteilen und Presseberichterstattungen sollen insbesondere auf eine im Netz frei zugängliche Umfrage unter Nutzern von Freggers, auf die Operation Game Over des Generalstaatsanwalt des Bundesstaates New York sowie auf einen Fernsehbeitrag über Habbo Hotel eingegangen werden.

Freggers ist eine 3D-basierende social Community, in denen die Nutzer – ähnlich wie bei Habbo Hotel – eigene virtuelle Zimmer bekommen, diese einrichten können und mit ihren Avataren in öffentlichen Bereichen und Zimmern interagieren und kommunizieren. Dabei setzt Freggers ebenfalls auf eine sehr farbenfrohe optische und durchaus kindgerechte Ausgestaltung. Die Internetseite freggers-wiki.de führt jedes Jahr unter den Nutzern des deutschsprachigen Freggers (Freggers.de) und des englischsprachigen Äquivalents (Freggers.com) eine Umfrage mit unterschiedlichen Schwerpunkten durch. Die jüngste Umfrage wurde 2012 veröffentlicht und widmete sich insbesondere den Erfahrungen der Nutzer im Chat-Bereich von Freggers (Freggers-Wiki, 2011).

An der in Rede stehenden Umfrage haben insgesamt 613 Nutzer (n) teilgenommen, wovon 38 Prozent Kinder unter 14 Jahren waren (absolut 236). Weitere 32 Prozent waren Minderjährige im Alter von 14 – 18 Jahren (absolut 200). Die übrigen Nutzer sind älter oder haben keine Angaben zum Alter gemacht. Auffällig ist dabei, dass 49 Prozent angegeben haben, weiblichen Geschlechts zu sein (absolut 303) und nur 39 Prozent ihr Geschlecht als männlich bezeichneten (absolut 242). Knapp 10 Prozent gaben kein Geschlecht an. In der Folge konzentrierte sich die Umfrage vornehmlich auf die Erfahrungen der Nutzer im Chat. Dabei differenzierte die Umfrage, ob die Erfahrungen mit einem weiblichen, männlichen, Erwachsenen oder als Kind erkennbaren Avataren gemacht wurden. In diesem Rahmen gaben 31 Prozent (absolut 191) der deutschsprachigen Nutzer von weiblichen Avataren an, bereits in Freggers sexuell belästigt worden zu sein (ebd.). Wenn die Nutzer hingegen mit männlichen Avataren gespielt haben, gaben nur 20 Prozent (absolut 125) an, bereits sexuell belästigt worden zu sein. Dieses Ergebnis ist ein Hinweis darauf, dass die Wahl des Geschlechts des Avatars eine Auswirkung auf die Häufigkeit der erlittenen Viktimisierung haben könnte und Nutzer mit weiblichen Spielfiguren und vermutlich auch Nicknames häufiger angesprochen werden als männliche Spielfiguren. Zumindest kann man aber festhalten, dass fast 70 Prozent der Nutzer von Freggers Minderjährige sind und immerhin knapp jeder dritte Nutzer von sexuellen Belästigungen berichtet.

Trotzdem die Polizeiliche Kriminalstatistik (PKS) in Deutschland im Hellfeld eine Steigerung der Anzeigen von entsprechenden Straftatbeständen von 934 im Jahr 2011 um annähernd 50 Prozent auf 1.406 im Jahr 2012 aufweist (BMI, 2013), erscheinen diese Zahlen vor dem Hintergrund, dass Millionen von Kindern täglich in Online-Spielen, Sozialen Netzwerken und Kinder-Chaträumen aktiv sind, relativ gering.

6 In der deutschen PKS ist der entsprechende Eintrag für Straftaten nach §176 Abs. 4 Nr 3. und 4 StGB unter dem Straftatenschlüssel 131.400 zu finden. Zu beachten ist jedoch, dass auch die Schlüssel 131.200 und 131.300 Cybergrooming Delikte beinhalten können, wie die Vornahme sexueller Handlungen vor einer Kamera (BMI, 2013). Da diese Schlüssel jedoch nicht zwischen klassischen Cybergrooming-Delikten, die bspw. vor einer Web-Kamera begangen werden und solchen Delikten unterscheiden bei denen die Täter in einem Raum mit dem Opfer sind, finden deren Aussagen keine Berücksichtigung.

Noch ein Indiz für den Phänomenumfang liefert die Operation Game Over, eine Initiative des Generalstaatsanwaltes des US-Bundesstaates New York. Im Rahmen dieser Operation wurden die Kontaktdaten von nur im Bundesstaat New York vorbestraften und registrierten Sexualtätern mit den Anmeldedaten in Online-Spielen und Spieleumgebungen verglichen (NewYorkStateOffice, 2012-1). Hintergrund dieser Operation waren die in den USA bekannt gewordenen Sexualdelikte, bei denen Spiele als Ausgangspunkt genutzt wurden (Fahey, 2011). Die Datensätze bekam die Staatsanwaltschaft dabei auf Grundlage eines Gesetzes des Bundesstaates, welches vorbestrafte Sexualstraftäter verpflichtet, alle persönlichen Daten und unter anderem auch Providerinformationen und Email-Adressen bekannt zu geben. Diese Email-Adressen gab die Staatsanwaltschaft an kooperierende Spielefirmen u.a. Microsoft, EA-Games, Blizzard, Disney, Sony sowie Apple weiter. Das Ergebnis der ersten Phase dieser Operation im April 2012 war, dass 3.580 Accounts durch Sexualtäter in den Spielen der kooperierenden Firmen registriert und in der Folge gebannt wurden. In einer zweiten Phase Ende Dezember 2012 wurden nochmals 2.100 Accounts verbannt (NewYorkStateOffice, 2012-2). Insgesamt wurden also 5.680 Accounts von Sexualtätern in den teilnehmenden Spielen festgestellt.

Das Ergebnis der ersten Phase dieser Operation im April 2012 war, dass 3.580 Accounts durch Sexualtäter in den Spielen der kooperierenden Firmen registriert und in der Folge gebannt wurden.

Bei der Bewertung dieser Operation müssen aber einige Aspekte berücksichtigt werden. So kann nicht per se davon ausgegangen werden, dass jeder registrierte Täter sich in Spielen angemeldet hat, um hier sexuelle Interaktionen mit Minderjährigen zu suchen. Denn auch unter vorbestraften Sexualtätern wird sich sicherlich die Mehrzahl aus reinem Spielinteresse anmelden. Im Gegenzug muss man bei den Zahlen aber auch berücksichtigen, dass nur die in einem Bundesstaat registrierten Sexualtäter abgeglichen wurden und dann auch nur bei einer begrenzten Anzahl von Spielen. Beispielhaft waren an der Aktion nicht die Spiele der Marken BigPoint, Zynga, Sulake, Gameforge, Riot Games, Turbine, Linden Labs vertreten.

Abschließend soll noch ein weiterer Aspekt in die Betrachtung einfließen. Anfang Juni 2012 berichtete der britische Fernsehsender „Channel4“ über die massiven sexuellen Übergriffe von Pädophilen in Habbo Hotel (Channel4, 2012). Sulake, der Betreiber von Habbo Hotel, sah sich durch den entstandenen öffentlichen Druck gezwungen, jegliche Kommunikation in Habbo stumm zu schalten (Habbokritik, 2012). Dabei spricht allein der Umstand, dass Sulake zunächst keine andere Möglichkeit mehr sah, die Übergriffe anders in den Griff zu bekommen, als keine Kommunikation mehr zuzulassen, für einen immensen Umfang von sexuellen Belästigungen in Habbo Hotel.

7. Kinder- und Jugendschutz

Aus dem Blickwinkel des Kinder- und Jugendschutzes leiden gegenwärtig fast alle virtuellen Welten an denselben Mängeln. Sofern Jugendschutzmechanismen vorhanden sind, basieren diese zumeist auf etwaigen Alterseingaben zu Beginn der Anmeldung oder etwaigen Meldefunktionen während der Nutzung. So bekommen Kinder beispielsweise bei der virtuellen Welt Smeet einen Sicherheitshinweis, wenn sie in Kontakt mit Erwachsenen treten wollen. Das Alter, welches aber zum Abgleich herangezogen wird, ist jenes, welches ohne Alterskontrolle durch den Anmeldenden freiwillig zu Beginn angegeben wird. Das dieses System durch einfachste Falschangabe des Alters umgangen werden kann ist offensichtlich. Der nächste offensichtliche Kritikpunkt besteht darin, dass üblicherweise die Reaktionsmechanismen der Betreiber auf ein Reagieren und nicht Agieren hinauslaufen. Beispielhaft findet man häufig den Hinweis, dass Kinder und andere Nutzer umgehend Melde-Funktionen oder Alarm-

buttons nutzen sollen, sofern es zu einer sexuellen Belästigung gekommen ist. Dies wiederum bedeutet aber, dass ein Kind im ungünstigsten Fall schon Texte mit verklausulierten oder eindeutigem sexuellen Inhalt zu lesen bekommen hat und dementsprechend eine Viktimisierung bereits vorliegt. Zudem rekrutieren sich die Ansprechpartner von virtuellen Welten – sogenannte Gamemaster oder Administratoren – vermutlich aus Kostengründen häufig direkt aus den Nutzern der jeweiligen Welt. Dabei wird dieses Personal, welches bei erfolgtem sexuellen Viktimisierungen ggf. als erster Ansprechpartner fungiert, offensichtlich nicht besonders für diese Aufgabe ausgesucht, sensibilisiert oder gar geschult. Dies liegt unter anderem auch darin begründet, dass es hierzu keine staatlichen verpflichtenden Vorgaben gibt. Was umso verblüffender ist, als das der deutsche Staat es für notwendig hält, Cybergrooming gem. §176 IV StGB insbesondere bei Kindern (bis 14 Jahren) unter Strafe zu stellen, aber das gesamte deutsche Jugendschutzsystem für Spiele keine Alterseinstufung ab 14 Jahren kennt.

Daher muss auch die Thematik der Alterseinstufungen noch intensiv hinterfragt werden. Dies gilt insbesondere für die Kriterien der Unterhaltungssoftware Selbstkontrolle (USK) im deutschsprachigen Raum und das Pan European Gaming Information System (PEGI) für den internationalen Bereich. Beide Systeme haben das vornehmliche Problem, dass ihnen noch kein Paradigmenwechsel hin zur Abspiegelung der Kommunikations- und Interaktionsrisiken des onlinebasierten Spielens gelungen ist. Insbesondere die USK, die für Deutschland und einige Bundesländer Österreichs gilt, ist von Gesetzes wegen her nur zuständig für Spiele, die auf Datenträger ausgeliefert werden und dann auch nur für die Frage, ob diese Spiele entwicklungsbeeinträchtigende oder –hemmende Faktoren beinhalten (überwiegend gewalthaltiger und pornografischer Inhalt[7]). Für reine onlinebasierte virtuelle Welten – wie Browser- und Social Games, Game Applikations, die meisten Lifesimulations und MMOPRGS sowie Online-Welten für Kinder – ist die USK gar nicht verpflichtend zuständig, sodass hier überhaupt keine staatlichen Alterseinstufungen vorgenommen werden. Online-Spiele, die hingegen eine Alterseinstufung von der USK bekommen, werden wiederum – vereinfacht dargestellt – auf pornografischen und gewalthaltigen Inhalt hin geprüft, was bei vielen Online-Spielen, die häufig gerade auf einen kindlichen Look setzen, gerade nicht der Fall ist. Problematisch ist dabei zudem, dass in dieser Situation die Betreiber selbst einschätzen, für welches Alter ihre Spiele freigegeben werden, um ein sog. elektronisches und für den normalen Anwender nicht sichtbares Labeling für einen automatischen Abgleich mit Jugendschutz-Programmen zu bekommen. Das Ergebnis ist, dass entsprechende Online-Spiele häufig für Kinder freigegeben werden. Noch ein Punkt sind Online-Spielmodi in Computerspielen, die ja letztlich auch die Kommunikation zwischen den Nutzern vorsehen. Diese können, bedingt durch das Fehlen gesetzlicher Grundlagen, durch die USK bei der Alterseinstufung nicht berücksichtigt werden. Dies hat faktisch zur Folge, dass eigentlich kindgerechte Computerspiele wie Little Big Planet (hier in der PSP Vita Fassung) ab 0 Jahren freigegeben werden und nur auf der Rückseite der Verpackung in einem kleinem Kästchen auf den „Network Modus 2 – 4“, also einem Online-Spielmodus mit anderen, hingewiesen wird. Eltern, die in einem Geschäft ein solches Spiel kaufen und sich in gutem Glauben an den USK-Richtlinien orientieren, sind hier vermutlich für die innewohnenden Kommunikationsrisiken weniger sensibilisiert.

Eltern, die in einem Geschäft ein solches Spiel kaufen und sich in gutem Glauben an den USK-Richtlinien orientieren, sind hier vermutlich für die innewohnenden Kommunikationsrisiken weniger sensibilisiert.

7 Eine ausführliche Darstellung der deutschen Jugendschutzsysteme und ihrer Schwächen können dem Artikel „Kinder- und Jugendschutz vor den Herausforderungen des Web 2.0“ entnommen werden.

PEGI geht hier einen anderen Weg, indem hier zumindest eine eigene Hinweisgrafik für Onlinegaming bei datenträgerbasierenden Spielen vorgesehen wird. Zudem bietet PEGI eine Art freiwilliges Sicherheitszertifikat den „PEGI Online Safety Code (POSC)“ für Firmen von Online-Spielen an, die einen Katalog an Sicherheitsrichtlinien einhalten (PEGI, 2012). Auch diese Vorgehensweise ist jedoch in der jetzigen Form kritikwürdig. Die Freiwilligkeit der Maßnahme bedingt, dass anscheinend eine Vielzahl von Firmen – u.a. Riot Games, Zynga, BIGPoint – nicht an dieser teilnimmt. Zudem beinhaltet der POSC auch keine wirksamen Präventionsmechanismen für Interaktions- und Kommunikationsrisiken. Vielmehr wird darauf Wert gelegt, dass keine jugendgefährdenden Inhalte in den Spielen vorkommen und z.B. entsprechende Meldeverfahren eingeführt werden. Diese Mechanismen sind aber wiederum nur geeignet, erlittene Viktimisierungen zu melden nicht aber diese zu verhindern.

Häufig konnte auch festgestellt werden, dass der Begriff Skype nicht mehr hintereinander in einem Textfenster stand, sondern mit einzelnen Buchstaben in jeweils einem neuen Text-Chat geschrieben wurde, wobei in der Gesamtheit aber klar erkennbar war, worauf es hinauslaufen sollte.

Am Beispiel der Reaktion von Sulake auf den oben beschriebenen Fernsehbericht des englischen Senders Channel 4, der die Missstände dort offenbarte, soll zudem noch die Hilflosigkeit bei der Durchsetzung eines effektiven Jugendschutzes aufgezeigt werden. Zum Hintergrundverständnis ist es hilfreich zu wissen, dass Habbo Hotel eine Art Franchising-Unternehmen ist, das verschiedenste voneinander unabhängige Sprachversionen weltweit unter dem Dach von Sulake betreibt. In den letzten Jahren wurde dabei offensichtlich immer weiter beim Jugendschutz abgebaut (Habbokritik, 2012). So wurden z.B. fremdsprachige Betreuer eingesetzt und keine der Landessprache mächtigen Moderatoren (ebd.). Als Reaktion auf diese Ereignisse versprach Sulake eine massive Verbesserung des Jugendschutzes. Diese sah unter anderem für das deutschsprachige Habbo ein Sicherheitsquiz (fünf einfache Fragen, die man beantworten muss), eine gewisse zeitliche Sperrfrist, ehe man chatten kann[8] (eine halbe Stunde, diese Bedingung existierte z.B. nicht in den englischsprachigen Ausgaben von Habbo) eine verbesserte Blacklist (Wörter, die nicht geschrieben werden dürfen) sowie eine stärkere Einbindung der Community durch sog. Wächter in die Kontrolle der Kommunikation vor. Die beiden einzigen feststellbaren Effekte, waren aber einerseits, dass die Erpressertäter – wie bereits beschrieben – verklausuliert die sexuellen Interaktionen starten und oder diese im Rahmen einer Kommunikation schneller verbannt werden und sich neu anmelden müssen. Wenn früher offen geschrieben wurde *„welches Mädchen mit cam will Sex“* wurde im Ergebnis der Sicherheitsmaßnahmen beispielhaft geschrieben *„welches Mädchen will eine MOLA („Morgenlatte“) sehen“*. Häufig konnte auch festgestellt werden, dass der Begriff Skype nicht mehr hintereinander in einem Textfenster stand, sondern mit einzelnen Buchstaben in jeweils einem neuen Text-Chat geschrieben wurde, wobei in der Gesamtheit aber klar erkennbar war, worauf es hinauslaufen sollte. Andererseits kann aber festgehalten werden, dass Täter offensichtlich bei sexuellen Kommunikationen früher gemeldet und verbannt wurden als dies früher der Fall war und dass Täter häufiger im Rahmen einer sexuellen Kommunikation mit Minderjährigen ihren Avataren wechseln mussten, da dieser jeweils aus dem Spiel entfernt wurde. Dies stellte aber eher ein lästiges Ärgernis für die Täter dar, als eine tatsächliche Hürde. Der Täter kann und konnte diese unkompliziert umgehen, indem er sich entweder mit einem neuen Avatare einloggt oder von vornherein über Multiboxing mit mehreren Avataren vertreten ist. An die wirklichen Schwach-

8 Dieser Sicherheitsmechanismus einer erzwungenen Wartezeit nach einer Anmeldung bevor man in Kontakt mit anderen Nutzern treten kann, wurde im Zeitraum Februar / März 2013 von Habbo Hotel erneut abgeschafft, sodass die Erstellung von neuen Avataren nach einer Bannung unproblematisch erfolgen kann. Dies hat erneut zu einem spürbaren Anstieg der sexuellen Kommunikation im deutschsprachigen Habbo geführt.

punkten, dass es keine vernünftige Überprüfung gibt, wer und mit welchem Alter sich den überhaupt in Habbo Hotel anmeldet, ist Sulake nicht herangegangen. Dies sieht auch die Community von Habbo Hotel so und beschreibt die getroffenen Maßnahmen bisher eher als ineffektiv (ebd.).

8. Fazit

Sicherheitsbehörden und Politiker weltweit akzeptieren mittlerweile Soziale Netzwerke wie Facebook und Google Plus als Plattformen von kriminogener Relevanz und entwickeln polizeiliche Reaktions- und Präventionsmechanismen (Denef et. al., 2012). Onlinegames und virtuelle Spieleumgebungen für Kinder standen bisher, trotz ihrer immensen Beliebtheit bei Minderjährigen und den Möglichkeiten einer anonymen Kontaktaufnahme mit den Nutzern, nicht auf der sicherheitspolitischen Agenda. Dies kann auch sehr gut daran verdeutlicht werden, dass Sulake, der Betreiber von Habbo Hotel, Ende 2011 durch die Europäische Kommission in die digitale Koalition führender Technologie- und Medienunternehmen zur Schaffung eines für Kinder sicheren und freundlichen Internets aufgenommen wurde (Europa, 2011). Eine einfache Überprüfung von Habbo Hotel oder Internetrecherche hätte jedoch bereits zu diesem Zeitpunkt die immensen sexuellen Belästigungen aufzeigen können, denen die Nutzer ausgesetzt sind und waren. Virtuelle Welten und insbesondere Online-Spiele werden jedoch – nach einem kurzem Aufflackern des Interesses rund um Second Life in den Jahren 2007 / 2008 – immer noch nicht in dem wünschenswerten Maße als Plattformen von Tathandlungen und letztlich Opferwerdungen akzeptiert (Krebs & Rüdiger, 2010).

Die Betreiber sind bisher nicht hinreichend gesetzlich verpflichtet, effektiv den Schutz von Minderjährigen sicherzustellen. Beispielsweise indem Nutzer in Kinderspielen oder solche die für Kinder freigegeben sind, aus der Anonymität gezogen werden – z.B. über ein Post-Ident-Verfahren. Hier erscheint es notwendig, eine Gesetzesinitiative einzuleiten, die sowohl für den deutschen Sonderweg als auch für den europäischen Markt verpflichtend sein sollte, um einerseits Wettbewerbsverzerrungen zu verhindern und andererseits einen möglichst effektiven Kinder- und Jugendmedienschutz zu gewährleisten.

Diese mangelnde politische und gesellschaftliche Aufmerksamkeit ist umso problematischer, da weitere Instanzen der sozialen Kontrolle – wie Eltern und Erziehungsberechtigte – teilweise die Risiken virtueller Welten aufgrund fehlenden medialen Wissens über solche, nicht immer erfassen und in den richtigen Kontext setzen können. Faktisch führt dies zu einer geringeren Sensibilisierung und kann somit auch zu einem erhöhten Viktimisierungsrisiko bei den Minderjährigen führen. Diesen Umstand darf ein Staat nicht übersehen und sollte handeln. Wie er das könnte, zeigt unter anderem die niederländische Polizei in Habbo Hotel mit ihrem Projekt DigiKids (siehe Artikel „Dutch police, vision on youth and internet“). Hier muss der Umgang genauso selbstverständlich werden wie es gegenwärtig bei den klassischen sozialen Netzwerken eingeleitet wurde.

Vor dem Hintergrund der rasant wachsenden gesellschaftlichen, ökonomischen und sozialen Bedeutung virtueller Welten erscheint eine politische Auseinandersetzung insbesondere mit den sozialen Interaktions- und Kommunikationsrisiken unvermeidbar. Erste Initiativen, wie die Durchführung einer Veranstaltung zum Kinder- und Jugendschutz in virtuellen Welten durch den Innenminister des Landes Brandenburg im September 2012, zeigen dass hier ein Umdenken eintritt (Woidke, 2012).

Onlinegames und virtuelle Spieleumgebungen für Kinder standen bisher, trotz ihrer immensen Beliebtheit bei Minderjährigen und den Möglichkeiten einer anonymen Kontaktaufnahme mit den Nutzern, nicht auf der sicherheitspolitischen Agenda.

Quellen und Literaturverzeichnis

Blizzard (2010): World of Warcraft subscriber base reaches 12 million worldwide onlineverfügbar unter http://eu.blizzard.com/en-gb/company/press/pressreleases.html?id=2443926 zuletzt geprüft am 07.02.2013.

Breichler, Inge / Knierim, Katja / Lübbesmeyer, Nina (2009): Chatten ohne Risiko? Sicher kommunizieren in Chat, Messenger und Community. Jugendschutz.net, Mainz.

Bullens, Ruud (1995): Der Grooming-Prozess – oder das Planen des Missbrauchs. In: Marquardt-Mau, B. (Hg.): Schulische Prävention gegen sexuelle Kindesmisshandlung. Grundlagen, Rahmenbedingungen, Bausteine, Modelle, München.

Bundesministerium des Innern (BMI) (2013): Polizeiliche Kriminalstatistik 2012, Berlin

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom-1) (2012): Zahlungsbereitschaft für Online-Games steigt. Online verfügbar unter http://www.bitkom.org/files/documents/bitkom-presseinfo_online-gaming_07_11_2012.pdf, zuletzt geprüft am 07.02.2013.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom-2) (2012): Gaming wird immer populärer. Online verfügbar unter http://www.bitkom.org/de/presse/74532_73098.aspx, zuletzt geprüft am 08.02.2013.

Bundesverband Interaktive Unterhaltungssoftware e. V. (BIU) (2011): Marktzahlen - Virtuelle Zusatzinhalte. Online verfügbar unter http://www.biu-online.de/de/fakten/marktzahlen/virtuelle-zusatzinhalte.html, zuletzt geprüft am 08.02.2013.

Bundesverband Interaktive Unterhaltungssoftware (BIU) (2012): Games-Report 2012. Zahlen und Fakten zur Deutschen Games-Industrie. Online verfügbar unter http://www.biu-online.de/fileadmin/user_upload/pdf/games_report_2012_druck.pdf, zuletzt geprüft am 08.02.2013.

Chalk, Andy (2010): Gamer Arrested For Using WoW Gold to "Groom" Underage Boys. Online verfügbar unter http://www.escapistmagazine.com/news/view/98088-Gamer-Arrested-For-Using-WoW-Gold-to-Groom-Underage-Boys, zuletzt geprüft am 08.02.2013.

Channel4 (2012): Should you let your child play in Habbo Hotel? Channel4. Online verfügbar unter http://www.channel4.com/news/should-you-let-your-child-play-in-habbo-hotel, zuletzt geprüft am 08.02.2013.

Choo, K.(2009). Australian Institute of Criminology Online child grooming: a literature review on the misuse of social networking sites for grooming children for sexuale offences. Online verfügbar unter ^http://www.aic.gov.au/documents/3/C/1/%7B3C162CF7-94B1-4203-8C57-79F827168DD8%7Drpp103.pdf, zuletzt geprüft am 07.02.2013.

Cole, Helena / Griffiths, Mark D. (2007): Social Interactions in Massively Multiplayer Online Role- Playing Gamers. In CyberPsychology & Behavior Volume 10, Number 4, S. 575 – 583.

Daily Mail (2009): Primary school teacher facing jail for sending lewd texts to schoolboy after grooming him on World of Warcraft. Online verfügbar unter http://www.dailymail.co.uk/news/article-1115603/Primary-school-teacher-facing-jail-sending-lewd-texts-schoolboy-grooming-World-Warcraft.html, zuletzt geprüft am 08.02.2013.

Denef, Sebastian; Kaptein, Nico; Bayerl, Petra S.; Ramirez, Leonardo (2012): Best Practice in Police Social Media Adaptation. Composite Comparative Police Studies in the EU.

Durkheim, E.(1965). Kriminalität als normales Phänomen. In: Ders., Die Regeln der soziologischen Methode. 2. Aufl. Neuwied 1965. Auch wiederabgedruckt in: Sack, F./König, R. (Hrsg.): Kriminalsoziologie. 2. Aufl. Frankfurt 1974, S. 3-8.

Dwell (2012): Second Life Statistical

Charts. Online verfügbar unter http://dwellonit.taterunino.net/sl-statistical-charts, zuletzt geprüft am 08.02.2013.

Erenli, K.(2008). Virtuelle Welten – Ausgewählte Aspekte des Vertrags- und Urheberrechts unter Berücksichtigung praxisrelevanter Problemstellungen. Universität Wien, Universitätslehrgang für Informationsrecht und Rechtsinformation.

Europa (2011): Self regulation: responsible stakeholders for a safer Internet. Online verfügbar unter http://ec.europa.eu/information_society/activities/sip/self_reg/index_en.htm, zuletzt geprüft am 08.02.2013.

Fahey, Mike (2011): Self-Professed Furry Charged With Xbox Live Child Abuse. Kotaku. Online verfügbar unter http://www.kotaku.com.au/2011/04/self-professed-furry-charged-with-xbox-live-child-abuse/, zuletzt geprüft am 08.02.2013.

Finkelhor, David / Mitchell, Kimberly J. / Wolak, Janis / Ybarra, J. Mitchell (2008): Online“Predators” and Their Victims Myths, Realities, and Implications for Prevention and Treatment. In American Psychologist Vol 63, S.111 – 128.

Freggers-Wiki (2011): Freggers Umfrage 2011. Online verfügbar unter http://www.freggers-wiki.de/umfragel/2011_freggers/, zuletzt geprüft am 08.02.2013.

Fritz, Jürgen; Lampert, Christian; Schmidt, Jan-Hinrik; Witting, Tanja (2011): Kompetenzen und exzessive Nutzung bei Computerspielern: Gefordert, gefördert, gefährdet. Zusammenfassung der Studie. Hans Bredow Institut. Hamburg (Schriftenreihe Medienforschung der Landesanstalt für Medien NRW (LfM)). Online verfügbar unter http://www.hans-bredow-institut.de/webfm_send/563, zuletzt geprüft am 08.02.2013.

HabboKritik (2012): Große Stummschaltung ohne Effekt. Da Sulake die Stummschaltung langsam wieder aufhebt, ziehen wir ein Fazit. Online verfügbar unter http://habbokritik.de/artikel/2447, zuletzt geprüft am 08.02.2013.

InStat. (2011). Virtual Goods in Social Networking and Online Gaming. Hg. v. INSTAT. Online verfügbar unter http://www.instat.com/abstract.asp?id=212&SKU=IN1004659CM, zuletzt geprüft am 08.02.2013.

Katzer, Catarina (2007): Gefahr aus dem Netz. Der Internet Chatroom als neuer Tatort für Bullying und sexuelle Viktimisierung von Kindern und Jugendlichen. Dissertation, Universität Köln.

KidsverbraucherAnalyse (KidsVA) 2012 (2012): Die Markt-Media-Studie für junge Zielgruppen im Auftrag des Egmont Ehapa Verlages GmbH. Berlin.

Kinder+Medien, Computer+Internet Studie (KIM) 2010 (2010): Basisuntersuchung zum Medienumgang 6- bis 13-Jähriger in Deutschland. Medienpädagogischer Forschungsverbund Südwest. Online verfügbar unter http://www.mpfs.de/fileadmin/KIM-pdf10/KIM2010.pdf, zuletzt geprüft am 28.02.2013.

Kornhaber, Spencer (2011): Lake Forest Woman Arrested on Suspicion of Sex with 13-Year-Old Boy. LakeforestPatch. Online verfügbar unter http://lakeforest-ca.patch.com/articles/lake-forest-woman-arrested-on-suspicion-of-sex-with-13-year-old-boy, zuletzt geprüft am 08.02.2013.

Krebs, C., Rüdiger, T.G.(2010). Gamecrime und Metacrime. Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Welten. Frankfurt, M: Verl. für Polizeiwiss.

Leschni (2012): PlayStation 3: Sony verkündet 70 Millionen verkaufte Konsolen. Play3.de. Online verfügbar unter http://www.play3.de/2012/11/16/playstation-3-sony-verkundet-70-millionen-verkaufte-konsolen/, zuletzt geprüft am 08.02.2013.

Livingstone, Sonka; Haddon, Leslie Görzig Anke; Olafsson, Kjartan (2011 - 1): Risks and safety on the internet. The perspective of European Children. Key findings from the EU Kids Online survey of 9-16 year olds and their parents in 25

countries. Online verfügbar unter http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Executive_Summary_Full_Findings.pdf, zuletzt geprüft am 09.02.2013.

Livingstone, Sonja; Haddon, Leslie; Görzig, Anke (2011 - 2): EU Kids Online aims to enhance knowledge of the experiences and practices of European children and parents regarding risky and safer use of the internet and new online technologies, in order to inform the promotion of a safer online environment for children. Online verfügbar unter http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/Final%20report.pdf, zuletzt geprüft am 09.02.2013.

Landgericht Saarbrücken (LG Saarbrücken) (2011). Aktenzeichen: 10 S 60/10 vom 22.06.2011.

Meyfarth, M. (2007). Zusammenspiel virtueller und realer Raum Beispiele und Möglichkeiten. Institute of Electronic Business. Online verfügbar unter http://www.mr-meyf.de/docs/Zusammenspiel%20virtueller%20und%20realer%20Raum.pdf, zuletzt geprüft am 10.02.2013.

Middelburg (2010). Urteil Gericht Niederlande Aktenzeichen: 2010/12/700056-10 vom 03.11.2010.

New York State Office (2012-1): Attorney General: "Operation: Game Over". Purges Thousands Of Sex Offenders From Online Video Game Networks. Pressemitteilung vom 05.04.2012. New York. Online verfügbar unter http://www.ag.ny.gov/press-release/ag-schneidermans-operation-game-over-purgesthousands-sex-offenders-online-video-game, zuletzt geprüft am 08.02.2013.

New York State Office (2012-1): Attorney General Schneiderman's "Operation Game Over" Continues With Thousands Of Additional Sex Offenders Purged From Online Gaming Platforms", Pressemitteilung vom 19.12.2013. New York. Online verfügbar unter http://www.ag.ny.gov/press-release/ag-schneiderman%E2%80%99s-%E2%80%9Coperation-game-over%E2%80%9D-continues-thousands-additional-sex-offenders, zuletzt geprüft am 08.02.2013

Pakalski, Ingo (2012): Fast jedes dritte Handy in Deutschland ist ein Smartphone. Online verfügbar unter http://www.golem.de/news/mobilfunk-fast-jedes-dritte-handy-in-deutschland-ist-ein-smartphone-1205-91858.html, zuletzt geprüft am 08.02.2013.

Parrish, Kevin (2011): Man, 54, ‚'Marries'' Teen in RuneScape, Arrested. Online verfügbar unter http://www.tomsguide.com/us/RuneScape-John-W-Phillips-MMORPG-Sexual-Assault,news-10069.html, zuletzt geprüft am 08.02.2013.

PcGames (2012): World of Warcraft: 30 Prozent Anteil am Umsatz von Activision-Blizzard - Ist der Publisher zu abhängig von WoW? Herausgegeben von PcGames. Online verfügbar unter http://www.pcgames.de/World-of-Warcraft-PC-16678/News/World-of-Warcraft-30-Prozent-Anteil-am-Umsatz-von-Activision-Blizzard-1015757/, zuletzt geprüft am 08.02.2013.

PEGI (2012): Was ist der POSC. PEGI Online. Online verfügbar unter http://www.pegionline.eu/de/index/id/37, zuletzt geprüft am 08.02.2013.

Pfeiffer, Christian; Mößle, Thomas; Kleimann, Matthias; Reh-bein, Florian (2009): Computerspielabhängigkeit und "World of WarcraftWorld of Warcraft". Fünf Thesen zu politischen Folgerungen aus aktuellen Forschungsbefunden des KFN. Herausgegeben von Kriminologisches Forschungsinstitut Niedersachsen. Online verfügbar unter http://www.kfn.de/home/WoW_Thesen_zu_politischen_Folgerungen.htm, zuletzt geprüft am 08.02.2013.

Phagura, Sabi (2012): Police worker who coaxed children into performing webcam ‚sex shows' is jailed Read more: http://www.dailymail.co.uk/news/article-2199095/Police-worker-coaxed-children-performing-webcam-sex-shows-jailed.html#ixzz2KWqVPipz. Online

verfügbar unter http://www.dailymail.co.uk/news/article-2199095/Police-worker-coaxed-children-performing-webcam-sex-shows-jailed.html#axzz2KWqSbzgL, zuletzt geprüft am 28.02.2013.

Pingdom (2012): Internet 2011 in numbers. Online verfügbar unter http://royal.pingdom.com/2012/01/17/internet-2011-in-numbers/, zuletzt geprüft am 18.02.2013.

Rumpf, H. J., Meyer, C. & John, U. (2011): Prävalenz der Internetabhängigkeit (PINTA) Bericht an das Bundesministerium für Gesundheit. Online verfügbar unter http://drogenbeauftragte.de/fileadmin/dateien-dba/DrogenundSucht/Computerspiele_Internetsucht/Downloads/PINTA-Bericht-Endfassung_280611.pdf , zuletzt geprüft am 08.02.2013.

Rüdiger, T.-G.(2012). Cybergrooming in virtuellen Welten. Neue Chancen für Sexualtäter. In: Deutsche Polizei Ausgabe 02/2012, S. 31–37.

Rüdiger, T.-G. (2013-1) Gamecrime und Metacrime - Kriminogene Aspekte virtueller Welten, in: Bigl/Stoppe (eds) ‚Playing with Virtuality', Frankfurt: Peter Lang, S. 397 – 417.

Rüdiger, T.-G. (2013-2) „Legendierte teilnehmende Beobachtung im deutschsprachigen Habbo Hotel am 28.02.2013 im Zeitraum von 13:00 – 16:00 Uhr und am 02.03.2013 im Zeitraum von 12:00 – 12:40 Uhr", tabellenförmige Auswertung unter Anwendung einer Screenshot- und Videodokumentation (unveröffentlicht).

Shaw, Gillian (2012): Amanda Todd: Her story and legacy live on Worldwide, anti-bullying campaigns have been launched following teenager's suicide. Online verfügbar unter http://www.vancouversun.com/news/Amanda+Todd+story+legacy+live/7756533/story.html.

Sulake (2012). Check in to check it out! Online verfügbar unter http://www.sulake.com/Habbo/index.html?navi=2.1, zuletzt geprüft am 08.02.2013.

Tagesspiegel (2012): Zynga-Desaster könnte Facebook-Zahlen belasten. Der Tagesspiegel. Online verfügbar unter http://www.tagesspiegel.de/wirtschaft/soziale-netzwerke-zynga-desaster-koennte-facebook-zahlen-belasten/6924488.html, zuletzt geprüft am 08.02.2013.

Ybarra, Michel / Mitchel, Kimberly (2005): Exposure to Internet Pornography among Children an Adolescents: In CyberPsychology & Behavior Volume 8, Number 5, S. 473 – 486.

YouGov (2012): Fast jedes zweite Kind unter 10 Jahren besitzt ein eigenes Mobiltelefon. Online verfügbar unter http://cdn.yougov.com/r/19/2012_07_PM%20Kinder%20Handy.pdf, zuletzt geprüft am 08.02.2013.

Woidke, Dietmar (2012): Woidke fordert mehr Schutz für Kinder und Jugendliche vor sexuellen Übergriffen bei Online-Spielen, Pressemitteilung des Ministerium des Innern des Landes Brandenburg vom 19.09.2012. Online verfügbar unter http://www.internetwache.brandenburg.de/sixcms/detail.php?gsid=land_bb_polizei_internet_01.c.11215104.de, zuletzt geprüft am 08.02.2013.

Zu dem Autor

Thomas-Gabriel Rüdiger (32), verheiratet und Vater von zwei Töchtern hat an der Universität Hamburg im Studienfach Kriminologie einen Master of Arts erworben. Er ist Kriminologe am Institut für Polizeiwissenschaft der Fachhochschule der Polizei des Landes Brandenburg und forscht hier insbesondere zu den Interaktionsrisiken sozialer Medien und dem polizeilichen Umgang mit diesen. Gegenwärtig promoviert er an der Universität Potsdam in einem intradisziplinären Projekt zur sexuellen Viktimisierung Minderjähriger in virtuellen Welten.

Cyber-Grooming im Lichte der Strafverfolgung[1]

Staatsanwalt Thomas Schulz-Spirohn und
Richterin am Landgericht Kristina Lobrecht

Abstract

Cyber-Grooming, ein in Deutschland bereits seit 2004 bestehender Straftatbestand rückt immer mehr in der Fokus der Medien und der Bevölkerung. Neben den juristischen Problemen, ob bei Onlinespielen und Chats im Internet, tatsächlich der sprachlich veraltete Tatbestand gem. § 176 Abs. 4 Nr. 3 StGB erfüllt ist, bereiten sowohl das Anzeigeverhalten der Tatopfer, aber auch die technische und personelle Ausstattung der Strafverfolgungsbehörden Schwierigkeiten bei der effektiven Verfolgung dieser Straftat. Neben dem Vergleich des deutschen Straftatbestandes mit dem des österreichischen Strafgesetzes wird erörtert, durch welche Maßnahmen der eigentliche Zweck der europäischen Richtlinie 2011/92/EU zur „Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie“ vom 13. Dezember 2011 erreicht werden kann.

1) Einleitung

Cyber-Grooming, d.h. das gezielte Ansprechen von Kindern und Jugendlichen im Internet mit dem Ziel der Anbahnung sexueller Kontakte, ist im deutschen Strafrecht bereits seit dem am 1. April 2004 in Kraft getretenen Sexualdelikte-Änderungs-Gesetz vom 27. Dezember 2003 jedenfalls soweit es sich um „Kinder“ im Sinne des Strafgesetzbuches handelt, unter Strafe gestellt. Dabei versteht der deutsche Gesetzgeber unter dem Begriff “Kinder” Personen unter 14 Jahren (§ 176 des Strafgesetzbuches, StGB), d.h. Personen, die zum Tatzeitpunkt das 14. Lebensjahr noch nicht beendet haben. Dieses sog. Schutzalter variiert innerhalb der europäischen Union erheblich. So liegt das Schutzalter z.B. in Malta[2] bei 12 Jahren, in Irland[3] bei 17 Jahren und im Eu-Anwärterland Serbien[4] bei 18 Jahren. Weltweit gesehen liegt das Schutzalter zwischen dem Beginn der Pubertät (ca. 10 Jahre in Jemen) und 18 Jahren (so auch in einigen Bundesstaaten der USA[5]). Die exakte Feststellung des Alters des/der Geschädigten bedarf deshalb einer eingehenden Prüfung, da bei Personen mit Migrationshintergrund der genaue Geburtstermin fraglich sein kann und Personen über 14 Jahren nach dem deutschen Strafrecht jedenfalls bei „Cyber-Grooming“ kein Schutz gewährt wird und auch die weiterhin in Betracht kommenden Strafvorschriften zum Schutz von Jugendlichen an besondere weitergehende Voraussetzungen geknüpft sind.

Weltweit gesehen liegt das Schutzalter zwischen dem Beginn der Pubertät (ca. 10 Jahre in Jemen) und 18 Jahren (so auch in einigen Bundesstaaten der USA).

2) Tatbestand

Seit der Einführung des Straftatbestandes gilt als Rechtsgrundlage zur Bekämpfung

1 Die kriminologischen Aspekte über die Erscheinungsformen von Cyber Grooming, werden bereits in dem Artikel von Herrn Thomas–Gabriel Rüdiger gesondert erläutert, sodass dieser Artikel nur die rechtliche Seite mit einer Fokussierung auf das deutsche Strafrecht behandeln wird.

2 http://www.welt.de/politik/deutschland/article7319676/Vatikan-erlaubt-Sex-mit-Kindern-ab-zwoelf-Jahren.htmlzum Thema „Schutzalter“

3 Bericht der europäischen Kommission vom 16.11.2007

4 Reise-und Sicherheitshinweise des Auswärtigen Amtes für Serbien

5 Reise-und Sicherheitshinweise des Auswärtigen Amtes für die USA

dieses Kriminalitätsphänomens im deutschen Strafrecht der § 176 Abs. 4 Nr. 3 Strafgesetzbuch (StGB).

Er lautet:
"§ 176 Sexueller Missbrauch von Kindern [...]
(4) Mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren wird bestraft,
3. wer auf ein Kind durch Schriften (§11 Abs.3) einwirkt, um es zu sexuellen Handlungen zu bringen, die es an oder vor dem Täter oder einem Dritten vornehmen oder von dem Täter oder einem Dritten an sich vornehmen lasse soll,[…]
(6) Der Versuch ist strafbar; dies gilt nicht für Taten nach Absatz 4 Nr. 3 und 4 [...]."

Die bis zu diesem Zeitpunkt geltenden Strafvorschriften ahndeten bislang gerade nicht solche Vorbereitungshandlungen, die noch vor dem unmittelbaren Ansetzen zu einem sexuellen Missbrauch lagen.

Dieser mit einigen unbestimmten Rechtsbegriffen versehene und sicherlich auch in seinem Wortlaut nicht mehr zeitgemäße Straftatbestand, soll - legt man die Gesetzesbegründung zu Grunde - den Tatbestand des Cyber-Groomings erfassen.

Hierzu wird in den Gesetzgebungsmaterialien[6] auf einen Pressebericht der Süddeutschen Zeitung von 1999 verwiesen, in dem das Vorgehen von (US-amerikanischen) Internetnutzern beschrieben wird, die sich mit Kindern in den Chatrooms zum Zwecke des sexuellen Missbrauches verabreden. Derartig motivierte Kontaktaufnahmen sollten mit der Einführung des § 176 Abs. 4 Nr. 3 StGB unter Strafe gestellt werden. Die bis zu diesem Zeitpunkt geltenden Strafvorschriften ahndeten bislang gerade nicht solche Vorbereitungshandlungen, die noch vor dem unmittelbaren Ansetzen zu einem sexuellen Missbrauch lagen.

a) Kritik am Tatbestand

Gegen die Einführung dieses Straftatbestandes erhob sich bis zum heutigen Tage massiver Widerstand durch die rechtswissenschaftliche Literatur. Obwohl in der Öffentlichkeit die Notwendigkeit gesehen wird, gerade Kinder vor den Gefahren neuer Medien - insbesondere des Internets - zu schützen, lassen sich kaum positive Stellungnahmen in der juristischen Literatur zu dem Straftatbestand gegen das Cyber-Grooming finden. Es wird von Absurditäten, Ungereimtheiten und widersinnigen Ergebnissen gesprochen[7].

So wird bilanziert[8], der Straftatbestand sei ein *"gut gemeinter, recht hilfloser Versuch einer unkontrollierbarer Kommunikation Herr zu werden"* und habe *"kaum mehr als einen symbolischen Droh-Charakter"*, *"Cyber Grooming ist in Deutschland gar nicht strafbar. Schützt endlich unsere Kinder"*[9] über *"... ist in Deutschland teilweise nicht strafbar, nämlich wenn gechattet wird"*[10] bis hin zu *"auch sozialadäquates Verhalten wird pönalisiert"*[11]. Hierbei wird gegen den Straftatbestand insbesondere zur Begründung angeführt, dass es zu weit gehe, Handlungen lange vor der eigentlichen Verletzung des zu schützenden Rechtsgutes, dem Recht auf sexuelle Selbstbestimmung und dem Schutz der Kinder, unter Strafe zu stellen[12]. Es erstaune zudem, dass Vorbereitungshandlungen für einen Mord gem. § 211 StGB, solange sie noch nicht in die unmittelbare Tatbestandsverwirklichung münden, nicht unter Strafe gestellt sind[13]. Diese Argumente können indes nicht überzeugen. Die Intention des Gesetzgebers, Kinder unter besonderen Schutz zu stellen, zeigt sich in mehreren Gesetzen, in denen auch z.B. Tötungsdelikte von der Wertung her nachrangig behandelt werden, so z.B. bei den Tilgungsfristen im

6 Bundestagsdrucksache 15/350, S. 177

7 so zusammenfassend, Hube, Kriminalistik 2/ 2011, S. 73

8 Fischer, StGB, 59 Auf., § 176, Rn. 15

9 Tatort Internet, RTL II

10 Hörnle, Leipziger Kommentar zum Strafgesetzbuch, 12. Aufl., § 176 StGB, Rn. 87 m.w.N

11 sinngemäß Perron/Eisele in Schönke/Schröder, StGB, 28. Aufl., § 176 Rn. 14

12 Hörnle, a.a.O

13 vgl. StrafO 2004, 265, 267

BZRG[14]. Die mit dem Straftatbestand des § 176 Abs. 4 Nr. 3 StGB erfassten Handlungen sind auch nicht vergleichbar mit den straflosen Vorbereitungshandlungen im Sinne von § 211 StGB. Der Mörder, der sich eine Axt kauft, erwartet nicht bzw. kann nicht erwarten, dass das Opfer der Tat zu stimmt und plötzlich vor ihm steht. Anders ist dies beim Cyber-Grooming. Durch die Anonymität des Internets verschleiert der Täter in vielen Fällen seine wahren Absichten und trifft dabei auf ein kindliches Gegenüber, dass weder Gefahren noch die Konsequenzen seines Handelns erkennt[15]. Dieser konkreten Gefahr für die Kinder kann nur durch ein entsprechend frühzeitig einsetzenden strafrechtlichen Schutz sowie geeignete Präventionsmaßnahmen begegnet werden.

b) Einwirken

Voraussetzung für die Verwirklichung des Straftatbestandes ist gem. § 176 Abs. 4 Nr. 3 StGB das "Einwirken" auf ein Kind durch „Schriften“. Bereits die Feststellung, wann der Täter auf ein Kind im Sinne dieses Gesetzes eingewirkt hat, bereitet in Ermangelung auf § 176 Abs. 4 Nr. 3 StGB bezogener höchstrichterlicher Rechtsprechung einigen Schwierigkeiten. Unter Zugrundelegung der Rechtsprechung des Bundesgerichtshofes – eigentlich zu einem anderen Delikt, nämlich dem alten Straftatbestand des Menschenhandels nach § 180 b Abs. I S. 2 StGB (nunmehr § 232 StGB) –, in dem auch das Tatbestandsmerkmal "einwirken" enthalten war, wird hierunter eine unmittelbare psychische Beeinflussung verstanden, die sich durch eine gewisse Hartnäckigkeit auszeichnet, etwa wiederholtes Drängen, Überreden, Versprechen, Wecken von Neugier, Einsatz von Autorität, Täuschung, Einschüchterung und Drohung[16]. Diese zutreffende Definition, die gerade auch in Hinblick auf das Bestimmtheitsgebot eine einschränkende und klar begrenzte Darstellung strafbaren Verhaltens beinhaltet, kann nach herrschender Meinung[17] auch als Definition im Sinne des § 176 Abs. 4 Nr. 3 StGB herangezogen werden.

Daraus ergibt sich aber auch, dass das einmalige Einwirken auf Kinder, mag es aus unterschiedlichsten Gründen nicht zur Fortsetzung kommen, kein strafbares Einwirken im Sinne dieses Gesetzes darstellt. Mangels Strafbarkeit des Versuches bleibt das einmalige Einwirken daher straffrei.

Der Mörder, der sich eine Axt kauft, erwartet nicht bzw. kann nicht erwarten, dass das Opfer der Tat zu stimmt und plötzlich vor ihm steht.

c) Schriftenbegriff

Die Einwirkung auf das Kind muss durch eine „Schrift“ erfolgen. Die Beeinflussung des Kindes in einer direkten persönlichen Kommunikation oder einem Telefongespräch wird nicht durch den Paragraphen erfasst. Zu den Begriff der Schrift verweist § 176 Abs. 4 Nr. 3 StGB wiederum auf § 11 StGB, der seinerseits in § 11 Abs. 3 StGB eine sog. Gleichstellungsklausel beinhaltet.

In § 11 Abs. III StGB heißt es:
„[...] Den Schriften stehen Ton- und Bildträger, Datenspeicher, Abbildungen und andere Darstellungen in denjenigen Vorschriften gleich, die auf diesen Absatz verweisen.“
Tatsächlich ist allgemein anerkannt, dass Chatprotokolle oder Kommunikationen während eines Onlinespieles, keine Schriften im Sinne von § 11 StGB darstellen. Die sich in der Bevölkerung aufdrängende Frage, warum etwas Geschriebenes keine Schrift darstellen soll, lässt sich allein mit dem strengen Maßstäben gem. § 11 StGB erklären. Danach setzt der Begriff „Schrift“ eine Verkörperung voraus und erfasst daher allein das auf Papier bzw. auf anderen transportablen und ohne Weiteres durch jedermann wahrnehmbaren Materialen geschriebene Wort voraus[18].

14 vgl. § 46 Abs. 3 BZRG im Verhältnis zu § 46 Abs. 4 BZRG

15 vgl. auch zusammenfassend den Artikel von Rüdiger

16 vgl. BGHSt 45, 158; BGH NStZ 2000, 86

17 vgl. NStZ 2011, 455; BGHSt 29, 30; NStZ 1991, 45

18 vgl. Prof. Dr. Marco Gercke, Aufsatz “Was wirklich strafbar ist-vielleicht“ vom 20.10.2010 aus „Legal

Daraus folgt, dass beim „Cyber-Grooming“ allein der Begriff des „Datenspeichers“ für die Feststellung der Tatbestandsmäßigkeit relevant sein kann. Unter dem Begriff des „Datenspeichers“, der erst im Jahre 1997[19] in § 11 Abs. 3 StGB eingefügt wurde, versteht man zunächst Speichermedien für elektronische, elektromagnetische, optische, chemische oder sonstige Aufzeichnung von Daten, welche ihrerseits gedankliche Inhalte verkörpern[20]. Nach zutreffender herrschender Meinung werden auch nicht permanente elektronische Arbeitsspeicher von Computern jeder Art und von Netzwerkservern hierbei erfasst[21]. Kommunikationen, deren Inhalte in einem Datenspeicher für längere Zeit festgehalten werden, fallen also unter den Schriftbegriff. Kontakte mittels E-Mail erfüllen deshalb das Tatbestandsmerkmal "Einwirken durch eine Schrift", ebenso beispielhaft Kontakte mittels „SMS“.

Denn auch bei einer Echtzeitübertragung erfolgt eine Speicherung des Textes zumindest kurzfristig auf dem PC des Täters bevor der Text abgesendet wird.

Problematisch und umstritten ist jedoch die Frage, ob Kontakte in Online-Spielen, Lebens-Simulationen, Chatrooms oder sozialen Netzwerken wie ICQ, Skype oder Facebook unter den Begriff des „Datenspeichers“ fallen. Ihnen ist gemein, dass es sich um eine Echtzeitübertragung mit nur einer kurzfristigen Speicherung auf dem Arbeitsspeicher handelt.

Hierzu wird unter anderem die Auffassung vertreten, es komme auf eine zumindest vorübergehende Ablage im Arbeitsspeicher an[22]. Bei einer Echtzeitübertragung ohne eine solche Zwischenprüfung – wie wohl bei allen Chats oder Online-Spielen – würde nicht durch eine Schrift eingewirkt werden, da lediglich eine kurzfristige Ablage im Zwischenspeicher erfolge[23].

Diese strenge Sichtweise widerspricht sowohl der offensichtlichen Intention des Gesetzgebers, durch den Straftatbestand Verhaltensweisen im Internet unter Strafe zu stellen, bei denen es um das Einwirken durch das geschriebene Wort, d.h. durch Gedankeninhalte, geht und zum anderen entbehrt die Sichtweise auch jeglichen praktischen Nutzen.

Denn auch bei einer Echtzeitübertragung erfolgt eine Speicherung des Textes zumindest kurzfristig auf dem PC des Täters bevor der Text abgesendet wird[24]. Soweit jederzeit durch einen sog. „Screenshot“ der geschriebene Text gespeichert und ausgedruckt werden kann, kann er verkörpert werden und ggf. in einem gerichtlichen Verfahren nach § 249 ff. StPO verlesen werden. Durch das Merkmal der „Verkörperbarkeit“ erreicht auch das im Internet geschriebene Wort eine Gleichstellung zu der gewöhnlichen Schrift im Sinne von § 11 StGB und wird damit der gesetzgeberischen Intention gerecht.

Jedoch kann in diesem Zusammenhang festgehalten werden, dass der vom deutschen Gesetzgeber verwendete Schriftbegriff nicht mehr zur gegenwärtigen technischen Entwicklung passt und daher zeitnah ersetzt werden müsste.

d) Vollendung der Tat

Vollendet ist die Tat bereits dann, wenn das Kind den Inhalt der Schrift(en) zur Kenntnis genommen hat. Es kommt nicht darauf an, ob der Täter Erfolg hat, d.h. das Kind sich mit ihm trifft. Ein "Einwirken" liegt demnach auch dann vor, wenn das Kind nicht in der vom Täter gewünschten Weise reagiert.

Tribune-Online“

19 eingefügt durch Art. 4 Nr. 1 IuKDG vom 22.07.1997 [BGBL. I 1870]; RegE BT-Drs. 13/7385, 35

20 vgl. Thomas Fischer a.a.O., § 11, Rn. 36.

21 vgl. BGHSt 47, 55ff; JR 2000, 125; NJW 2000, 1051

22 Hörnle, a.a.O, BGH NJW 2001,3558, NJW 2010, 1893, Radtke in Münchener Kommentar zum StGB, 2. Aufl. zu § 11, Rn. 147

23 Radtke a.a.O.

24 vgl. Renzikowski, Münchener Kommentar zum Strafgesetzbuch, 2. Aufl., § 176 Rn. 39

e) Vorsatzproblematik

In subjektiver Hinsicht ist die Absicht des Täters zur Verwirklichung einer Tathandlung nach § 176 Abs. 4 Nr. 3 StGB erforderlich, dass es zu sexuellen Handlungen des Kindes mit oder vor dem Täter oder einer dritten Person kommen soll. Die Absicht, das Kind solle allein an sich sexuelle Handlungen vornehmen, genügt daher nach dem Gesetzeswortlaut nicht, ebenso wenig die Absicht des Täters, sich exhibitionistisch vor dem Kind zu betätigen oder in späterer Kommunikation über das Internet sexualbezogene Gespräche zu führen.

Kommuniziert der Täter in der Hoffnung, ein Kind zu finden, das von sich aus sexuelle Kontakte sucht, handelt er nicht in der Absicht, das Kind zu sexuellen Handlungen zu bringen. So die einhellige Meinung in der Strafrechtswissenschaft[25].

Für die Strafbarkeit nach § 176 Abs. 4 Nr. 3 StGB genügt dabei auch eine nach außen hin harmlose Kommunikation, wenn der Täter damit beabsichtigt, das Kind zu sexuellen Handlungen zu verleiten, und die Kommunikation die Schwelle zur Hartnäckigkeit entsprechend überschritten hat.

Daraus folgt für die forensische Praxis ein erhebliches tatsächliches Problem bei der Entscheidung über entsprechende Cyber-Grooming- Fälle. Dieser innere Tatbestand, lässt sich, sollte kein Geständnis des Täters vorliegen, nur mit Mühe anhand von Indizien nachweisen. Eine geschickte Verteidigungsstrategie gerade bei der Vorsatzproblematik kann in diesen Fällen eine entsprechende Verurteilung verhindern. Ohne entsprechende verlesbare Verkörperungen der Kommunikation oder Zeugen (Eltern oder andere Kinder), die bei der Kommunikation zu gegen waren, wird die Beweisführung daher schwierig, aber nicht unmöglich. Gem. § 176 Abs. 4 Nr. 3 StGB genügt der sog. Eventualvorsatz zur Erfüllung des subjektiven Tatbestandes, d.h. der Beschuldigte braucht es nur für möglich zu halten, dass er mit einem Kind kommuniziert. Kommuniziert er trotzdem mit dem Kind, nimmt er es billigend in Kauf bzw. findet sich damit ab und erfüllt damit den subjektiven Tatbestand[26]. Etwaige Verurteilungen scheitern deshalb nicht bereits an der Einlassung eines Beschuldigten: *"Ich dachte, das ist doch alles nur Fantasie, ein Rollenspiel, in Wahrheit wäre das ein Erwachsener."* Denn diese Aussage wird anhand der festgestellten oder bekannten Tatsachen im Rahmen des Verfahrens überprüft. Hierbei sollte man überprüfen, in welchen sozialen Netzwerk oder virtuellen Welten fand die Kommunikation statt, welche sexuellen Präferenzen hat der Beschuldigte, in welchen sozialen Netzwerken oder Spielen spielte er.

Dieser innere Tatbestand, lässt sich, sollte kein Geständnis des Täters vorliegen, nur mit Mühe anhand von Indizien nachweisen.

f) Fazit

Im Ergebnis einer ersten rechtlichen Prüfung kann festgehalten werden, dass das auf Kommunikation basierende Cyber-Grooming bereits nach dem seit 2004 geltenden Strafrecht von § 176 Abs. 4 Nr. 3 StGB erfasst wird und strafbar ist, insbesondere erfüllt er die Vorgaben "Richtlinie des Europäischen Parlamentes und des Rates zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornographie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates" vom 4. November 2011. Hierbei ist auch zu berücksichtigen, dass der Strafrahmen des § 176 Abs. 4 Nr. 3 StGB deutlich höher, als durch die Richtlinie gefordert (in der Richtlinie eine Höchststrafe von einem Jahr), ist und Deutschland diesen Straftatbestand bereits zu einem Zeitpunkt eingeführt, als es noch nicht hierzu verpflichtet war.

3) Vergleich zwischen dem deutschen und dem österreichischen Tatbestand

Insgesamt führte die besagte Richtlinie in den europäischen Ländern zu verschiedenen neuen Straftatbeständen, bei denen

25 Hörnle a.a.O. Rn. 92

26 Fischer a.a.O. Rn. 30

die Formulierungen von besonderem Interesse sind. Nachfolgend soll daher ein Vergleich mit der österreichischen Regelung erfolgen.

Durch § 208a StGB des Landes Österreich, eingeführt durch die Strafrechtsnovelle 2011 und in Kraft getreten am 1.01.2012 wird das Cyber-Grooming und weitere entsprechende Anbahnungstaten unter Strafe gestellt.

Entgegen dem deutschen Straftatbestand hat der österreichische Gesetzgeber nicht nur Cyber-Grooming, sondern jegliche Kontaktaufnahme, auch im realen Raum, zu sexuellen Zwecken gegenüber Kindern unter Strafe gestellt.

§ 208a StGB lautet:

„(1) Wer einer unmündigen Person in der Absicht, an ihr eine strafbare Handlung nach den §§ 201 bis 207a Abs. 1 Z 1 zu begehen

1. im Wege einer Telekommunikation, unter Verwendung eines Computersystems oder

2. auf sonstige Art unter Täuschung über seine Absicht ein persönliches Treffen vorschlägt oder ein solches mit ihr vereinbart

und eine konkrete Vorbereitungshandlung zur Durchführung des persönlichen Treffens mit dieser Person setzt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.

(2) Nach Abs. 1 ist nicht zu bestrafen, wer freiwillig und bevor die Behörde (§ 151 Abs. 3) von seinem Verschulden erfahren hat, sein Vorhaben aufgibt und der Behörde sein Verschulden offenbart.“

Entgegen dem deutschen Straftatbestand hat der österreichische Gesetzgeber nicht nur Cyber-Grooming, sondern jegliche Kontaktaufnahme, auch im realen Raum, zu sexuellen Zwecken gegenüber Kindern unter Strafe gestellt. Während der Ministerialentwurf[27] nur die Kontaktaufnahme über Telekommunikationsmittel und Computersysteme erfasste, wurde die Regierungsvorlage auf jegliche Kontaktaufnahme „unter Täuschung über seine Absicht“ ausgedehnt. Obwohl auch gegen die Einführung dieses Straftatbestandes massive Kritik geübt wurde, führte dennoch die Verpflichtung zur Umsetzung der europäischen Richtlinie und der Aspekt, ein deutliches Zeichen der Bekämpfung von sexuellen Missbrauch von Kindern zu setzen[28], letztendlich zum Erlass des Gesetzes in der dargestellten Form. Dabei ist im Vergleich zum deutschen Tatbestand positiv hervorzuheben, dass dem oben genannten Problem des „Schriftbegriffes“ durch die pauschale „Verwendung eines Computersystems“ entgegengewirkt wird. Diese Formulierung ist zeitgemäß und zukunftsorientiert, erfasst es doch auch weitere technische Entwicklungen, die möglicherweise nicht mehr unter den deutschen „Schriftenbegriff“, aber unter den österreichischen Begriff des „Computersystems“ zu subsumieren sind.

Dennoch ergibt sich auch bei dem österreichischen Straftatbestand eine offensichtliche Lücke im Straftatbestand. Der Täter, der als Erwachsener nur über sein Alter, nicht aber über seine Absicht täuscht, wird von dem Tatbestand nicht erfasst. Die tatsächlichen Erscheinungsformen des Cyber- Groomings[29] beinhalten aber auch den Täter, der die sexuelle Neugierde pubertierender Kinder ausnutzt und offen über das Thema Sexualität spricht und dessen Täuschungshandlung allein in der korrekten Altersangabe zu sehen ist. Wie die österreichische Rechtsprechung letztendlich diese Problematik löst, bleibt abzuwarten.

Zutreffend hat der österreichische Gesetzgeber zusätzlich zu der Kontaktanbahnung ein weiteres objektives Tatbestandsmerkmal eingefügt, indem es „eine konkrete Vorbereitungshandlung zur Durchführung des persönlichen Treffens“ mit dem Kind verlangt. Ungeklärt bleibt jedoch, was eine konkrete Vorbereitungshandlung in diesem Sinne ist. Bei einem Treffen mag es im Zweifel auch nicht viele Vorbereitungs-

27 Vgl. KU Aktuelle Kriminalpolitik 4. Einheit zu § 208a StGB-Österreich

28 KU Aktuelle Kriminalpolitik 4. Einheit zu § 208a StGB-Österreich, S. 5

29 hierzu näher auch Rüdiger

handlungen geben. Denkbar wäre jedoch z.B., dass sich der Täter auf den Weg zum Treffen machen muss, z.B. die Fahrkarte kaufen etc. Aber auch diese Konkretisierung obliegt der Rechtsprechung.

Welche Tendenzen sich sowohl auf deutscher als auch auf österreichischer Seite innerhalb der Rechtsprechung ergeben, bleibt abzuwarten. Obwohl der Straftatbestand in Deutschland bereits seit 2004 in Kraft getreten ist, gibt es keine höchstrichterliche Rechsprechung dazu. Das liegt sicherlich daran, dass der Straftatbestand in der Bevölkerung nicht bekannt ist, und daher selten Anzeigen erstattet werden, aber auch daran, dass die Tatopfer – Kinder – aus Scham oder aus anderen Beweggründen – mag es sein, dass sie solche Gespräche im Internet für normal halten – gegenüber ihren Eltern oder Dritten nicht offenbaren. Tatsächlich kommt es typischerweise nur dann zu Anzeigen, wenn die Eltern bzw. Dritte die Kommunikation zufällig verfolgen oder wenn es konkret zu einem entsprechenden Treffen gekommen ist, von dem z.B. die Eltern Kenntnis genommen haben.

Diese Probleme im Anzeigeverhalten sind so auch auf Österreich übertragbar. Bis Oktober 2012 konnten im Bundesland Kärnten seit Einführung des Straftatbestandes lediglich fünf Strafverfahren festgestellt werden[30].

4) Probleme bei der statistischen Erfassung

In Deutschland ist das Aufzeigen des konkreten statistischen Umfanges oder der statistischen Entwicklung von Cyber-Grooming Delikten schwierig, wenn nicht sogar unmöglich, umsetzbar. Dies liegt darin begründet, dass die polizeilichen Kriminalstatistiken (Bund und Länder) das Cyber-Grooming nur zusammen mit dem Vorzeigen pornographischer Abbildungen gegenüber Kindern erfassen. Tatsächlich tritt das Delikt häufig mit dem Vorzeigen oder sogar dem Erstellen pornographischer Abbildungen zusammen auf. Innerhalb der erhobenen Statistik gibt es in den letzten Jahren keine nennenswerten Entwicklungen, was aber nichts über Verschiebungen zwischen den Delikten besagt. Die Verurteilungsstatistik des Bundes erfasst nur den sexuellen Missbrauch von Kindern in allen gesetzlichen Varianten. Auch hier sind keine signifikanten Zuwächse oder Rückgänge in den letzten Jahren zu verzeichnen, woraus nichts über die Entwicklung des Cyber-Groomings geschlossen werden kann. Zu berücksichtigen ist nämlich, dass das Cyber-Grooming gem. § 176 Abs. 4 Nr. 3 StGB, sollte es danach zu darauf beruhenden sexuellen Handlungen gekommen sein, durch den Straftatbestand des § 176 Abs. 1 StGB konsumiert werden und daher zurücktreten. Die Anbahnung interessiert dann allenfalls als Vorgeschehen – der Tathintergrund – und gerät bei der polizeilichen und juristischen Aufbereitung häufig aus dem Blickfeld.

Die Anbahnung interessiert dann allenfalls als Vorgeschehen – der Tathintergrund – und gerät bei der polizeilichen und juristischen Aufbereitung häufig aus dem Blickfeld.

Bislang sind entsprechende Verurteilungen weder in den Kommentaren oder Lehrbüchern zum Strafrecht oder in die Datenbank für das deutsche Recht "Juris" aufgenommen worden.

a) Landgericht Koblenz

Lediglich in der Presse wurde im Dezember 2008 über ein Vergewaltigungsverfahren vor dem Landgericht Koblenz berichtet. Dort hatte ein 53-jähriger eine 14-jährige im Internet in einem Chat überredet, sich mit ihm ohne die Erlaubnis ihrer Eltern am Bodensee zu treffen. Tatsächlich fuhr die 14-jährige zu dem vereinbarten Treffpunkt, wo es sodann zu nicht ausschließbar freiwilligen sexuellen Handlungen kam. Das Landgericht Koblenz sprach den Angeklagten wegen des Tatvorwurfes der Vergewaltigung frei, verurteilte ihn jedoch wegen Kindesentziehung zu einer unbedingten Freiheitsstrafe von einem Jahr und neun Monaten. In der Urteilsbegründung

30 Kleine Zeitung Österreich, Artikel vom 20.10.2012

führte der Richter aus, der „53-Jährige hatte beim Chat nur den Gedanken, junge Mädchen zu sich ins Bett zu bringen“. Dafür habe er sich jünger gemacht und mit "großer List" dem Mädchen "den Lover vorgespielt, der sie auf Händen trägt“. Früher waren es böse Onkels, die Kinder mit Bonbons ins Auto lockten, heute wird das Internet zunehmend zum Ausgangspunkt erheblicher Straftaten, leider auch sexueller. Der Arbeitslose, der täglich mehrere Stunden vor dem PC saß, habe "mit unglaublicher Fantasie, kaum zu überbietender Hartnäckigkeit und unglaublicher Frechheit" gearbeitet. Dafür legte er sich verschiedene Chat-Nicknames ("Spitznamen") wie "Schmusebärchen" oder "Binlieb24" zu und schmückte sein Internet-Profil mit Herzchen oder Blümchen. Als die 14-Jährige von Stress mit den Eltern berichtete, überredete er sie, zum ihm zu ziehen und holte sie mit dem Auto ab.[31]“

Als die 14-Jährige von Stress mit den Eltern berichtete, überredete er sie, zum ihm zu ziehen und holte sie mit dem Auto ab.

b) Landeskriminalamt Berlin

Eine Nachfrage bei den fünf Kommissariaten des Landeskriminalamtes des Bundeslandes Berlin, die sich mit Sexualstrafsachen beschäftigen, ergab eine Schätzung von ca. 20 Verfahren pro Jahr, in den denen der Tatvorwurf des Cyber-Groomings verfolgt wird. Rückschlüsse auf die tatsächlichen Gefahren die vom Cyber-Grooming für die Kinder ausgehen, können daraus aber nicht gezogen werden. Der erst seit neun Jahren bestehende Straftatbestand gegen Cyber-Grooming ist bislang nicht in dem Rechtsbewusstsein Aller so fest verankert, wie andere Straftatbestände, die zum Teil bis auf die alttestamentarischen zehn Gebote bzw. noch früher zurückreichen. Mit der zunehmenden Diskussion in der Presse, auch über das allgemeine Phänomen der Cyber-Kriminalität, und steigender Präventionsarbeit in den Schulen ist für die Zukunft mit einer Sensibilisierung der Bevölkerung und ggf. mit einem höheren Anzeigeverhalten zu rechnen.

Auf Seiten der Strafverfolgungsbehörden besteht jedoch in der Praxis derzeit ein anderes Problem–Cyber-Grooming wird gar nicht erkannt. Beispielsweise erzählt ein Kind eine technisch völlig unwahrscheinliche bis unsinnige Geschichte von "downloaden" und verändern seiner Fotos aus seinen Facebook-Account und dem Versenden solcher Dateien an Dritte. Schnell stellt sich heraus, so kann es gar nicht gewesen sein. Aber so ähnlich! Das Kind schämte sich die Wahrheit zu sagen, dass es von einer fremden Person zum Posieren für kinder- oder jugendpornographische Aufnahmen überredet und damit erpresst wurde. In der Praxis führen solche Angaben eines Kindes vorschnell zu einer Abgabeverfügung der Polizei an die Staatsanwaltschaft mit dem Schlusssatz „Keine Straftat“. Erst bei eingehender Prüfung durch sensibilisierte Ermittler ist auch ein solcher Fall sachgerecht aufklärbar.

5) strafrechtliche und/oder politische Konsequenzen?

a. Benötigen wir gesetzliche Änderungen im deutschen Strafrecht?

Der Straftatbestand des Cyber-Groomings in Deutschland gem. § 176 Abs. VI StGB pönalisiert das entsprechende Verhalten bereits sehr weit im Vorfeld der Rechtsgutsverletzung. Dabei ist das Delikt schon vollendet, wenn ein Kind die Anbahnung auch nur zur Kenntnis nimmt[32]. Eine weitere Ausdehnung des Tatbestandes in Hinblick auf eine Versuchsstrafbarkeit, die bislang ausdrücklich ausgeschlossen ist, geht an der wahren Problematik vorbei und würde in der Praxis keinen Anwendungsbereich mehr haben. Allein die Motivation des Täters, ohne dass sie in der physischen Auswirkungen hat, kann und darf nicht unter Strafe gestellt sein. Ein reines Gesinnungsstrafrecht findet in unseren Gesetzesvorstellungen keinen Halt[33]. Dies gebietet auch der Schutzzweck

31 Stern.de, Artikel „Eingeschleimt, angemacht, verurteilt“ http://www.stern.de/digital/online/urteil-zum-cyber-grooming-eingeschleimt-angemacht-verurteilt-649925.html vom 22.12.2008

32 Fischer a.a.O. Rn. 31

33 Jürgen Rath: *Gesinnungsstrafrecht - Zur Kritik*

der Norm nicht, denn eine Schädigung des Rechtsgutes bei der versuchten Anbahnung ist schon begrifflich ausgeschlossen.

Dennoch stellt sich die Frage, ob das Cyber-Grooming nicht auch noch auf die Straftatbestände des §184 b – „Kinderpornografie“ – und 184 c StGB – „Jugendpornografie“ – ausgeweitet werden sollte. In vielen Fällen geht es dem Täter nicht allein darum, sich mit dem Kind zu treffen, sondern er lässt von dem Kind bzw. dem Jugendlichen pornographisches Bildmaterial erstellen[34]. Das in diesem Zusammenhang ebenso hartnäckig durch den Täter forcierte Verhalten, verwirklicht im Erfolgsfall ebenfalls einen Straftatbestand (§ 184 b und c StGB) und kann erheblichen Einfluss auf die psychische Entwicklung eines Kindes oder Jugendlichen nehmen (vgl. den Fall „Amanda Todd“).

Was in der Praxis große Schwierigkeiten bereitet sind die Fälle, in denen der Altersunterschied zwischen der geschützten Person und dem „vermeintlichen“ Täter des sexuellen Missbrauchs oder des Cyber-Grooming nur gering ist und es sich jedem aufdrängt, dass sich um eine „normale“ sexuelle Beziehung unter Minderjährigen handelt. Ist bei den sexuellen Handlungen eine Person dennoch über 14 Jahren die andere jedoch unter 14 Jahren ist der Straftatbestand gem. § 176 StGB erfüllt. Sowohl die Schweiz[35] als auch Österreich[36] haben daher eine so genannte Altersstoleranzklausel eingeführt. Danach sind in der Schweiz sexuelle Handlungen an Personen unter 16 Jahren (Schutzalter in der Schweiz) dann nicht strafbar, wenn der Altersunterschied zwischen den Beteiligten nicht mehr als drei Jahre beträgt. In Österreich wird zudem differenziert zwischen sexuellen Handlungen mit Geschlechtsverkehr und solchen ohne Geschlechtsverkehr. Sexuelle Handlungen ohne Geschlechtsverkehr sind gem. § 207 Abs. 4 StGB Österreich dann nicht strafbar, wenn der Altersunterschied nicht mehr als vier Jahre beträgt und die jüngere Person nicht jünger als 12 Jahre alt ist. Sexuelle Handlungen mit Geschlechtsverkehr sind gem. § 206 Abs. 4 StGB Österreich nicht strafbar, wenn die jüngere Person mindestens 13 Jahre alt ist und der Partner nicht mehr als drei Jahre älter ist. Beide den sexuellen Entwicklungen von Jugendlichen gerecht werdende Gesetzesfassung bietet sich sowohl für die Begrenzung des sexuellen Missbrauchs als solches als auch des Cyber-Groomings im deutschen Strafrecht an.

b. <u>Brauchen wir strengere/höhere Strafen?</u>

Ein Zusammenhang zwischen Strafhöhe und Prävention ist in der kriminologischen Forschung nicht erwiesen und wird überwiegend verneint[37]. Der gesetzliche Strafrahmen des § 176 Abs. 4 Nr. 3 StGB übersteigt das in der Richtlinie des EU-Rates und Parlamentes vom 4. November 2011 (dort Art. 6 zum Grooming) Strafmaß bereits deutlich. Dort wird eine Höchststrafe von mindestens einem Jahr gefordert. Im deutschen Strafgesetzbuch beträgt die Höchststrafe fünf Jahre, in Österreich nur zwei Jahre. Bei der Wahl des entsprechenden Strafrahmens hat der Gesetzgeber sich auch an die Wertigkeit des Tatbestandes innerhalb des Deliktsbereiches zu halten, aber auch die Strafrahmen der einzelnen Deliktsbereiche müssen innerhalb des Strafgesetzbuches maßvoll miteinander abgewogen sein. So muss auch weiterhin der sexuelle Missbrauch von Kindern ohne körperlichen Kontakt – wie z.B. in § 176 Abs. 4 Nr. 3 StGB – niedriger bestraft sein als der mit körperlichen Kontakt – wie z.B. § 176 Abs. 1 StGB. Im europaweiten Vergleich hat

Ein Zusammenhang zwischen Strafhöhe und Prävention ist in der kriminologischen Forschung nicht erwiesen und wird überwiegend verneint.

der Destruktion des Kriminalunrechtsbegriffs in der Rechtsprechung des Bundesgerichtshofs. Hamburg 2002, siehe auch Prof.Dr. Marco Gehrke a.a.O.

34 vgl. Beitrag von Rüdiger

35 Art. 187 Abs. 2 StGB der Schweiz

36 §§ 206 Abs. 4, 207 Abs. 4 StGB Österreich

37 statt Aller: Eisenberg, Kriminologie, 6. Aufl. § 15

Deutschland hohe Strafen und insgesamt eine vergleichbar hohe Vollstreckungsdichte. Bei der Frage, ob man höhere Strafen braucht, darf zudem nicht außer Acht gelassen, dass viele europäische Länder hohe Strafen auswerfen, tatsächlich jedoch frühzeitig mit der Entlassung der Verurteilten beginnen, während in Deutschland eine Halbstrafenentlassung selten ist und eine Zweidrittelentlassung nicht bei jedem in Betracht kommt.

Der rein technische Umgang mit Internet, Computer etc. ist schnell erlernt, in vielen Schulen inzwischen auch Unterrichtsstoff ab der 2. Klasse, die konkreten Gefahren und die Möglichkeiten, diesen Gefahren zu begegnen, werden jedoch nur selten vermittelt.

c. Brauchen wir andere / höhere Altersgrenzen?

Als Schutzalter bezeichnet man das Alter, von dem ab eine Person juristisch als einwilligungsfähig in sexuelle Handlungen angesehen wird. Dabei hängt das Schutzalter in vielen Ländern von verschiedenen Faktoren ab, z.B. dem Geschlecht, dem kulturellen Verständnis etc. Innerhalb des deutschen Strafrechts existiert kein einheitliches Schutzalter, vielmehr gelten je nach Tatbestand unterschiedliche Altersgrenzen. So bestimmt z.B. § 182 StGB, dass sexuelle Handlungen mit Personen unter 18 Jahren unter bestimmten, dort genannten Voraussetzungen strafbar sind, gem. § 174 StGB können auch sexuelle Handlungen an Jugendlichen strafbar sein, wenn sich diese zu dem Täter in einem Erziehungs-, Ausbildungs- oder Betreuungsverhältnis befinden. Die Grenze des Schutzalters, hier gem. § 176 Abs. 4 Nr. 3 StGB 14 Jahre, beinhaltet die Aussage des deutschen Gesetzgebers, Personen ab diesem Alter seien psychisch und physisch in der Lage über die Frage ihrer Sexualität frei zu entscheiden. Diese Aussage impliziert – wie in vielen Gebieten des Strafrecht – eine voluntatives und ein kognitives Element (vgl. § 16 StGB). Nähert man sich der Fragestellung (höheres Schutzalter) für den Straftatbestand des Cyber-Groomings aus diesem Blickwinkel, muss geprüft werden, ob man den Jugendlichen im Alter von und über 14 Jahren zutraut, Gefahren im Internet zu erkennen, diese richtig einzuschätzen und sich dementsprechend zum Schutz ihrer eigenen sexuellen Selbstbestimmung verantwortungsvoll zu entscheiden. Tatsächlich muss man dies unseren Kindern in dem Alter bereits zutrauen. Im Alter von 12 bis 14 Jahren befinden sich fast alle Kinder auf der Oberschule, sie dürfen alle zur Schule gehen, mit dem Fahrrad fahren etc. Die Aufzählung, was wir unseren Kindern in diesem Alter bereits zutrauen und zutrauen müssen, wäre noch um Einiges fortsetzbar. Das voluntative Element stellt auch in der Gesellschaft daher kein Problem dar. Tatsächlich würde aber niemand, ein Kind Fahrrad lassen, dass nicht Fahrrad fahren kann. Es mangelt jedoch bei vielen Kindern auch noch in diesem Alter an der notwendigen Medienkompetenz. Der rein technische Umgang mit Internet, Computer etc. ist schnell erlernt, in vielen Schulen inzwischen auch Unterrichtsstoff ab der 2. Klasse, die konkreten Gefahren und die Möglichkeiten, diesen Gefahren zu begegnen, werden jedoch nur selten vermittelt.

d. Der Fall Amanda Todd

Im Zeitraum der Erstellung dieses Aufsatzes, wird in den Medien exzessiv über den Fall des kanadischen Mädchens Amanda Todd berichtet. Amanda nahm sich am 10. Oktober 2012 im Alter von 15 Jahren nach jahrelangen Belästigungen, Verhöhnungen und Schmähungen über das Internet das Leben. Sie begann in der siebten Klasse neue Kontakte zu Freunden auch via Internet zu knüpfen. Eines Tages überredete sie ein Cham-Chat-Partner, ihm ihre Brüste zu zeigen. In ihrer Unbekümmertheit folgte Amanda den Drängen des vermeidlichen Freundes. Dieser meldete sich sodann wieder bei ihr und erpresste sie mit den Nacktaufnahmen, die er selbst per Screenshot während des Chats von ihr hergestellt hatte. Als Amanda darauf nicht einging, versendete der Mann die Bilder an ihre Freunde und Bekannte. Amanda wurde depressiv und zerstritt sich mit ihrem Umfeld. Sie wechselte mehrfach

die Schule, unternahm einen ersten Selbstmordversuch. Schließlich nahm sie sich 2012 das Leben.

In juristischer Hinsicht ist im Fall von Amanda Todd mit der Herstellung des Screenshots weder der Tatbestand des Cyber-Grooming noch des Herstellens oder Verbreitens jugendpornographischer Schriften erfüllt. In Betracht käme höchstens eine Strafbarkeit nach § 33 KunstUrhG, die Schmähungen und Verhöhnungen stellen, wobei hierzu nichts näher bekannt ist, vielleicht eine Beleidigung gem. § 185 StGB dar. Auch der Tatbestand der fahrlässigen Tötung gem. § 222 StGB wird im Zweifel nicht erfüllt sein. Dieses „Tatgeschehen" wird zusammenfassend als Cyber-Mobbing verstanden.

Im bundesdeutschen Recht gibt es keinen eigenen Straftatbestand gegen Cyber-Mobbing, jedoch können einzelne Taten gegen deliktische Straftatbestände verstoßen. Hier kommen vor allem die Beleidigungsdelikte gem. §§ 185 ff. StGB, Delikte wegen Verletzung des persönlichen Lebens- und Geheimbereichs nach §§ 201 ff. StGB, Straftaten gegen die persönliche Freiheit §§ 232 ff. StGB insbesondere § 238 StGB (Nachstellung und Stalking) sowie der Verletzung des Rechts am eigenen Bild nach § 22 ff. Kunsturhebergesetz in Betracht. Aber auch Delikte wie das sich Verschaffen von Kinder- und Jugendpornographie nach den §§ 184b und c StGB können hinzutreten.

Die deutschen Straftatbestände sind generell geeignet zur Abwehr der Angriffe auf diese Rechtsgüter. Zum Zeitpunkt des Erlasses der entsprechenden Gesetze[38] war jedoch die Intensität der Angriffe im Vergleich zu den heutigen Möglichkeiten via neue Medien deutlich verringert, eine Beleidigung z.B. konnte nur wenige Personen erreichen. Heutzutage können durch das Internet Millionen von Nutzern Kenntnis von Beleidigungen erlangen. Durch die Möglichkeit rund um die Uhr und aus dem Verborgenen die Betroffenen u.a. zu Verunglimpfen, lächerlich zu machen und massiv unter Druck zu setzen, ist der Schaden für das Rechtsgut erheblich gestiegen. Dieser Entwicklung werden die Tatbestände nicht mehr gerecht. Abgesehen von dem prinzipiellen Einwand, dass es regelmäßig unvernünftig ist, von einem tragischen Fall auf – scheinbar - bestehende Gesetzeslücken zu schließen, kann eine angemessene Bestrafung von über das Internet begangenen Straftaten wie z.B. Beleidigungen etc. aufgrund des erweiterten Wirkungskreises nur dann sachgerecht erfolgen, wenn entweder durch Einfügung eines besonders schweren Falles oder einer Qualifizierungen der Strafrahmen erhöht wird – wie z.B. für die Verleumdung gegen Personen des politischen Lebens nach § 188 Abs. 2 StGB.

Durch die Möglichkeit rund um die Uhr und aus dem Verborgenen die Betroffenen u.a. zu Verunglimpfen, lächerlich zu machen und massiv unter Druck zu setzen, ist der Schaden für das Rechtsgut erheblich gestiegen. Dieser Entwicklung werden die Tatbestände nicht mehr gerecht.

e. Sonstige Schutzvorkehrungen

Neben den genannten gesetzlichen Anpassungen ist ein wirksames Entgegentreten letztlich auch eine gesamtgesellschaftliche Herausforderung. Hier müssen sowohl die Legislative als auch die Exekutive dafür Sorge tragen, dass der Schutzschirm des Strafrechts auch tatsächlich aufgeklappt werden kann. Dies kann aber nur wirksam erfolgen, wenn Polizei und Staatsanwaltschaft die personellen und technischen Ressourcen zur Anwendung der gesetzlichen Vorschriften zur Verfügung gestellt bekommen und eine entsprechende fachliche Medienkompetenz der Beamten sichergestellt wird.

Sogar bei der Verfolgung des Besitzes und Verbreitens von Kinderpornographie kommt die Polizei angesichts ständig wachsender Speicherkapazitäten („Big Data") und neuer Speichermöglichen ("Cloud") an ihre zum Teil veralteten technischen und personellen Grenzen. Aber auch bei der Verfolgung des Cyber-Grooming werden regelmäßig PC's, Laptops und andere Datenträger beschlagnahmen und auszuwerten sein. Diese

38 § 201 StGB z.B. 1967, § 185 StGB im Kern wie im RGStGB

Auswertungen dauern – je nachdem ob tatsächlicher Missbrauchsverdacht oder "nur" Verdacht auf Besitz und Verbreitens von Kinderpornographie besteht und welche Datenmengen gesichtet werden müssen – in der Regel z.B. bei der Berliner Polizei zwischen 2 Wochen und bis zu 3 Jahren.

Weiterhin ist es dringend geboten, für die Verfolgung des Cyber-Groomings das prozessrechtliche Instrumentarium von Polizei und Staatsanwaltschaft den kriminalistischen, kriminologischen und technischen Realitäten anzupassen. Ohne die europarechtlich gebotenen Einführung einer verfassungsfesten Mindestdatenspeicherung[39] (oder auch Vorratsdatenspeicherung genannt) werden Cyber-Grooming und darauf zurückgehende schwerste Sexualverbrechen an Kindern häufig nicht aufzuklären und zu sühnen – in der Folge auch nicht zu verhindern – sein. Werden die erforderlichen prozessrechtlichen Instrumente nicht zur Verfügung gestellt, bleiben Strafvorschriften ausschließlich symbolisch. Aber auch entsprechend technische Maßnahmen – wie dem Aufzeichnen von Kontaktdaten bei der Nennung von Schlüsselwörtern in Online-Kinderspielen – sollten geprüft und erörtert werden[40].

Neben der Unterstützung der Strafverfolgungsbehörden in technischer und personeller Hinsicht ist die Aufklärungsarbeit an Schulen wesentlich. Kinder müssen nicht allein wissen, wie man einen Computer und das Internet benutzt. Sie müssen über Gefahren und Wirkungsweisen von Veröffentlichungen im Internet aufgeklärt werden und dies zu einem Zeitpunkt, wo sie beginnen, das Internet zu nutzen. Das kann und wird zunehmend schon in den ersten Klassen der Fall sein. Präventionsprogramme an Schulen[41] sind sinnvoll, aber auch die Aufklärung der Eltern sollte ein wesentlicher Bestandteil sein. Nur wenn Eltern wissen, was ihre Kinder im Internet tun, können sie Einfluss nehmen.

Zu den Autoren:

Thomas Schulz-Spirohn ist Staatsanwalt in Berlin und Vater von zwei Kindern. Er studierte von 1983-1989 Rechtswissenschaften an der Freien Universität Berlin. Nach dem Referendariat war er zunächst als wissenschaftlicher Mitarbeiter bei der Bundesanwaltschaft und anschließend als Staatsanwalt in Berlin in verschiedenen allgemeinen- und Spezialabteilungen tätig. Seit dem Jahr 2002 arbeitet er in der Abteilung für Sexualstrafsachen, gewaltverherrlichende, pornografische und jugendgefährdende Schriften.

Kristina Lobrecht, Mutter von zwei Kindern, studierte an der Freien Universität Berlin Rechtswissenschaft mit dem Schwerpunktfächern Kriminologie und Rechtsphilosophie. Nach einer anderthalb jährigen berufspraktischen Tätigkeit auf dem Gebiet der Zwangsvollstreckung und der Abwicklung vereinigungsbedingter Sonderaufgaben absolvierte sie mit dem Schwerpunkt Strafrecht ihr Referendariat in Berlin und anschließend das 2. Staatsexamen. Seit 2011 ist sie Richterin am Landgericht und dort im Betäubungsmittelstrafrecht tätig. Zusätzlich ist sie Referentin für das Aus-und Fortbildungsdezernat beim Kammergericht.

39 vgl. die Richtlinie 2006/24/EG vom 15. März 2006

40 Siehe hierzu auch den Artikel von Prof. Dr. Lucke.

41 z.B. im Landkreis Teltow-Fläming (Brandenburg)

Dutch police, vision on youth and the internet

Solange Jacobsen and Manuel Mulder

Abstract

The Dutch police has chosen to be actively in contact with young people on the internet. The underlying belief is that, for the police Youth task (prevention, signaling, advise and repression) to perform optimally, it is of crucial importance to be present in the virtual world. It is the only way to be in intensive contact with them, find out what they are doing and be there for them if they need the police.

There is a website for youngsters at www.vraaghetdepolitie.nl, twitter is used frequently, an awareness game (at www.kenjevrienden.nu) has been developed, and there is even a police officer in the virtual Habbo hotel with its own police station. There is a toolbox for police officers providing assistance and case studies on how to deal with youth (problems) and the internet. The how and why are explained by Solange Jacobsen and Manuel Mulder in this article. They sketch the current context, including the many forms of internet use and abuse, that young people face these days.

1. Digitization of society

1.1. Media use in the Netherlands

Recent research[1] indicates that 94% of households in the Netherlands have a fixed internet connection. The Netherlands is the leader in Europe, followed by Denmark, Sweden and Luxembourg (all 92%). In Europe the average is 76%. Four years ago 86% of Dutch households had internet access.

Almost 60% of Europeans use the internet daily. More than seven out of ten people go online at least once a week. The penetration of fixed internet connections is stagnating. Mobile internet on the other hand is growing exponentially. A third of Europeans between the ages 16 and 74 makes use of mobile internet. The rate among young people aged 16 to 24 is much higher: 58%.

Mobile internet growth

Recent research[2] conducted by the CBS (Dutch Central Statistical Office) also shows that mobile internet use is increasing. The number of internet users in the Netherlands in 2012 was 12.4 million, which equals 96% of all 12 to 75-year-olds. Six out of ten internet users use mobile devices. This is a threefold increase compared to 2007. Especially among young people, the use of mobile internet has increased. In 2007, 21% of young people aged 12 to 25 were online with their mobile device. In 2012, this has grown to a staggering 86%.

Growth of mobile devices

The rise of the smartphone and tablet especially has led to an increase in mobile internet use. Users maintain their contacts this way. Nearly three-quarters of them use email and almost two-thirds participate in social networks such as Hyves, Facebook and Twitter. Reading news and newspapers (62%) and playing games and listening to music (58%) are favorite pursuits, too. They do not only use mobiles devices while out and about, but also at home even when a fixed internet connection is available.

They do not only use mobiles devices while out and about, but also at home even when a fixed internet connection is available.

Four out of ten internet users do not use mobile equipment. Nearly three quarters of them (73%) indicate no need for internet outside home or work. High cost is

1 Eurostat ‚Statistics in Focus ,, week 50/2012

2 CBS, Statline, ICT use of households and persons, October 2012

mentioned in 16% of the cases as a reason not to go online with a mobile device.

Popularity of social media

Previous research of the CBS zoomed in on the use of media. It showed that more than half (53%) of internet users in 2011 were active on social networks such as Hyves, Facebook and Twitter. Especially young people up to 25 use it a lot (88%). In addition, one in five internet users is active on the business networking site LinkedIn.

Young people are growing up with "2.0" and find it obvious that they can influence websites themselves by posting content, responding to content, receiving responses, making contacts with friends, 'friends of friends' and strangers.

1.2. Digital youth culture

In recent years various national and international studies have looked into the use of media by young people from a great number of angles. How many young people are online? How often? What do they do when they are? How do they do that? What influence has media use on their development? What influence has media use on school performance?

The common denominator in all research is very clear: media plays an ever increasing role in the daily lives of children and young people. There is more to conclude from these studies:

- the average age at which young people go online is dropping;
- the frequency and intensity of media use is increasing;
- there are more risks online than young people think;
- young people are less media-savvy than adults.

1.2.1. Growing up and developing with media

Young people today grow up with an overkill of media and are more "connected" than ever. They spend more time on the internet than watching television and they are constantly connected to their networks. Moreover, watching television is done through the internet at a time that suits them! With their smartphones they can, at any time and from any location, be in contact with whomever they want, gather and share information, and have fun with all conceivable forms of entertainment.

EU Kids Online Research[3] shows that 93% of 9-16-year-olds go online at least once a week and 60% do it (almost) daily. Age is a strong determining factor; the older, the more intensive. Of the 9 to 10-year-olds who use the internet, 30% are online daily. Of all 15-16-year-old internet users the figure is 80%. The average age at which children start actively using the internet for the first time is seven years.

The transition from primary education to secondary education seems a natural time for children to get their own mobile phone. The table below from the study "Hey, what's app?"[4] about the possession and use of cell phones shows that 75% of all 9-11-year-olds have their own phone. From 12 years, this figure rises to 98%.

Source: Mijn Kind Online "Hey, what's app?"

Decide "what, when and how"

Young people are growing up with "2.0" and find it obvious that they can influence websites themselves by posting content, responding to content, receiving responses, making contacts with friends, 'friends of friends' and strangers. Hidden behind vague profile pictures or avatars they exercise social skills, push their limits, build self-confidence and experience what

3 Haddon, Leslie and Livingstone, Sonia (2012) EU Kids Online: national perspectives.EU Kids Online, The London School of Economics and Political Science, London, UK. Version available at: http://eprints.lse.ac.uk/46878/

4 Foundation my child Online, Hey, what's app?, March 2012

suits them and what not. Young people discover their own identity this way. Quick interaction is pivotal and young people want to decide how and when they do something; using What's app, making calls, chat or write online messages via Facebook and Twitter. Sometimes they do it using the home computer, at other times, such as on the train, by using their mobile phone. They leave environments very quickly that do not comply with their needs. They don't want to wait long for replies or responses.

Being creative with language

As a way of communicating, young people have created their own new forms of language. MSN language (or chat language) and sms language are the best known. Chatting speed is essential here. The use of emoticons (☺) and the use of numerals instead of letters (w8 instead of wait) have their origin here. Abbreviations such as BFF ("Best Friends Forever"), and YOLO ("You Only Live Once") are widely used.

Go online or being online?

Many adults who access the internet see the internet as a virtual world where they can find information and where they can do business. They '*go online* ' to attend to their banking affairs, to find a holiday or to order something. On the other hand, young people '*are* online '... They are simply doing the things they do and use the technologies available to them. For them there is no difference. Online = offline...!

Ten years ago the internet was mainly a gigantic library. Nowadays, it can be compared with a meeting center that is open all day and night and offers many possibilities for service and entertainment. The fact that the internet is the underlying infrastructure that makes all of this possible is irrelevant, especially for young people. For them it›s simple: you can get in touch with friends and be a part of a larger community. It is an essential part for growing up, which includes the development of social skills and finding your own identity. That happens nowadays for a large part online. Contact with classmates is not limited to the schoolyard or school hours. Via social media and what's app they are connected 24/7, to the great frustration of teachers and other adults. They worry about this 'face-down generation' who only seem to have an eye for smartphones or tablets and are distracted from homework and 'real' contacts.

Nevertheless, this generation is not actually any different to their parents. They have the same need for connection and they adapt to belong to a group. The significant difference, however, is that schoolyard dynamics does not stop anymore. Not participating is not a real option. If you don't participate, you are no longer a member of the group. Do you want to stand alone in the schoolyard?

When it comes to finding their own identity, young people today have exactly the same questions as their parents had: 'who am I?', 'who do I want to be?', 'what suits me?' and 'what doesn't?'. And they also find the answer, like their parents, through contact with others. But, of course, the internet offers many more possibilities for this and thus plays an important role. You can present yourself on profile sites with photos and videos that you upload. In chat sessions, whether or not you use a webcam, you can practice your social skills. The way the interaction proceeds is crucial for the image that teenagers have of themselves. Who am I, what do others think of me, am I 'good' or 'cool', what are my hopes and expectations and what do I want from life. Sometimes the internet is the place to be in touch with people who share your passion, or your orientation. Flirting and experimenting with sexuality has expanded to include not just the schoolyard, the hangout, the pub and nightclub, but also the internet.

In chat sessions, whether or not you use a webcam, you can practice your social skills. The way the interaction proceeds is crucial for the image that teenagers have of themselves.

Generation Einstein?

Give a toddler a smartphone or tablet and he will soon find out how to create larger or smaller images. He learns this by doing, seeing and he remembers. Children are not afraid to discover something new and learn that way how new technology works very quickly (aided by the fact that new technology is increasingly more intuitive).

Because of this adults may believe that they cannot teach anything to young people anymore. That is not true. The fact that children can adapt quickly to new technology does not mean that they understand everything, appreciate the consequences or know how to deal with them. This is certainly not the case if they are confronted with age-inappropriate information or footage. Young people between 12 and 18 prove[5] less able than is often thought. They make a lot of mistakes because they are impatient and bad readers. They are also naive and not very critical. Research by Dialogic[6] shows that 80% of high school youngsters don't check the reliability of the sources they use. It also showed that "finding privacy as important" is not the same as "knowing what to do to protect ones privacy" or "to act correspondingly".

Young people between 12 and 18 prove less able than is often thought. They make a lot of mistakes because they are impatient and bad readers. They are also naive and not very critical.

Young people know in theory what is wise and/or safe. But searching and pushing the boundaries is exciting and is inevitably linked to growing up. During the moment, doing something comes before thinking. They simply don't see the consequences of their behavior; YOLO ...!

1.2.2. Where are they?

A frequently asked and investigated question is what is popular among young people on the internet; What do they like? Which sites do they visit the most? What internet application is their favorite? YouTube, the website where users can post videos and that everyone can use to watch movies is by far the most popular in all age categories. Young children watch fun movies on 'Joeptjoep' together with their parents

Finding answers to such question as 'where are they ' and 'how long for', however, is of little value for understanding digital youth culture. It is far more important to know how websites and applications facilitate and support the development of young people.

For young people social network sites are important for a number of reasons:

- **Being in contact.** The need to share, join a group and oppose adults is part of growing up. Online you can do this continuously. The fear of adults that social networking sites replace 'real' friendships and that young people become more antisocial is unjustified. They just amplify it ...
- **Comparing yourself to others.** For young people it is important to compare themselves with others. What do others look like? What do they wear? What music do they like? What do they do? Social networking sites are an excellent way to 'peep' unabashedly at what others do. It helps young people to determine their own identity.
- **Presenting yourself.** If you look at other people's sites and profiles you know that others also come to visit yours. Young people therefore give endless attention to their online profile. They choose the best picture, the funniest texts, the right movie and the hippest music. At Hyves young people can also indicate what brands they want to be associated with. The success of sites such as Facebook and Hyves depends entirely on the fact that young people are constantly concerned with the question how they are seen by others. The fact that they themselves have control over how they present themselves gives young people

5 my child Online, Research Foundation "Einstein does not exist", October 2010

6 Dialogic, research "behind the scenes: Media use and behavior vmbo-youth", November 2012

a feeling of being better and stronger. Even when you're not the most popular person in the classroom, a strong profile on a social networking site gives you the chance to distinguish yourself in a positive way.
- **Receiving feedback.** The internet is all about action and reaction. Young people watch each other closely and are on standby to give a (usually positive) reaction to pass on messages and photos. The attention and compliments contribute to the group's feeling and to self-confidence.
- **Making contact.** Social network sites are easily accessible; it is very easy to make contact with 'vague acquaintances', including people from their wider circle of friends and acquaintances. Here you can leave a message (a Scribble) whenever and for whoever you want.

Computer games are as old as the first computer. The game Pacman had it all. It was fun, exciting and very addictive. Most games stimulate creative ability through playing. Young people learn to negotiate, practice solution-oriented thinking and their social skills. Even for the little ones there are games that suit their age.

Internet games have evolved into what they are today: beautiful, realistic and often complex games with an infinite number of variations and possibilities. You can play alone or online with others around the world. By any means whatsoever: computer, smartphone, iPod, tablet, handheld game consoles (such as Nintendo DS) and game consoles for television (Xbox, Wii, Kinect). Online games are very attractive. You play with others, get instant rewards for assignments that you perform and receive appreciation from the other players.

1.2.3. Online risks

The internet clearly offers young people a world with a lot of possibilities and opportunities, but also risks they are not, or insufficiently, aware of. The internet is anonymous and takes away inhibitions. This means that 'ordinary' norms and values are shifting on the internet. Boundaries are not always very clear and youngsters are already pushing the limits by looking for their own boundaries and by having quite a different perception of the use of the internet.

Research shows that young people from 12 to 18 make massive use of the possibilities the internet offers for romance and erotic encounters. Most adults have no idea that almost all young people who are active on the internet have been sexually approached by someone, or that one in four boys and one in five girls have had some kind of online 'sex' experience.

The internet clearly offers young people a world with a lot of possibilities and opportunities, but also risks they are not, or insufficiently, aware of.

Sometimes 'internet friends' have other intentions and can be very annoying. Young people see that risk much less and sometimes not at all. They just give out personal information, make appointments or expose themselves literally in front of the webcam, with all sorts of consequences. Usually they resolve it themselves, whether or not with the help of friends, parents or the school. But it also requires action from the police when criminal conduct is involved.

Sexting

Sexting is sending sexually suggestive messages or spicy photos or videos, usually via a mobile phone. "Sexting" consists of the English words "sex" and "texting". Both adults and young people find this exciting to do with their friend or girlfriend. It is increasingly becoming part of a sexual relationship. For young people it is logical to experiment with media such as mobile phone or webcam as part of their sexual development.

Sexting, however, is not without risk. The consequences can be far-reaching if the images are put online by an angry ex to take revenge. Sexting however is not always voluntary. Victims can be manipulated, blackmailed or threatened to send a nude photo. Once they have done it,

the offender threatens to put the photo on the internet or to distribute it in some other way. Victims are then forced to engage in further sexual acts, for example, through the webcam or even in real life.

According to current Dutch legislation sexting is punishable for youngsters under 18. It's punishable by law to create, possess or disseminate child pornography. The law itself doesn't take sexual experimenting by teenagers into consideration, but fortunately the administration of Justice does.

Webcam sex (abuse)

Most young people think it's fun to flirt and experiment with sexual behavior on the internet. They generally can also deal well with unpleasant experiences. But there are also victims and losers. Especially girls find it sometimes difficult to refuse things, forcing them go further than they actually would like to. In some cases, webcam sex images are published online; out of revenge after a broken relationship or in the form of cyber harassment. The same as mentioned for sexting applies here. The damage that this can cause is great; it is even possible for the images to continue to haunt the victim all her life, often without the offender even realizing this when performing such an impulsive act.

Under threat of disclosure of recorded images young people are pressured to go much further in front of the webcam or even to meet for physical sex.

The risk of abuse is very real and the impact, when this is the case, immense. Under threat of disclosure of recorded images young people are pressured to go much further in front of the webcam or even to meet for physical sex. This is also a way lover boys operate and leverage young people's loyalty.

Fake scouts

There are fake scouts that pretend to be scouts for a modeling agency or photo studio who shower young people with compliments and promises and take advantage of people's lack of self-esteem and their need for positive confirmation. They continue until these children sign up and pay the so-called photo studios and modeling agencies. In addition to the financial abuse (scam), sexual abuse is also just around the corner.

Unwanted publication

Photos or videos of yourself that you prefer not to share with the whole world can appear online; drunk, naked, crazy faces, in your bikini at the new year's party. It happens regularly that images without the consent of the 'protagonist' are put on the internet by someone else. This can be done as a reminder of a nice evening or just for fun because he or she does not understand why the other person would have a problem with it. Sometimes it happens with the express purpose of bullying, as revenge or with the conscious intention to annoy the other person. Given the enormous growth of social media, the threshold to publish is low and the impact is often great.

Insult, Slander/Libel

The internet offers many ways to hurt someone's good name and honor. For example, by creating a video of edited (profile) photos and making it clear through text or lyrics that the protagonist is a whore. Or by spreading a so-called 'Banga-list'. This is a list of girls by name, supplemented by personal data, (profile) photos and an explanation why they are among the top X 'largest sluts' of the school, city or province. Young people are very creative with finding new ways to do this and may go far. Other examples are:

- creating a hate profile with edited photos
- emailing edited photos
- putting offensive lyrics on forums under the name of another person
- putting some person's name or photo next to offensive lyrics

Virtual theft

A common form of theft takes place in (paid) online games: the looting of rooms in the virtual game Habbo, where players have paid for the decoration of rooms and therefore this represents value. Robbery on the internet is of course different from

robbery at home or in the street. By obtaining passwords or codes you can login to someone's account and 'become' that person's online identity. You then have free access to the game and his or her virtual property which you can book to other accounts. User data can be obtained in different ways. They are:

- told in confidence (best friends have no secrets)
- collected through so-called. 'phishing'
- simply guessed by obvious name and password
- obtained by threat

Cyber bullying

The tendency to find one's own limits can hurt other youngsters. Teens have a different view on bullying than adults. In the eyes of many young people bullying has a high fun factor and you are a tough guy when you go to the edge, and beyond. Bullying on the internet is anonymous and easy. A bad message is sent within a heart beat. What they don't realize, or what just doesn't interest them, is that what happens on the internet will not simply disappear again and can even become criminal.

Online bullying has a much bigger impact than classic bullying because as a victim you are not safe anywhere anymore. The bullying continues even if you're at home. It is invisible to parents and teachers and can continue for a very long time because victims do not dare to tell for fear that the bullying will get worse. When online bullying is recognized, in general it's dealt with by parents and the school. Not only do youngsters cross limits easily, they often are victims of cyber bullying themselves. Research shows that often there is a relationship between offline and online bullying. Cyber bullying is, like bullying, in itself is not punishable, but it can certainly contain criminal elements.

Minimizing risks starts with your own behavior

Many of these risks can be minimized by making young people aware that they themselves have a responsibility and by teaching them how they can protect themselves. Herein lies an important role for parents, educators and teachers. But also operators of online environments can minimize the risks and take measures to provide a secure environment to young people. In the Netherlands a lot has already been done in this area.

European research[7] into the use of media by young people places Dutch youngster (just like young people from Cyprus, Finland, Poland, Slovenia and England) in the category **'Higher use, some risk'**.
Despite the fact that they are intensive users of media, they are less likely to become the victim of online risks than young people in other European countries. As a possible reason for this increased resilience is mentioned:

- effective awareness campaigns
- active involvement of parents in their children's use of the internet

The bullying continues even if you're at home. It is invisible to parents and teachers and can continue for a very long time because victims do not dare to tell for fear that the bullying will get worse.

1.3. The online domain

Taking a helicopter view of all the facts and figures in the preceding paragraphs it becomes obvious that with the advent of the internet and all its applications a new social environment has been created where (young) citizens spend time, make contact, make money, can commit criminal offences and therefore can be victims. In this document we use the following description for the online domain:

"the total of all online environments and applications through which contact between people and the resources they use for it is possible".

7 Haddon, Leslie and Livingstone, Sonia (2012) EU Kids Online: national perspectives.EU Kids Online, The London School of Economics and Political Science, London, UK. Version available at: http://eprints.lse.ac.uk/46878/

Characteristics of the online domain

It is a challenge for every organization that is geographically organized to find an efficient and effective solution to existing processes.

1. Not tangible
The contacts and interactions take place in the "internet cloud". You can't look people in the face, put handcuffs on them and haul them off for example. The presence of the police in the virtual world requires us to consider in depth how you can display confidence and exercise authority.

2. Boundless
The internet has no borders. People contact each other all over the world. Offenders and victims of internet abuse may live kilometers apart. Moreover, it is not inconceivable for the many victims of one offender to all reside in different geographical areas. It is a challenge for every organization that is geographically organized to find an efficient and effective solution to existing processes.

3. No public space
Everyone surfs freely and without restrictions on the internet. Contrary to what you might think (certainly about the term "world wide web"), you cannot compare it with a public space. The internet is a network of computer networks on which all kinds of services are offered. Every website or online environment is therefore the property of a company or private person. The internet is a concentration of private spaces where the owner sets the rules (terms and conditions!). This is a very important factor in determining the size and content of the task of the police in the virtual world.

4. Information all over
The present situation, in which you can 'listen' as an outsider to conversations between people, look at their photo album and have access to personal information, is unique. There is a lot of publicly accessible information around through the use of social media : what keeps people busy, where they go, who their friends are, who their family is, what hobbies they have, and what they have experienced and seen.

5. Privacy
The issue of privacy in the online domain is associated with additional complexity. Most citizens seem not overly worried about the issue of privacy because they think 'I have nothing to hide '. They publish information about themselves on a public profile without realizing the range or possible consequences. Only when they are confronted with ? do they become obsessive about their privacy. Equally the question 'what do third parties do with information once published' doesn't matter to many citizens. For the police this presents opportunities; public profiles are still seen as public sources, provided that information is not systematically collected.

6. Nothing is what it seems
The internet is anonymous. People hide behind (a homemade) profile and use nicknames and Hotmail addresses. Data can be manipulated on the internet, so you should always be critical and ask yourself: "What is true?", "Can I trust this person?" This is not always easy; a rumor on the internet quickly turns into the "truth". After all, if so many people talk about it, there must be a kernel of truth in it!? And when there are even pictures to support it, then all doubt quickly disappears and only a few people are left who wonder whether the image may perhaps have been manipulated.

7. Dynamic
How quickly communication travels these days and what impact communication can have is illustrated by the various experiences from the 2012 projects X. There are, however, also numerous examples that illustrate how quick 'smaller' items of communication travel nowadays. The first photos of an accident, for example, are sent by twitter within a few minutes (sometimes even before a police control room was informed about the accident), and regularly a tweet proves to be the actual source for reporting in the national media. Today everyone is a producer of news and dissemination is faster and better targeted than in any other medium.

The above examples focus on the differences between the online environment and the 'physical' environment that we know. However, there are also a number of similarities between the two environments that are important to bear in mind for further reflection on the role of the police in this domain:

1. It involves real people, really money and genuinely criminal behavior
2. Legislation in respect of minors (special position, both criminal and civil)
3. Expectations of citizens towards the police to be "watchful and helpful"
4. Preventing, identifying and advising are important factors for preventing an escalation
5. Certain situations require (emergency) assistance
6. Cooperation between organizations is essential

The online domain generates challenging issues when it comes to translating them into the core processes of the police and the implementation of the tasks of the police and more specifically the police youth task.

1.4. Online victims and offenders

With the advent of the internet, new forms of crime have emerged. Crime that does not exist without the necessary IT facilities (computer and/or network). We speak of 'cybercrime in the strict sense'. Examples are:

- Hacking (accessing data on computers without permission)
- Defacing (changing, replacing, or destroying data from a website without permission)
- Spreading malware (malicious software that damages computers and network connections and/or gives access to the computer or data to another person without the consent of the user).

In addition, there is also "cybercrime in the broad sense". This concerns criminal behavior in which IT plays a role, but is not a necessary condition for the crime itself. It applies to all offences in the criminal code, but in a new form. Some examples:

Theft: *"all my furniture in Habbo is gone!"*
Threat: *"@anyorganization I will kill you all tomorrow #deaththreats"*
Libel/slander: *"Help, I'm placed on a banga list" (girls names on list, called a whore)*
Various*: *"the whole school has seen my nude photo. First only on what's app, but now also on twitter"*

* in the case of the distribution of a nude photo there can be several relevant legislative measures. Child pornography (if the victim is a minor), grooming (if the offender is an adult), libel/slander, portrait rights, sexual abuse (if not entered into voluntarily). The context is essential for determining which offence we are dealing with.

The basis for the prevention of internet-related crime for a large part lies with the awareness of the users. The more users understand how the Internet works and what the consequences of their actions are, the more aware they will be with regard to their own behavior and that of their environment. The basis of media wisdom is:

- knowing what the opportunities and risks of the internet (applications) are
- understanding the impact of your own behavior and actions on the internet
- understanding what you can do yourself to minimize risks and prevent victimization
- being able to apply this knowledge for using media responsibly and consciously

The more users understand how the Internet works and what the consequences of their actions are, the more aware they will be with regard to their own behavior and that of their environment.

1.5. Stakeholders

Security is a collective responsibility in the virtual world!
Countering blurring of moral standards and lowering the number of criminal offences in the online domain is a task that the police cannot perform alone and should not have

to do alone. Creating a safe environment for young people on the internet is (should be) a shared responsibility of many parties. Below you find a list of parties which are relevant in addition to the police for increasing security in the virtual world.

An important responsibility, of course, remains with the young people themselves. When they are aware of the risks, their own behavior and its consequences, the risk of victimization is reduced.

Young people, parents and schools

An important responsibility, of course, remains with the young people themselves. When they are aware of the risks, their own behavior and its consequences, the risk of victimization is reduced. They will be self-reliant and recognize possible abuse earlier; this knowledge will also be actively used to protect yourself and others in your social network.

It is important that parents support their children in discovering the virtual world. Education determines to a large extent the standards and values of young people. This is no different when it comes to using media. It is for a large part about social skills. Depending on the age of their children parents will accompany their media use and learn how they can use this in a positive way. It also requires that they make children aware of the risks and teach them how to protect themselves: with rules and by reflecting on their own behavior. Schools also play an important role in teaching values and raising awareness to young people. They also have an important function when it comes to early signaling of unpleasant situations.

Owners/administrators (providers)

The responsibility for a safe environment lies to a large extent with the owner and/or operator of a site. He is primarily responsible for rules and the monitoring of compliance. Possible measures include:

- house rules and imposed conditions on the use of/visit to the online environment
- moderators overseeing compliance with house rules and taking measures in case of infringement
- providing the option for young people to contact the moderator to report misdemeanors
- prevention through technical restrictions (language filters)
- providing information on safety for young people and parents

Private parties

Several large and smaller initiatives focus on information and assistance, such as the (online) de Kindertelefoon, Meldpunt Kinderporno op Internet, Meldpunt Discriminatie, Slachtofferhulp, Bullyweb, Stoploverboys.nu, Pestweb etc.

Centers of expertise „Youth and Media“

In the area of security for young people in the virtual world various parties engage with the question "how is the digital youth culture developing" and what is needed to increase awareness and safety.

Internet Security Platform

The platform consists of several market stakeholders, the Ministries of Economic Affairs and Justice, and it aims at a structural contribution to improve internet safety for consumers/internet users. It focuses on strategic issues in relation to internet security and aims to set an agenda, identify trends and suggest concrete initiatives.

2. Impact on the police

The digitalization of society is a development that affects the entire police organization and all of its core processes. Not only because of the fact that citizens want to be able to make reports online, and expect the internet to be used efficiently and effectively in matters of detection. But above all, because the police has a responsibility when it comes to criminal behavior that is committed using the internet. The physical world is no longer the only environment in which people can commit criminal offences and therefore also be victims. Insight into the digital youth culture offers an integral perspective for wider issues and organizational challenges that the police faces:

- 'New' criminal offences
- Other forms of existing criminal offences
- New forms of knowledge about crime and legal system
- Using the internet as a new channel (communication, detection, service for citizens)
- No insight into new trends and developments
- Heavily reduced level of information without a focus on online domain
- Risk of incorrect assessment of powers through a lack of knowledge
- Inefficient business processes and chain cooperation
- Growing gap between online crime and likelihood of detection
- Less respect and trust from citizens

Young people indicated that if they need the police, they cannot find them in the online domain. To contact the police they generally have to go to a physical police station. The threshold for young people to get in touch with the police about what they experience online is great. This has several reasons:

- shame; they dare not talk about the immediate cause
- fear of not being taken seriously by the police;
- fear that the police will not understand them;
- perception that nothing happens with their report
- don't want their parents to be involved;
- lack of direct (online) contact options is discouraging

It has therefore been decided to take the challenge and (literally to an extent!) move into the virtual world. The Dutch police has launched various initiatives in recent years in order both to learn and to use this newfound knowledge for finding answers to the organisational challenges they face. Many meaningful steps have been taken. In the following paragraphs a brief overview on the role of the police on the internet will be discussed.

Young people indicated that if they need the police, they cannot find them in the online domain. To contact the police they generally have to go to a physical police station.

2.1 Police in the virtual world

Citizens' expectations for the police to act no differently online than in real life was an important starting point for developing and conducting the various initiatives as these expectations are legitimate. The police should be there when they are needed, help victims and arrest perpetrators. However, there are a number of constraints on the way responsibilities can be performed in the online domain. The police on the internet cannot:

- be responsible for the public order; they are private domains,
- directly apply its powers; quite often it requires special investigative techniques,
- exercise the same authority as on the street because of visibility, recognition and limitation in applying its powers,
- be the only one responsible for the safety of young people.

1. Police officer on Habbo

Within the virtual Habbo world the police has experimented with a digital community police officer, Boudewijn Mayeur. Young people can get in touch with him while playing online in Habbo. They ask a lot of

questions and also confide in him about serious personal problems such as domestic violence and sexual abuse. They also regularly show him new phenomena and inform him when they are being approached for webcam sex (cyber grooming).

The reason the Dutch police started this initiative in Habbo Netherlands in 2010 was because both the community manager and the Habbo users themselves said to need the presence of the police. It started with monthly consultations for young people in what was called 'the information-bus' at Habbo Hotel, where other organizations like Child phone, Bullyweb, Help-wanted and Stop loverboys also were regularly online for one hour chats with the kids.

It turned out that the request from youngsters was not only to talk about the problems that took place within Habbo itself, but also about situations that happened to them outside, in the real world. They were anxious to talk with a real police officer online in their own trusted environment. Habbo created a special police-avatar and to make clear that this is the only real police officer in Habbo, a special police badge was designed. And in autumn 2012 even a virtual police station was opened.

Habbo created a special police-avatar and to make clear that this is the only real police officer in Habbo, a special police badge was designed.

By being present in Habbo the police fulfills the objective to be available online to young people and thus also directly meets its responsibilities of prevention, enforcement, detection and signaling. Visibility and presence in particular are important conditions as those provide an easy contact opportunity between these young people and the police. It helps the police to better understand the experiences of young people regarding current (online) issues. On top of that they gather useful experience when chatting with young people and learn how young people value the possibility to have contact with the police online.

Last year the digital police officer worked for more than 150 hours in Habbo during 350 sessions. Over the course of 6 months there were nearly 11,000 unique Habbo users who visited the police station. Online young people are willing to provide the police with information, either upon prompting or voluntarily, about unwanted and/or harmful behavior that they have experienced. Almost every session provides us with indications for detection or further research. Because it is impossible for one officer to research all this information in the pilot phase decision was to only perform advisory and signaling work. Very serious matters were immediately passed on to colleagues in the country with the request to take over the investigation. The ambition is to extend police capacity.

2. Website Vraaghetdepolitie.nl (ask-the-police)

In addition to the existing general site of the Dutch police www.politie.nl there is a separate one for young people, which was launched in 2006. The site www.vraaghetdepolitie.nl was developed to answer questions and provide easily accessible information on topics young people themselves chose as relevant. The purpose of the website is to improve the image of the police among young people (12-16) and reach the target group that actively becomes involved in security issues in their own environment.

The presence of the website is an important step for the police in increasing their visibility and accessibility for young people in the virtual world as it enables online contact between police and young people. Young people can ask their

questions, look up information, get in contact with their local police officer, take part in regular chat sessions. In the process of developing the site research was done among young people about what they expect from the police and what topics are most relevant for them. They answered that they see the police especially as an authority and wanted to find reliable factual information about topics that concern them as well as tips on how to deal with problems in this area. They also wanted to find information about laws and rules and how to contact the police. Based on this research 14 topics were chosen, such as internet, cyber bullying and drugs.

Frequently asked questions (FAQ) and answers are available for everyone to see and anyone can join chat sessions if they want. The chats topics are either themes communicated in advance or issues related to current news. The site is a huge success and at the time of writing there are approximately 70,000 unique monthly visitors to the site. Incidentally, local police officers themselves also use this site to find the answers to the questions that they were asked by young people in their district on the street.

The website is actively affiliated with a number of governmental and private bodies to allow young people to directly ask for help when they find themselves in a difficult situation online. The website www.meldknop.nl (report!) was launched on Safer Internet Day, on 6 February 2012, by the Minister of Safety & Justice, Mr Ivo Opstelten.

3. Communicate via Twitter

Twitter is becoming increasingly popular and virtually all sworn police officers already have (or very soon will be in the possession of) a mobile phone that allows them to search police databases themselves, but also to use Twitter independently to send short messages about their work and to inform the public or ask them for assistance. More than 1000 Twitter accounts actively communicate about police and regional matters. Before the officers start twittering they attend a short training course about what does and doesn't fit in the communication policy and share experiences and lessons learned.

4. Information about online risks

To reduce online victimization information is needed. It is for this reason that an information and awareness-raising process was developed in the form of a short "game". This game about choosing what friends to accept is called www.kenjevrienden.nu and can be played and shared with friends throughout the internet and social media. It illustrates that on the internet everyone can pretend to be anyone. The message is that it is good to think twice about who you add to your online network(s).

The concept was developed together with young people and is based on true facts. We know from conversations with young people that there is a high threshold to go to the police when they have got into trouble online. Often they are ashamed and think they are not entitled to help. An additional reason is that they think that the police still don't understand what they play online and therefore their problem will not been taken seriously. With this 'game', we want to reduce the threshold for young people by showing that the police does understand what is going on online, how you can become a victim while you are online and that we understand that it is difficult to talk about it.

We know from conversations with young people that there is a high threshold to go to the police when they have got into trouble online.

5. Increase knowledge level

It is important that every policeman and woman understands how online and offline are interwoven and that there are situations that require police action. To this end, various initiatives were taken, such as the production of a brochure (online) in cooperation with a center of expertise in the field of 'children and the media' about digital youth culture and its impact on the police.

It is important that every policeman and woman understands how online and offline are interwoven and that there are situations that require police action.

Furthermore, various workshops were organized on the subject of youth culture and the internet and a toolbox is designed for every colleague who, in their daily work, encounters the subject "youth & the virtual world". With the introduction of the toolbox the digikids expert group also wanted:

- to promote exchange of specific knowledge,
- give insight into local and regional initiatives,
- make proven successes available,
- to encourage cooperation.

The toolbox is not static, but constantly under development and the content grows 'with' current developments.

3. Our ambition

The ambition is to carry out an active policy on the youth task (prevention, signaling & advise and repression) in the online domain. This means reduction of online victimization and increasing the chances of arresting online offenders. Activities are designed to contribute to being present online, to be approachable and to identify what's happening at an early stage and to be able to anticipate matters. The skills of employees will have to include understanding online risks and the underlying mechanisms so that this can be translated into desirable and/or required police actions. Active knowledge sharing and cooperation with external stakeholders in the area of online safety is one of the basic conditions.

Source Entry

Eurostat, 'Statistics in Focus', week 50/2012

CBS, Statline, ICT gebruik van huishoudens en personen, oktober 2012

Marketingfacts, 'What's happening online?', juni 2012

EU Kids Online: national perspectives. Haddon, Leslie and Livingstone, Sonia (2012)

Stichting Mijn Kind Online, Hey, what's app?, maart 2012

Stichting Mijn Kind Online, onderzoek "Einstein bestaat niet", oktober 2010

Dialogic, onderzoek "Achter de schermen: Mediagebruik en –gedrag vmbo-jongeren, november 2012

Oriënterende gesprekken met Habbo, Hyves en Meldpunt Kinderporno

Onderzoek Universiteit Twente "Grooming, Sexting en Virtuele diefstal; VMBO-Jongeren en praktijkexpert aan het woord", december 2012

Beleidsadvies Expertgroep Digikids "Het organiseren van de politiële jeugdtaak in de virtuele wereld", januari 2013

Authors

Solange Jacobsen is an independent project manager associated with the Foundation Mijn Kind Online (My Child Online) and works for the Dutch police as program manager of the expert group Digikids.

Manuel Mulder (MBA) is a Dutch police commissioner and chairman of the expert group Digikids whose responsibility it is to develop initiatives on the subject of “reducing online risks for children” and “increasing the chance of getting caught”.

Kinder- und Jugendschutz vor den Herausforderungen des Web 2.0

Ines Kawgan-Kagan, M.A.

Abstract
Die Aufgaben, vor denen der deutsche Jugendmedienschutz steht sind komplex und müssen sich stetig neuen Aspekten des Internets stellen. Die Gesetzeslage in Deutschland ist jedoch noch komplexer. Verschiedene Gesetze wurden den Veränderungen auf dem Markt lediglich angepasst. Leider ging dabei der Blick für das Ganze abhanden und zahlreiche Aspekte des Jugendmedienschutzes sind auf unterschiedliche Weise in verschiedenen Gesetzen geregelt. Zu nennen sind insbesondere das Jugendschutzgesetz (JuSchG), geltend für Computerspiele, der Jugendmedienschutz-Staatsvertrag (JMStV), der Rahmenbedingungen für telemediale Dienste und Inhalte schafft, sowie das Strafgesetzbuch (StGB). Ein Paradigmenwechsel muss her, der eine einheitliche und möglichst internationale Lösung der regulierten Selbstregulierung für Computerspiele und andere telemediale Inhalte und Dienste sowie eine Erweiterung der Kriterien für die Alterseinstufung dieser Inhalte und Dienste beinhaltet. Essentiell ist darüber hinaus die Sensibilisierung und Schulung von Kindern und Jugendlichen, Eltern und Lehrern.

Das Internet ist zweifelsohne eine der kontrovers diskutiertesten Erneuerungen der Neuzeit, die jedoch nicht mehr wegzudenken ist.

1. Introduction

„Denn diese Erfindung wird der Lernenden Seelen vielmehr Vergessenheit einflößen aus Vernachlässigung des Gedächtnisses, weil sie im Vertrauen darauf sich nur von außen vermittels fremder Zeichen, nicht aber innerlich sich selbst und unmittelbar erinnern werden.“
(Platon, Phaidros)

„Bei Kindern und Jugendlichen wird durch Bildschirmmedien die Lernfähigkeit drastisch vermindert. Die Folgen sind Lese- und Aufmerksamkeitsstörungen, Ängste und Abstumpfung, Schlafstörungen und Depressionen, Übergewicht, Gewaltbereitschaft und sozialer Abstieg.“
(Spitzer, 2012)

Zwischen diesen Zitaten liegen 2.400 Jahre. Vor den Folgen digitaler Demenz warnt aktuell ein Hirnforscher ebenso wie Platon vor geraumer Zeit, der ebenfalls Demenz befürchtete, ausgelöst durch Einführung der Schrift – welche zweifelsohne eine Erfolgsgeschichte wurde. Es ist interessant, dass viele Menschen offenkundig Schwierigkeiten haben, das Unbekannte und Fremde bei Innovationen weniger mit den Chancen, als vielmehr mit den Risiken und Gefahren in Verbindung zu bringen. So warnten selbst Ärzte bei der Einführung der ersten Eisenbahnen zu Beginn des 19. Jahrhunderts vor den unkalkulierbaren Auswirkungen der hohen Geschwindigkeiten für das Gehirn (Joerges, 1996).

Das Internet ist zweifelsohne eine der kontrovers diskutiertesten Erneuerungen der Neuzeit, die jedoch nicht mehr wegzudenken ist. Viele Eltern sehen ein Verbot als einzige Möglichkeit, ihre Kinder zu schützen. Nur ist dies weder möglich noch ist es sinnvoll den Fortschritt aufzuhalten und Kinder und Jugendliche von der digitalen Welt komplett abzuschirmen.

2. Hintergrund

Kindern und Jugendlichen den Umgang mit dem Internet und neuen Medien gänzlich zu verbieten, ist schlichtweg nicht machbar,

da Eltern ihre Kinder ab einem gewissen Alter nicht auf Schritt und Tritt begleiten können und Freiräume wichtig für die Entwicklung sind. Auch sind der elterlichen Verfügungsgewalt in Zeiten mobiler Endgeräte klare Grenzen gesetzt. Eigene Erfahrungen sind wichtig für eine gesunde Entwicklung. Dabei sollten Heranwachsende jedoch nicht allein gelassen werden, vielmehr sollten ihnen wichtige Verhaltensregeln mit auf den Weg gegeben werden. Leider ist vielen Eltern nicht bewusst, wie intensiv Kinder und Jugendliche bereits im Netz agieren. Ein Blick auf die Zahlen lässt erahnen, dass ein immer jünger werdendes Publikum immer häufiger diese Medien nutzt. So haben nach der aktuellen KIM-Studie 57% der Kinder zwischen 6 und 13 Jahren in Deutschland zumindest selten Erfahrungen mit dem Internet (KIM-Studie, 2011). Für zwei Drittel der Kinder steht überwiegend die Kontaktpflege mit Freunden im Vordergrund. (Schröder, 2012). Aber auch Online-Spiele stellen einen beliebten Zeitvertreib im Internet dar. Diese Form der Nutzung des Internets findet überwiegend unüberwacht statt: Laut einer europaweiten Studie nutzen gerade einmal ein Drittel der Eltern einen Filter, noch weniger (27%) haben eine Monitoring Software installiert. Dieselbe Studie offenbart, dass aber knapp 80% der Eltern sich Sorgen um ihre Kinder machen, wenn sie das Internet nutzen. In Deutschland ist die Zahl der Nutzer von Jugendschutzprogrammen laut einer anderen Umfrage noch geringer mit gerade einmal 20% (Hasebrink, 2011), obwohl 95% eine solche Software als wichtig empfinden. Diese Diskrepanzen können auch mit einem gewissen Gefühl von Machtlosigkeit der Eltern erklärt werden. Viele wissen einfach nicht, wie sie ihre Kinder effektiv schützen können und welche Programme ausreichenden Schutz bieten.

Diese Form der Nutzung des Internets findet überwiegend unüberwacht statt: Laut einer europaweiten Studie nutzen gerade einmal ein Drittel der Eltern einen Filter, noch weniger (27%) haben eine Monitoring Software installiert.

Eines der bekanntesten Probleme ist der Umgang mit privaten Daten und den Privatsphäreeinstellungen in sozialen Netzwerken, wie Facebook oder Myspace. Nur 43% der 9- bis 16-Jährigen in ganz Europa nutzen den Schutz, ihr Profil nicht öffentlich zu setzen; mehr als ein Viertel haben keinerlei Schutz und ein öffentlich zugängliches Profil erstellt (Haddon et al.,2011). Welche Probleme ergeben sich aus dem verstärkten Nutzungsverhalten?

Häufig genannte Probleme sind Online-Sucht und Cybermobbing bzw. Bullying. Fast einer von fünf 12- bis 17-Jährigen aus gesamt Europa, zusammen mehr als 4,5 Millionen Kinder und Jugendliche, geben an bereits Opfer von Cybermobbing geworden zu sein (National survey of American attitudes on substance abuse XVI: teens and parents). Dabei ist die tägliche Nutzungsdauer ausschlaggebend: Je länger soziale Netzwerke genutzt werden, umso höher ist die Wahrscheinlichkeit Opfer von Cybermobbing zu werden. Während gerade einmal 3% der Kinder und Jugendlichen, die an den meisten Tagen nicht in sozialen Netzen unterwegs sind, betroffen sind, steigt die Wahrscheinlichkeit auf 33% für diejenigen, die mehr als eine Stunde online sind.

Ein weiteres Problem stellt die Online-Sucht dar, wobei ein Zusammenhang zwischen dieser Suchtform und dem Missbrauch anderer Substanzen wie Tabak, Alkohol oder Drogen zu nennen ist (Dyckmans, 2012). In der Gruppe der 14- bis 16-Jährigen lässt sich bei 17% der Mädchen ein allgemein problematischer Internetgebrauch feststellen, im Vergleich dazu bei den Jungen 14%. Insgesamt sind 100.000 abhängige und 400.000 problematische Nutzer zu nennen. Gerade für weibliche Personen sind soziale Netzwerke sehr wichtig, für Jungen stehen weiterhin Spiele im Vordergrund (Schröder, 2012).

Neben anderen Problemen, wie zu einfache Bezahlsysteme (z.B. über die Telefonrechnung der Eltern) ist das Phänomen Cybergrooming weitestgehend unbekannt. Cybergrooming ist die Planungs- und Anbahnungsphase, die einem sexuellen Übergriff durch eine Person auf eine/n

Minderjährige/n vorausgeht und diesen einleitet (Rüdiger, 2012). Die Anonymität und mangelnde Privatsphäreeinstellungen bieten Pädokriminellen leichten Zugang zu potenziellen Opfern. Dieses Problem ist eins zu eins auf Online-Spiele und deren Sicherheitseinstellungen anzuwenden. Zumal in sozialen Netzwerken immer häufiger Online-Spiele genutzt werden. Wo viele Kinder sind und keine Kontrolle über die Kommunikation stattfindet, sind auch Täter zu finden. Laut der aktuellen KIM-Studie wurde bereits jedes vierte Kind schon einmal im Internet sexuell belästigt. Eine US-Studie weist aus, dass 48% der Opfer von internetbasierten Sexualstraftaten zwischen 13 und 14 Jahre alt waren. Der reale Missbrauch hat zunehmend seinen Ursprung in der virtuellen Welt: 10% der Vergewaltigungen wurden über das Internet angebahnt (Finkelhor, 2008).

Betroffen sind häufiger Mädchen als Jungen. Nur 8% können darüber mit ihren Eltern oder Freunden sprechen (Katzer, 2007). Oft sind die Kinder ratlos, was sie tun können. Viele Eltern wissen nichts von diesem Problem und in der Öffentlichkeit wird meist nur der reine Datenschutz bei sozialen Netzwerken als problematisch wahrgenommen. Oftmals findet sogar eine Bagatellisierung von Cybergrooming statt, obwohl das Einwirken auf Kinder durch Schriften oder pornographische Bilder nach § 176 (4) Nr. 3 und 4 StGB sogar strafbar ist.

Es ist in erster Hinsicht ein Generationenproblem, denn die meisten Eltern sind selbst noch mit Brief, Postkarte, Faxgerät und gerade mal den Anfängen wie dem VC 64 groß geworden. Der Zugang zum Netz bietet ungeahnte Möglichkeiten der weltweiten Kommunikation, die es im Zeitalter von Brief und Postkarte so nicht gegeben hat. So können Menschen ohne größeren Aufwand in Kontakt kommen und/oder bleiben. Auch die Recherche und Informationsbeschaffung wird um ein Vielfaches erleichtert. Eine Aktualität wie das Internet sie bietet, wäre sonst kaum möglich. Obwohl sich auch dieser Beitrag mit den Risiken und Gefahren des Internets für Kinder und Jugendliche befasst, lohnt es sich dabei die Chancen des Internet nicht aus den Augen zu verlieren.

Um diese Vorteile jedoch sicher nutzen zu können, bedarf es der Wahrnehmung von mehr Verantwortung durch Politik und Betreiber. Diese haben für effektive Schutzmechanismen sowie die Etablierung einer flächendeckenden, systematischen und zielgerichteten Medienkompetenzvermittlung für Kinder und Jugendliche, aber auch deren Eltern und Lehrpersonal Sorge zu tragen, um die generationsbedingte Lücke zu schließen.

3. Kompetenzen im Online Jugendschutz in Deutschland: Wer? Was? Wann?

Eines der Grundprobleme beim Jugendschutz im Internet in Deutschland besteht darin, dass in der Vergangenheit versucht wurde, gängige Jugendschutzmechanismen der realen auf die digitale Welt zu übertragen – ein Ansatz, der zum Scheitern verurteilt ist. Eine gedruckte Zeitschrift kann konfisziert, eingestampft und der Vertrieb verboten werden. Bei Online-Medien ist dies durch grenzenlose Verbreitungsmöglichkeiten und dem einhergehenden kollektiven Gedächtnis nicht möglich. Das Internet vergisst nicht. In diesem Zusammenhang ist die Debatte über das Sperren von kinderpornographischen Seiten, also von Missbrauchsdarstellungen, zu nennen. Kinderschutzorganisationen ebenso wie Politiker haben anfangs geglaubt, mittels einer technischen Sperre ließe sich dieses Problem bekämpfen. Dass dies weder technisch machbar – Blockaden können schnell umgangen werden – , noch dem Grundverständnis des Internets entsprechend sinnvoll ist – so sind Verlagerungen auf andere Seiten oder gar gänzlich auf private Netzwerke zu befürchten – , wurde

Es ist in erster Hinsicht ein Generationenproblem, denn die meisten Eltern sind selbst noch mit Brief, Postkarte, Faxgerät und gerade mal den Anfängen wie dem VC 64 groß geworden.

erst nach einer intensiven und teilweise sehr emotional geführten Debatte deutlich.

Da einerseits eine Kontrolle des Internets durch staatliche Überwachung nicht möglich und von keiner Seite gewollt ist, andererseits eine Selbstregulierung der Märkte nicht zu gewünschten Erfolgen kommt, wird in Deutschland auf das Prinzip der regulierten Selbstregulation gesetzt. Dieses Steuerungskonzept ist definiert als Selbstregulierung, die in einem rechtlichen Rahmen erfolgt, den der Staat zur Erreichung der Regulierungsziele gesetzt hat (Schulz, Held, 2002).

Diese meist kostenlosen Spiele im Internet (abgesehen von käuflich erwerblichen, sehr kostspieligen virtuellen Güter) sind in der Realität frei für jedermann zugänglich und müssen sich keinem Prüfverfahren unterziehen.

Was kann also getan werden, um dennoch einen effektiven Jugendschutz zu etablieren? Um dieser Frage nachgehen zu können, sollen an dieser Stelle die rechtlichen Rahmenbedingungen erörtert werden. Welches Gesetz ist als einschlägig für den Kinder- und Jugendschutz im Internet zu nennen? Die rechtlichen Rahmenbedingungen und Ansprechpartner sind nicht einheitlich geregelt, da es nicht nur ein Gesetz und einen Ansprechpartner in Deutschland gibt.

Um einen Einstieg in den Jugendmedienschutz in Deutschland zu finden, sollen an dieser Stelle drei einschlägige Gesetzesgrundlagen genannt und erörtert werden. Zu nennen sind insbesondere das Jugendschutzgesetz (JuSchG), der Jugendmedienschutz-Staatsvertrag (JMStV) und auch das Strafgesetzbuch (StGB). Neben verantwortlichen Institutionen und Prozessen wird auch auf bestehende Defizite eingegangen.

3.1 Jugendschutzgesetz

Auf Bundesebene schützt das deutsche Jugendschutzgesetz seit 1952 Kinder und Jugendliche in der Öffentlichkeit und im Bereich der Medien. Seit 2003 regelt dieses Gesetz auch verbindlich die Altersbeschränkung von Computer- und Videospielen. Wie bereits davor bei Filmen werden Spiele einer Kontrolle unterzogen und auf deren Inhalte hin geprüft und dementsprechend nur für bestimmte Altersgruppen freigegeben. 1994 wurde die Unterhaltungssoftware Selbstkontrolle (USK) als verantwortliche Stelle für die Alterskennzeichnung von Videospielen durch das Jugendschutzgesetz eingesetzt. Aus § 14 JuSchG ergeben sich die Obersten Landesjugendbehörden als zuständig für die Alterskennzeichung. Diese haben zusammen mit den Sachverständigen der Länder bei der USK die letztendliche Entscheidungsgewalt über die Altersfreigabe, da diese als Verwaltungsakt erlassen wird. Diese Freigabe ist für den Handel maßgeblich: Spiele müssen deutlich gekennzeichnet und dürfen nur an die freigegebene Altersgruppe verkauft werden. Leider ist hinzuzufügen, dass das JuSchG nicht alle Arten von Spielen erfasst, sondern lediglich solche, die mittels eines Trägermediums verkauft werden. Darunter fallen nicht die rein serverbasierten Online-Spiele, da diese nicht im Laden zu kaufen sind. Diese meist kostenlosen Spiele im Internet (abgesehen von käuflich erwerblichen, sehr kostspieligen virtuellen Güter) sind in der Realität frei für jedermann zugänglich und müssen sich keinem Prüfverfahren unterziehen. Dieser wichtige Teil der Online-Welt wird also gesetzlich durch das JuSchG nicht geregelt.

Aus den §§ 17 bis 25 JuSchG ergibt sich ein weiterer Akteur für die Überprüfung der Einhaltung der Bestimmungen aus dem JuSchG: die Bundesprüfstelle für jugendgefährdende Medien. Diese dem Bundesministerium für Familie, Senioren, Frauen und Jugend nachgeordnete selbstständige Oberste Bundesbehörde kann Schriften, Ton- und Bildträger sowie Webseiten in die Liste der jugendgefährdenden Schriften aufnehmen (indizieren) und somit den Vertrieb maßgeblich einschränken. Indizierte Spiele dürfen nicht in den freien Verkauf gebracht werden (§ 15 JuSchG). Das damit einhergehende Verkaufsverbot stellt eine enorme Beeinträchtigung dar

und wird von vielen Spieleanbietern umgangen, indem speziell für den deutschen Markt geschnittene und gekürzte Versionen erstellt werden. Für Computerspiele gilt in Deutschland, soweit sie als Trägermedium verkauft werden, dass sie der Prüfung durch die USK unterzogen werden müssen, um nicht von vornherein als jugendgefährdend eingestuft und indiziert zu werden (§ 12 (5) JuSchG).

Der Grundgedanke der Alterskennzeichnung ist, ein einheitliches und verbindliches Erkennungssignal für Eltern und Konsumenten zu schaffen, um Sicherheit bei dem Erwerb von Spielen zu bieten.

3.2 Jugendmedienschutz-Staatsvertrag

Die USK bietet mittlerweile zwar Prüfverfahren zur Alterskennzeichnung sowohl von Computer- und Videospielen auf Datenträgern als auch von Computer- und Videospielen im Internet und sonstigen telemedialen Inhalten an. Das Prüfungsverfahren für telemediale Inhalte und Dienste erfolgt jedoch ohne staatliche Beteiligung – ist also nicht verbindlich vorgeschrieben und bringt keinerlei Konsequenzen bei Nichteinhaltung mit sich. Grundsätzlich fallen diese Inhalte in den Geltungsbereich des von den Bundesländern gemeinsam vereinbarten Jugendmedienschutz-Staatsvertrages (JMStV). Seit 2003 deckt der JMStV neben Radio und Fernsehen auch die Dienste und Inhalte sowie Online-Spiele, die im Internet angeboten werden, ab. Die Lücke, die sich aus dem JuSchG ergibt, wird hier aber – wie sich folgend zeigen wird – nicht ganz deckungsgleich geschlossen. Gemäß §§ 14 ff. JMStV überprüft die Kommission für Jugendmedienschutz (KJM) die Einhaltung der Vorgaben des Jugendmedien-Staatsvertrages. Die KJM wird dabei von verschiedenen Unternehmen (z.B. Jugendschutz.net gemäß § 18 JMStV) und anderen durch die KJM anerkannte Einrichtungen der Freiwilligen Selbstkontrolle gemäß § 19 JMStV unterstützt (FSK, FSF, FSM, USK). Letztere können, eingesetzt als Jugendschutzbeauftragte, die Pflicht erfüllen, die sich aus § 7 JMStV für „geschäftsmäßige Anbieter von allgemein zugänglichen Online-Angeboten, die jugendschutzrelevante Inhalte enthalten“ (§ 7 (1) JMStV) ergibt.

In Bezug auf telemediale Inhalte (ausgenommen politisches Zeitgeschehen, soweit ein berechtigtes Interesse gerade an dieser Form der Darstellung oder Berichterstattung vorliegt (§ 5 (6) JMStV)) werden mehrere Möglichkeiten genannt, um ausreichend Sorge zu tragen, dass Kinder und Jugendliche nicht mit für sie ungeeigneten Inhalten in Kontakt kommen (§ 5 (3), (4), (5) i.V. mit § 11(1) JMStV):

- Einschränkung der Zugangszeiten
- Nutzung von technischen oder sonstigen Mitteln zur Zugangsbeschränkung
- Programmierung für eines von der JVM akzeptierten Jugendschutzprogrammes

§ 5 (4) JMStV bietet die Möglichkeit Inhalte ohne Jugendfreigabe ausschließlich zwischen 23 und 6 Uhr zugänglich zu machen; Inhalte ab 16 Jahre nur zwischen 22 und 6 Uhr. Eine weitere Zugangsbeschränkung kann durch die Nutzung eines als von der KJM positiv bewerteten Altersverifikationssystems erreicht werden. Der Zugangsschutz ist durch zwei Schritte sicherzustellen: „erstens durch eine zumindest einmalige zuverlässige Volljährigkeitsprüfung (Identifizierung), die über persönlichen Kontakt erfolgen muss; zweitens durch eine sichere Authentifizierung bei jedem Nutzungsvorgang, um das Risiko der Multiplikation, Weitergabe oder des sonstigen Missbrauchs von Zugangsdaten an Minderjährige zu minimieren.“ (Döring, Günter, 2004, S. 232). Der Wirksamkeit allein wird nicht genüge getan, wenn die Altersprüfung anhand der Personalausweisnummer erfolgt, da solch eine Nummer einfach zu fälschen oder über das Internet zu beziehen

Das Prüfungsverfahren für telemediale Inhalte und Dienste erfolgt jedoch ohne staatliche Beteiligung – ist also nicht verbindlich vorgeschrieben und bringt keinerlei Konsequenzen bei Nichteinhaltung mit sich.

ist. Dennoch muss die zu ergreifende technische Maßnahme in jedem Fall verhältnismäßig sein und darf nicht gegen bestehende Verfassungsgrundsätze verstoßen. Allgemein wird die Nutzung eines Postident-Verfahrens von der KJM empfohlen.

Da Anbieter selten ihren Zugang beschränken wollen – sei es zeitlich oder durch eine geschlossene Gruppe – bleibt für viele der Weg der Programmierung mit einer Alterskennzeichung gemäß § 5 (3) Nr. 1 JMStV i.V. mit § 11 (1) JMStV. Dies hört sich komplizierter an als es tatsächlich ist und wird unter anderem auf der Internetseite der USK erläutert (USK, 2012). Technisch wird ein Alterslabel im Hauptverzeichnis der Webseite hinterlegt, welches von einer Jugendschutzsoftware gelesen werden kann. Diese Programme, soweit von Eltern entsprechend eingestellt, verhindern den Zugriff auf eine Seite, die eine höhere Alterskennung besitzt als für den Nutzer freigegeben.

Es bleibt festzuhalten, dass es eine Gesetzeslücke in Bezug auf rein serverbasierte Online-Spiele gibt: Eine Alterskennzeichnung wird dem Nutzer auf der Seite nicht angezeigt, sondern kann lediglich von einer vorgeschalteten Jugendschutzsoftware erkannt werden.

Das Internet lässt sich nicht säubern und die Möglichkeit von generellen Filtern ist weder gewünscht noch technisch machbar. Ebenso sind Inhalte nicht per se für Kinder und Jugendliche geeignet oder ungeeignet. Daher haben individuelle Abstufungen dem Alter entsprechend zu erfolgen. In Anbetracht dessen ist die Nutzung einer Jugendschutzsoftware gemäß dem Jugendschutzgesetz und dem Jugendmedienschutz-Staatsvertrag die einzige sinnvolle Alternative. Wie eingangs bereits gezeigt, setzen jedoch zu wenige Eltern auf eine entsprechende Jugendschutzsoftware, um ihre Kinder ausreichend zu schützen. Zur Erinnerung: gerade einmal ein Fünftel der Eltern haben ein entsprechendes Programm installiert (Hasebrink, 2011). Dass es sich bei allen 20% auch um die von der KJM anerkannten Programme zur Erkennung des Alterslabels handelt, darf bezweifelt werden. Darüber hinaus müssen diese Programme richtig eingestellt sein, um den Zugriff von Kindern und Jugendlichen auch auf nicht gelabelte Seite zu verhindern. Leider können Eltern solche Programme nur auf ihren eigenen Rechnern installieren; was außerhalb des eigenen Haushalts passiert, obliegt nicht mehr ihrer Kontrolle.

Seit 2011 ist die USK gemäß § 19 JMStV auch für die Alterskennzeichnung und als Bestellung zum Jugendschutzbeauftragten für Online-Spiele anerkannt. Aus diesem Gesetz ergibt sich jedoch keine Prüfplicht. Für welche Altersgruppe die Inhalte und Dienste geeignet sind, entscheidet allein der Anbieter. Den Anbietern von serverbasierten Online-Spielen steht auf der Seite der USK kostenlos ein Label-Generator zu Verfügung, mit dem eine Alterseinstufung sichtbar gemacht werden kann. Dieses Label ist technisch jedoch nur für Jugendschutzprogramme erkennbar. Eltern, die sich auf der Internetseite einen Überblick über ein Spiel verschaffen wollen, sehen dieses Label nicht. Lediglich, sofern das Spiel auch als Trägermedium erworben werden kann, muss der Anbieter laut § 12 JuSchG und JMStV das Kennzeichen der USK, das auch auf der Verpackung des Spiels zu finden ist, entweder in Textform oder als Symbol sichtbar auf der Internetseite vermerken. Hinzu kommt, dass erstmals am 8. Februar 2012 die Jugendschutzprogramme der Deutschen Telekom, Mitglied der FSM, und des JusProg e.V. durch die Kommission für Jugendmedienschutz anerkannt wurden (KJM, 2012).

Es bleibt festzuhalten, dass es eine Gesetzeslücke in Bezug auf rein serverbasierte Online-Spiele gibt: Eine Alterskennzeichnung wird dem Nutzer auf der Seite nicht angezeigt, sondern kann lediglich von einer vorgeschalteten Jugendschutzsoftware erkannt werden.

3.3 Strafgesetzbuch

Eine weitere für das Problem des Cybergroomings relevante Gesetzesgrundlage ist das Strafgesetzbuch. Doch auch

das StGB bietet keinen ausreichenden Schutz vor der Verbreitung von Cybergrooming im Netz, da nicht präventiv gegen Cybergrooming vorgegangen werden kann. Konkret heißt es hier:

> *„Mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren wird bestraft, wer […] auf ein Kind durch Vorzeigen pornographischer Abbildungen oder Darstellungen, durch Abspielen von Tonträgern pornographischen Inhalts oder durch entsprechende Reden einwirkt."* (§ 176 (4) StGB)

In Absatz 6 heißt es weiter:

> *„Der Versuch ist strafbar; dies gilt nicht für Taten nach Absatz 4 Nr. 3 und 4 und Absatz 5."* (§ 176 (6) StGB).

Der Versuch allein ist also nicht strafbar. In spektakulären Fällen wie der „Operation Donau" der Tuttlingener Polizei konnte gezeigt werden, dass die Rechtslage nicht ausreichend ist, um Cybergroomern effektiv das Handwerk zu legen, bevor es zu einer anderen Straftat wie dem Besitz von Kinderpornographie oder auch tatsächlichem Missbrauch kommt. Der Paragraph aus dem StGB ist prinzipiell nicht auf die Situation im Netz zugeschnitten: Auf einem Spielplatz würde sich die Frage nicht stellen, ob es ein Versuch war, mit sexuellen Schriften auf ein Kind einzuwirken oder ob es tatsächlich dazu kam. Um Straftaten vorzubeugen, wird sich kein Polizist als Kind ausgeben und darauf warten angesprochen zu werden. Im Netz stellt sich eine andere Situation dar: Um strafverfolgend tätig werden zu können müsste man demnach mit Kindern als Köder arbeiten. Als Kinder getarnte Polizei- und Kriminalbeamte haben rechtlich gesehen keine Eingriffsgrundlage, auch wenn das Gegenüber davon ausgeht, dass auf der anderen Seite des Bildschirms ein Kind unter 14 Jahren sitzt. Die Strafverfolgungsbehörden haben lediglich die Möglichkeit tätig zu werden, wenn es zum Beispiel Hinweise auf den Besitz von kinderpornographischem Material gibt. Obwohl Cybergrooming als Anbahnungsphase von sexuellem Missbrauch von Kindern definiert ist (Rüdiger, 2012) und häufig in tatsächlichem Missbrauch resultiert (Finkelhor, 2008), haben Ordnungshüter nach geltender Gesetzeslage lediglich eine Kontrollfunktion. Diese ist dennoch nicht ganz zu verachten. Denn wo gar keine Kontrolle ist, werden Täter nicht gestört und können ungehindert vorgehen. Umso wichtiger ist die Aufklärung der Bevölkerung: Vorfälle, bei denen Kinder involviert waren, müssen gemeldet werden, um diese entsprechend ahnden zu können.

Als Kinder getarnte Polizei- und Kriminalbeamte haben rechtlich gesehen keine Eingriffsgrundlage, auch wenn das Gegenüber davon ausgeht, dass auf der anderen Seite des Bildschirms ein Kind unter 14 Jahren sitzt.

4. Alterskennzeichnungen von Spielen und telemedialen Inhalten

Ein wichtiges Instrument im Jugendschutz ist die Alterskennzeichnung von Inhalten – sei es durch den Aufdruck auf Verpackungen, dies hat Signalwirkung für Eltern – oder rein technisch als Label, das von einer Jugendschutzsoftware gelesen werden kann. An dieser Stelle sollen nur kurz die einzelnen Themenbereiche genannt werden, ohne detailliert auf die Entwicklungsbeeinträchtigung einzugehen. Darüber hinaus werden Probleme der derzeitigen Kennzeichnung beleuchtet. Da der Begriff der Entwicklungsbeeinträchtigung weder im Jugendschutzgesetz noch im Jugendmedien-Staatsvertrag genau definiert ist, wird die Begriffserläuterung nach der FSM, eine der anerkannten Einrichtungen der Freiwilligen Selbstkontrolle gemäß § 19 JMStV, herangezogen. Ebenso wird mit den Vorgaben der USK gearbeitet.

4.1 Entwicklungsbeeinträchtigung gemäß JMStV und Jugendschutzgesetz

Der Begriff der Entwicklungsbeeinträchtigung entstand im Zuge der Novellierung

des JMStV aus dem Jahr 2003. Genau definiert wurde er dabei jedoch nicht.

Im Jugendmedienschutz-Staatsvertrag heißt es wörtlich:

> *„Sofern Anbieter Angebote, die geeignet sind, die Entwicklung von Kindern oder Jugendlichen zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit zu beeinträchtigen, verbreiten oder zugänglich machen, haben sie dafür Sorge zu tragen, dass Kinder oder Jugendliche der betroffenen Altersstufe sie üblicherweise nicht wahrnehmen."* (§ 5 (1) JMStV)

Dabei werden Wertmaßstäbe, die sich aus dem Grundgesetz ablesen lassen, in unserer Gesellschaft als entscheidend angesehen.

Die FSM kam zu einer Definition in der ersten Entscheidung ihres Beschwerdeausschusses:

> *„Entwicklungsbeeinträchtigend sind Angebote, die durch Hervorrufen einer erheblichen Irritation von Kindern und/ oder Jugendlichen in Bezug auf ihre gewöhnliche Lebenswelt geeignet sind, auf die Entwicklung der Persönlichkeit von Kindern und Jugendlichen einen negativen, dem Menschenbild des Grundgesetzes widersprechenden Einfluss auszuüben und somit die Entwicklung zu einem eigenverantwortlichen, sich innerhalb der sozialen Gemeinschaft frei entfaltenden Menschen zu hemmen, zu unterbrechen oder zurückzuwerfen."* (FSM, 2004)

Diese mehrfach zitierte Begriffsbestimmung beinhaltet die Frage nach der Auswirkungen auf Handlungen, Einstellungen und Erlebnisweisen der Kinder und Jugendlichen. Dabei werden Wertmaßstäbe, die sich aus dem Grundgesetz ablesen lassen, in unserer Gesellschaft als entscheidend angesehen. Insbesondere für die thematische Unterteilung der Inhalte in die Bereiche Erotik, Gewalt und Extremismus sind zu nennen:

- Achtung der Menschenwürde
- Gleichbehandlung
- Demokratieprinzip

Weiterhin lässt sich die Abstufung der Beeinträchtigung nach Altersgruppen ausmachen, da Kinder und Jugendliche unterschiedlichen Alters auch unterschiedlich anfällig für Entwicklungsbeeinträchtigungen sind. Es gibt also keine allgemeingültigen Maßstäbe für Kinder und Jugendliche; vielmehr sind diese im Kontext zu betrachten (FSM, 2004).

Der Beirat der USK beschließt und passt die Bewertungskriterien der USK an. Hier wird der Begriff der Entwicklungsbeeinträchtigung in den USK-Grundsätzen folgendermaßen definiert:

> *„Unter Beeinträchtigung sind Hemmungen, Störungen oder Schädigungen durch Überreizung, Überlastung, Übererregung zu verstehen. Insbesondere Inhalte von Spielen, welche die „charakterliche, sittliche (einschließlich religiöse) oder geistige Erziehung hemmen, stören oder schädigen oder sozialethisch desorientierend wirken, können die Entwicklung von Kindern und Jugendlichen oder ihre Erziehung zu einer eigenverantwortlichen und gemeinschaftsfähigen Persönlichkeit beeinträchtigen."* (§19 (2) USK-Grundsätze)

Spiele werden durch die USK in insgesamt 15 verschiedenen Dimensionen, denen einen Wirkungsmacht eingeräumt wird, untersucht (USK, 2011):

- Visuelle und akustische Umsetzung der Spielidee
- Gameplay
- Atmosphäre
- Realismus
- Glaubwürdigkeit
- Menschenähnlichkeit
- Jugendaffinität und Identifikationspotenzial
- Handlungsdruck
- Gewalt
- Krieg
- Angst und Bedrohung
- Sexualität
- Diskriminierung
- Sprache

- Drogen

Die Erläuterungen der USK zu ihren Grundsätzen machen deutlich, dass es lediglich auf statische Inhalte von Spielen und telemedialen Inhalten und deren Wirkung ankommt. Es wird jedoch nur oben genannten Aspekten eine relevante Wirkung unterstellt.

Sehr vielen verschiedenen Dimensionen wird bei der USK Beachtung geschenkt, dennoch ist die Gefahr für Kinder Opfer einer Straftat zu werden keineswegs in dieser Sichtweise enthalten. Außer Acht gelassen wird gänzlich, dass Kinder auch anderen Gefahren, die außerhalb der USK-Kriterien liegen, ausgesetzt sind. So bieten nicht nur serverbasierte Spiele, sondern auch Konsolenspiele die Möglichkeit zur Kontaktaufnahme, bei der es zu einer sexuellen Belästigung kommen kann. Dieser Gedanke der Viktimisierung ist in den Überlegungen zur Einstufung von Spielen, Online-Diensten und Inhalten nicht enthalten.

Während Spiele auf Trägermedien durch die USK geprüft werden, müssen Anbieter von Online-Spielen, aber auch sonstigen telemedialen Inhalten und Diensten gemäß JMStV selbst einschätzen inwiefern die angebotenen Inhalte und Dienste entwicklungsbeeinträchtigend sind. Grundvoraussetzungen dafür sind, sich in die psychologische Verfassung von Jugendlichen versetzen zu können, die Wirkungsmacht des Mediums Internet im Alltag der betreffenden Altersgruppen und die verfassungsimmanenten Werte unserer Gesellschaft zu kennen.

4.2 Alterseinstufung und Cybergrooming

Die Kriterien der USK oder auch der FSM sind keineswegs in Stein gemeißelt. Sie könnten also angepasst und erweitert werden. Dies ist in Bezug auf das Problem des Cybermobbings, vielmehr aber noch des Cybergroomings sehr zu begrüßen, da ein wichtiger Punkt bisher nicht beachtet wurde und eine Ergänzung der Kriterien notwendig ist, um effektiven Schutz vor Viktimisierung zu bieten: Das Risiko der anonymen Online-Kommunikation.

Die Alterskennzeichnungen gehen in keiner Weise auf die Gefahren des Cybergroomings ein. Die zuvor erläuterten Einstufungskriterien bei Online-Medien und -Spielen sind ungeeignet, Risikopotentiale zu erkennen, geschweige denn zu lösen. Alle bisherigen Einstufungskriterien basieren vornehmlich auf der Prüfung des Spieleinhalts auf Jugendbeeinträchtigung oder -gefährdung. Im Kern liegt der Alterseinstufung lediglich zu Grunde, ob das Spiel übermäßige und/oder menschenverachtende Gewaltanwendung beinhaltet und/oder ob pornografische Inhalte dargeboten werden. Die dabei angewandten Kriterien für eine Alterseinstufung basieren noch auf der Annahme, dass der Nutzer alleine und nicht über das Internet kommunizierend spielt. Dies entspricht jedoch nicht mehr der modernen Mediennutzung. Mittlerweile kommt fast kein Spiel ohne die Möglichkeit des onlinebasierten Zusammenspiels aus. Die dort ablaufenden Interaktions- und Kommunikationsprozesse bergen das Risiko der Begehung von schwerwiegenden Delikten zwischen den Nutzern. Die Anonymität des Internets begünstigt das besonders gravierende und für Kinder höchstgefährliche Phänomen des Cybergroomings. Eine Vielzahl von Online-Spielen oder sozialen Plattformen ist von der grafischen Gestaltung auf die Zielgruppe der Kinder und Jugendlichen ausgerichtet (vgl. Habbo Hotel, NeoPets, Knuddels). Es ist dabei naheliegend, dass solche von Kindern genutzten und ungesicherten Spiele und Dienste auch für Pädokriminelle äußerst attraktiv sind. Im selbigen Maß wie ein Anbieter Kinder als Zielgruppe hat oder diese akzeptiert, sollte er auch verpflichtet werden, Schutzmechanismen zu integrieren, die diese Gefahren des Cybergroomings weitest-

Die Kriterien der USK oder auch der FSM sind keineswegs in Stein gemeißelt. Sie könnten also angepasst und erweitert werden. Dies ist in Bezug auf das Problem des Cybermobbings, vielmehr aber noch des Cybergroomings sehr zu begrüßen, da ein wichtiger Punkt bisher nicht beachtet wurde und eine Ergänzung der Kriterien notwendig ist, um effektiven Schutz vor Viktimisierung zu bieten: Das Risiko der anonymen Online-Kommunikation.

gehend verhindern. Effektive Sicherheitsvorkehrungen fehlen leider in fast allen heutigen Spielen – unabhängig davon ob diese auf Datenträgern oder rein online erhältlich sind.

Wichtig ist zu erkennen, dass vielen Kindern und Jugendlichen nicht einmal bewusst ist, dass sie gerade Opfer einer Straftat geworden sind und dieses Problem der sexuellen Ansprache und Belästigung gesellschaftlich bagatellisiert wird. Vielen Eltern ist dieses Phänomen weder bekannt noch kennen sie die Ausmaße. Zum einen lässt sich der Generationenkonflikt als Ursache ausmachen. Dieser führt dazu, dass Eltern, Lehrer und sonstige Vertrauenspersonen als kompetente Ansprechpartner ausgeschlossen werden. Die meisten Eltern sehen sich die Seiten im Internet, die ihre Kinder besuchen, nicht an und erfahren somit nicht, welche Gefahren es dort konkret gibt. Zum anderen verlassen sich selbst Eltern, die den Kinder- und Jugendschutz ernstnehmen, auf die offiziellen Angaben der Altersfreigabe der USK und den anderen dazu befähigten Akteuren. An dieser Stelle ist anzuknüpfen und die Kriterien für die Altersfreigaben sind zu überarbeiten.

Wichtig ist zu erkennen, dass vielen Kindern und Jugendlichen nicht einmal bewusst ist, dass sie gerade Opfer einer Straftat geworden sind und dieses Problem der sexuellen Ansprache und Belästigung gesellschaftlich bagatellisiert wird.

Nichtregulierte Freiwilligkeit und bisherige Maßnahmen wie die Bestellung eines Jugendschutzbeauftragten nach § 7 JMStV, der keinerlei Weisungsbefugnis hat, versteckte Hinweise für den Umgang mit Cybergroomern geben kann oder auch eine rein Blockier- oder Ignorierfunktion reichen einfach nicht aus. Der Täter wird dadurch keinesfalls unschädlich gemacht. Er würde seine Bemühungen lediglich auf das nächste Kind verlagern oder einfach mit einem anderen Account auf das gleiche Kind erneut zugehen (Rüdiger, 2012).

5. Reformbedarf

Da es sich bei der Problematik um ein nicht auf Deutschland beschränktes Phänomen handelt, sind, auch wenn eine internationale Lösungsstrategie zeitnah nicht realistisch ist, Kooperationen zu erarbeiten, die besonders auch auf kulturelle Unterschiede eingehen. Allein innerdeutsche Konflikte bei der Thematik des Jugendmedienschutzes zeigen, dass man noch weit von einer internationalen Lösung entfernt ist. Daher sollen an dieser Stelle zumindest für Deutschland Reformvorschläge aufgezeigt werden.

5.1 Gesetzesreform Jugendmedienschutz

Angesichts der verschwimmenden Grenzen zwischen online und offline auch bei Computerspielen wird klar, wie nötig eine einheitliche Anlaufstelle und eine Gesetzesgrundlage ist, die das Thema Jugendschutz umfassend abdeckt. Eine Differenzierung zwischen Computerspielen auf Trägermedien und serverbasierten, die mit einer unterschiedlichen Verpflichtung in Bezug auf den Jugendschutz einhergeht, geht an der Realität vorbei und ist schlichtweg antiquiert. Neben einer Vereinheitlichung ist die Dynamik der Prozesse zu berücksichtigen. Umständliche Gesetzesnovellierungen, bei denen jedes Mal ein ideologischer Kampf entfacht, können keinen effektiven und den Marktveränderungen angepassten Jugendmedienschutz bieten. Daher ist weiter verstärkt auf die regulierte Selbstregulierung zu setzen.

Die Natur des Internets – anders als die von herkömmlichen Medien – beinhaltet Interaktionsmöglichkeiten. Die Anonymität im Internet verringert die Hemmschwelle, die von einer Viktimisierung von Kindern und Jugendlichen in der realen Welt, z.B. auf dem Spielplatz, schützen könnte. Um Cybergroomer effektiv verfolgen zu können, ist eine Überarbeitung des Strafgesetzbuches dahingehend notwendig, dass bereits der Versuch strafbar ist. Die Intention der Täter sollte dabei im Vordergrund stehen.

In Anbetracht der Tatsache, dass rechtlich zwischen Kindern, Jugendlichen und Erwachsenen unterschieden wird, sollten Altersgruppen dementsprechend angepasst werden, um nicht zu viele Altersstufen im Netz zu erhalten. Einen wichtigen Beitrag stellen die Altersverifikationssysteme in Form von geschlossenen Gruppen dar gemäß § 5 JMStV. Diese Form der Zugangsbeschränkung vom Anbieter selbst gewählt, sollte eine bessere Förderung erfahren. Hier sollten Anreize geschaffen werden, um Kindern den Zugang zu jugendgefährdenden Inhalten, selbst wenn sie gezielt danach suchen, effektiv zu erschweren. Auf der anderen Seite bedarf es der Schaffung von mehr und vor allem von sichereren Surfräumen für Kinder und Jugendliche.

5.2 Paradigmenwechsel „Entwicklungsbeeinträchtigung“

Nicht nur die Gesetzeslage sollte vereinfacht werden, auch die Transparenz bei der Vergabe von Alterskennzeichnungen ist zu verbessern. Erst nach genauer Recherche ist eine Zuordnung von Inhalten und Diensten möglich. Wie aber sollen Konsumenten, Eltern und Kinder erkennen, was hinter der Alterklassifizierung steckt, wenn sie ein Produkt im Laden in den Händen halten? Da hilft es wenig, das bekannte Label der USK noch größer auf die Verpackung zu drucken. Vielmehr sollte deutlich gemacht werden, was sich dahinter verbirgt. Eine Möglichkeit wäre, wie bei dem paneuropäischen System PEGI, mit kleinen Symbolen zu arbeiten, die genaueren Aufschluss darüber geben, was von diesem Spiel oder Inhalt zu erwarten ist.

Wichtig ist weiterhin, dass die gesetzliche Regelannahme des Alleinspielers aufgegeben wird und die Risiken der anonymen und meist unkontrollierten Online-Kommunikation beachtet und in die Bewertung einbezogen werden. Die zuvor erfolgte Diskussion der Problematik der Kriterien der USK für die Vergabe von Alterskennzeichnung führt zu folgenden Verbesserungsvorschlägen bezüglich der Einstufung von kinder- und jugendgefährdenden Inhalten und Diensten.

Als erstes ergibt sich die Forderung nach der prinzipiellen Aufnahme eines Kriteriums zur Sicherheit des Kommunikationsweges für Online-Spiele in die Leitkriterien für die Bewertung von Spielen und Inhalten. Die neuen Kriterien sollten nicht nur für rein serverbasierte Online-Spiele gelten, sondern auch für Konsolen-Spiele (Wii, X-Box, Playstation, Nintendo DS, usw.), da auch diese die Möglichkeit zur Online-Kommunikation bieten.

Konkret können Auflagen erstellt werden, die Betreiber verpflichten, Kinder und Jugendliche besser zu schützen, sofern sie ihre Spiele gezielt Kindern überlassen wollen: Unkontrollierte Kommunikationswege setzen Kinder und Jugendliche der Gefahr der Viktimisierung durch Cybergrooming oder andere Delikte aus. Eine Lösungsmöglichkeit bietet die Kommunikation nur über vorgefertigte Sätze und Wörter, wie es bereits bei einigen kindgerechten Chats funktioniert. Auch könnte die permanente Anwesenheit von qualifizierten Moderatoren eine effektive Schutzmaßnahme sein. Unbeaufsichtigte Chats sollten für Kinder prinzipiell nicht möglich sein. Die Qualität der Moderatoren, d.h. Aufsichtspersonal und Ansprechpartner eines Spiels oder Chats, sollte sichergestellt werden. Nach einer sexuellen Viktimisierung sind sie oftmals die ersten Ansprechpartner für Kinder. Die Betreiber setzen derzeit überwiegend unausgebildete Laienkräfte, sog. Gamemaster, ein, die aus dem Spielerkreis rekrutiert werden. Auch der gemäß dem Jugendmedienschutz-Staatsvertrag eingesetzte Jugendschutzbeauftragte kann diese Rolle allein nicht übernehmen, da diese im JMStV nicht hinreichend konkretisiert ist noch auf die Qualität der übrigen Moderatoren Einfluss hat. Eine Verpflichtung für eine entsprechende Schulung oder ein Nachweis eines

Konkret können Auflagen erstellt werden, die Betreiber verpflichten, Kinder und Jugendliche besser zu schützen, sofern sie ihre Spiele gezielt Kindern überlassen wollen: Unkontrollierte Kommunikationswege setzen Kinder und Jugendliche der Gefahr der Viktimisierung durch Cybergrooming oder andere Delikte aus.

Zertifikats wäre hier ein wichtiger Schritt, um fachkundig mit Folgen von sexueller oder sonstiger Viktimisierung umgehen zu können. Ein solches Zertifikat könnte ähnlich einem IHK-Zertifikat aufgebaut werden. Um zu verhindern, dass Personen mit kriminellen Intentionen als Moderatoren eingesetzt werden, sollte die Vorlage eines erweiterten polizeilichen Führungszeugnisses ebenso verpflichtend sein.

Wie im vorherigen Teil bereits skizziert, ist die Diskrepanz zwischen Gesetz und Einstufungskriterien zu überdenken. Nicht nur, da es für viele Anbieter schwierig ist, die eigenen Inhalte entsprechend richtig zu klassifizieren, sollten die Alterskategorien für Spiele, telemediale Inhalte und Dienste vereinfacht werden. Ferner unterscheidet der Gesetzgeber zwischen Kindern, Jugendlichen und Erwachsenen. Bis 14 gilt man gesetzlich als Kind, von 14 bis 18 Jahren als Jugendlicher. Eine Einteilung bzw. zumindest aber eine Berücksichtigung dieser wichtigen Altersstufe ist beim Kinder- und Jugendschutz wichtig. Der Schutzauftrag vor sexuellem Missbrauch und auch vor Cybergrooming aus §176 (4) Nr.3 StGB bezieht sich auf Personen unter 14 Jahren, also auf Kinder. Daraus ergibt sich zwangsläufig eine Diskrepanz zu den aktuellen Altersstufen der USK-Labels „freigegeben ab 12“ oder „ab 16 Jahren“. Der Gesetzgeber stellt einerseits die sexuelle Kommunikation mit Kindern unter 14 unter Strafe, suggeriert den Eltern jedoch andererseits eine falsche Sicherheit durch die Altersfreigabe ab 12 Jahren. Hier wird suggeriert, dass das Spielen von Online-Spielen und die damit einhergehende unkontrollierte Kommunikation ungefährlich sei. Die im StGB vorgesehene Altersgrenze ab 14 Jahren sollte daher auch für die Alterseinstufung der USK berücksichtigt werden.

Im Bereich Medienkompetenz sind es in erster Hinsicht die Kinder der Elternzeitschriftenleser, die durch Netz- und Flyerkampagnen erreicht werden, nicht aber diejenigen, die ohnehin benachteiligt sind und bei denen der Medienkonsum weit über dem Durchschnitt liegt.

5.3 Medienkompetenz in den Lehrplan

Abschließend soll ein wichtiger Baustein im Jugendmedienschutz in den Blick genommen werden, der gerne auch von der Politik aus den Augen gelassen wird: das Thema Medienkompetenz. Es geht darum, junge Menschen so früh wie möglich mit der digitalen Welt vertraut zu machen, aber auch Lehrern und Eltern Kompetenz zu vermitteln. Diese sind sich häufig nicht bewusst, welchen Stellenwert das Internet für Kinder einnimmt. Ferner sind Eltern und Lehrer zum Teil auch mit dem Thema überfordert oder haben kein Interesse dafür. Vielfach fehlen auch grundlegende Kenntnisse über soziale Netzwerke, Möglichkeiten und Mechanismen im Internet sowie über Kommunikations- und Interaktionsmöglichkeiten in Online-Games und Chat-Foren. Die aktuelle Bildungslandschaft, insbesondere die Schulen, sind in diesem Punkt noch nicht im 21. Jahrhundert angekommen. Auch wenn das Thema Internetsicherheit europaweit in 23 Ländern als eigenes Unterrichtsthema im Lehrplan vorgesehen ist, bleibt das Thema engagierten Lehrerinnen und Lehrern, einzelnen Initiativen vor Ort oder NGOs vorbehalten. Weder in den Lehrplänen noch in der Lehrerausbildung spielt dieses für die Zukunft der Kinder aber auch der Gesellschaft entscheidende Thema die Rolle, die es verdient.

Durch die allgemeine Schulpflicht ist sichergestellt, dass jedes in Deutschland lebende Kind die Chance und Möglichkeit erhält Lesen und Schreiben zu lernen. Dies bezieht sich auf Kinder aller Schichten und Nationalitäten und ist einer der Garanten für Chancengleichheit und soziale Gerechtigkeit. Im Bereich Medienkompetenz sind es in erster Hinsicht die Kinder der Elternzeitschriftenleser, die durch Netz- und Flyerkampagnen erreicht werden, nicht aber diejenigen, die ohnehin benachteiligt sind und bei denen der Medienkonsum weit über dem Durchschnitt liegt. Es bedarf einer verbindlichen Aufnahme dieser Themen in die Lehrerausbildung. Medienführerscheine sollten nicht fakultativ, sondern fester Bestandteil des Lehrplans werden. Es ist wichtig über Regelangebote in Kita und Schule den Zugang zu den Eltern zu

bekommen, um sie einzubinden. Dies lässt sich nicht allein an die Schulen delegieren – ohne Eltern wird und kann Jugendschutz auch als allgemeine Erziehungsaufgabe nicht funktionieren. Um eine flächendeckende Medienkompetenz im Lehrplan zu verankern, Eltern einzubeziehen aber auch Lehrer und Erzieher fit für das Netz zu machen, haben Regierung, Anbieter, Öffentlichkeit und Schulen an einem Strang zu ziehen.

Als sinnvoll erscheint dabei auch die Verankerung dieser Bemühungen im Jugendmedienschutz-Staatsvertrag und Jugendschutzgesetz. Dabei sollte nicht nur Verpflichtungen, sondern auch um konkrete Maßnahmen handeln. Die Mehrzahl der NGOs verfügt bereits über den Willen, aber nicht über ausreichende Mittel, die es ermöglichen, einen optimalen Beitrag zur Medienkompetenzvermittlung zu leisten. Im Rahmen von Public Privat Partnerships könnten die standardisierenden und kontrollierenden Eigenschaften des Staates mit dem Engagement von NGOs sowie den finanziellen Mitteln, technischen Ressourcen und hervorragenden Möglichkeiten der Distribution von Anbietern verbunden werden.

Gute Praktiken sollten etabliert werden, damit Sensibilisierungskampagnen stets alle Kinder, Eltern, Lehrer und Betreuer in der gesamten EU erreichen. Effektive Sensibilisierungsstrategien berücksichtigen die unterschiedlichen Entwicklungsstände jüngerer bzw. älterer Kinder und Jugendlicher und konzentrieren sich insbesondere auf die jüngsten und schutzbedürftigen Kinder, darunter auch jene mit Lernschwierigkeiten und geistigen Behinderungen. Gleichzeitig stellt die gegenseitige Erziehung unter Gleichaltrigen für Kinder aller Altersgruppen eine wichtige Strategie dar, um ihnen ihre Rechte und ihre Verantwortung im Online-Umfeld bewusst zu machen.

Dem Konzept der Freiwilligen Selbstkontrolle folgend, sollten auch die Ressourcen der Netzgemeinde und User eingesetzt werden. Sie sind direkt am Geschehen beteiligt und können wertvolle Hinweise geben. Somit wird die Selbstkontrolle nicht nur von den Anbietern, sondern auch den Nutzern sichergestellt.

6. Zusammenfassung und Ausblick

Es wurde der Reformbedarf für den Jugendmedienschutz in Deutschland aufgezeigt. Die Ankündigung einer geplanten Reform des Jugendschutzgesetzes vom 13.04.2012 durch das Bundesministerin für Familie, Senioren, Frauen und Jugend, um Online-Filme und Online-Spiele nach den Bestimmungen des Jugendschutzgesetzes kennzeichnen lassen zu können, ist nur ein erster Schritt. Es bedarf aber eines echten Paradigmenwechsels. Wichtig ist die Aufhebung der Trennung zwischen virtueller und realer Welt in den Köpfen und in den Gesetzen und die Etablierung eines einheitlichen transparenten Gesetzes mit einer Anlaufstelle zum Schutz von Kindern und Jugendlichen. Jugendschutzprogramme sind bei Eltern bisher nicht weit verbreitet. Gerade deswegen ist es auch sinnvoll, Eltern und Konsumenten die Bedeutung von Alterskennzeichnungen im Rahmen des Jugendmedienschutzes deutlich zu machen. Auch bei Online-Spielen sollte dieses Merkmal auf den ersten Blick erkennbar sein. Wichtig ist weiterhin, beim Jugendschutz nicht nur die statischen Angebote des Netzes zu bewerten. Vielmehr sind auch die Kommunikationswege, also die dynamischen Prozesse, in die Kontextbetrachtung aufzunehmen, um der potenziellen Viktimisierung von Kindern und Jugendlichen entgegenzuwirken.

Dabei ist zu berücksichtigen, dass die Entwicklung von Technologien schneller und schneller weiter voranschreitet, so dass meist keine Zeit für zeitaufwendige Gesetzesnovellierungen bleibt. Die Unfähigkeit Deutschlands, auf Marktver-

Effektive Sensibilisierungsstrategien berücksichtigen die unterschiedlichen Entwicklungsstände jüngerer bzw. älterer Kinder und Jugendlicher und konzentrieren sich insbesondere auf die jüngsten und schutzbedürftigen Kinder, darunter auch jene mit Lernschwierigkeiten und geistigen Behinderungen.

Freie Meinungsäußerung und der Zugang zu Informationen stehen nicht im Gegensatz zum Jugendschutz.

änderungen dynamisch zu reagieren, zeigt sich daran, dass in Deutschland die Behandlung von Online-Spielen immer noch nicht ausreichend geregelt ist, während zum Beispiel das Paneuropäische System PEGI – gültig in allen anderen Ländern Europas – bereits seit 2003 Online-Spiele abdeckt und seit 2012 bereits Apps für Smartphones und Tablets in ihre Bewertungen aufgenommen hat.

Ein weiterer Punkt stellt den Kinder- und Jugendschutz vor ein noch größeres Problem als die Rasanz der Marktentwicklung: Bereits 2008 gab Google bekannt, dass es mittlerweile 1 Billion URLs im Internet gibt (Google, 2008). Die Zahl dürfte mittlerweile weiter gestiegen sein. Dagegen gibt es derzeit über 15 Millionen Seiten mit der Domain „.de“ (DENIC eG, 2013). Obwohl diese nicht gleichzusetzen sind mit allen Seiten aus Deutschland, kann davon ausgegangen werden, dass durch die deutsche Gesetzeslage nur ein geringer Bruchteil der in Deutschland abrufbaren Seiten durch das Jugendschutzgesetz, den Jugendmedien-Staatsvertrag und das Strafgesetzbuch geregelt werden können. Auf Seiten außerhalb der Zuständigkeit, welche an den Grenzen der Bundesrepublik enden, haben diese Gesetze keinen Einfluss. Langfristig kann nur eine grenzübergreifende Kooperation zu einem effektiven Schutz vor entwicklungsbeeinträchtigenden Inhalten führen.

Um Kindern und Jugendlichen genügend Kompetenzen zu vermitteln und in ihren Werten zu stärken und um die Gesellschaft entsprechend zu sensibilisieren, ist das Thema Medienkompetenz in den Lehrplänen zu verankern. In vielen weiterführenden Schulen gibt es bereits Informatik als Arbeitsgemeinschaft oder als Unterrichtsfach. Dabei liegt der Schwerpunkt jedoch mehr auf technischen Aspekten und weniger auf sozialer Kompetenz im Internet.

Notwendig für die Etablierung eines einheitlichen Jugendschutzes in Deutschland ist die Überwindung von Vorurteilen und verhärteten Fronten. Netzaktivisten sollten in den Jugendmedienschutz verstärkt eingebunden werden, um gar nicht erst in eine oppositionelle Ecke gedrängt zu werden. Freie Meinungsäußerung und der Zugang zu Informationen stehen nicht im Gegensatz zum Jugendschutz. Gute Lösungen erfordern fachkundige Spezialisten, die Vorschläge erarbeiten und prüfen, und um das Internet für jene sicherer zu machen, die den Schutz der Gesellschaft dringend brauchen: Kinder und Jugendliche.

7. Literature

Google (25.07.2008): We knew the web was big… Alpert, Jesse; Hajaj, Nissan. Online verfügbar unter http://googleblog.blogspot.de/2008/07/we-knew-web-was-big.html, zuletzt geprüft am 14.01.2013.

DENIC eG (14.01.2013): www.denic.de. DENIC eG. Online verfügbar unter www.denic.de, zuletzt geprüft am 14.01.2013.

Döring, Martin; Günter, Thomas: Jugendmedienschutz: Alterskontrollierte geschlossene Benutzergruppen im Internet gem. § 4 Abs. 2 Satz 2 JMStV. In: MMR, 4/2004, S. 231–237. Online verfügbar unter http://www.jugendschutz.net/pdf/mmr_avs.pdf, zuletzt geprüft am 14.01.2013.

Dyckmans, Mechthild (2012): Drogen- und Suchtbericht. Hg. v. Die Drogenbeauftragte der Bundesregierung. Online verfügbar unter http://www.drogenbeauftragte.de/fileadmin/dateien-dba/Presse/Downloads/12-05-22_DrogensuchtBericht_2012.pdf, zuletzt geprüft am 14.01.2013.

Finkelhor, David (2008): Childhood victimization. Violence, crime and abuse in the lives of young people. New York: Oxford University Press.

Freiwillige Selbstkontrolle der Multimedia-Diensteanbieter (2004): Der Begriff der Entwicklungsbeeinträchtigung in § 5 des Jugendmedienschutz-Staatsvertrags. Hg. v. FSM. Online verfügbar unter http://www.fsm.de/de/entwicklungsbeeintraechtigung, zuletzt geprüft am 14.01.2013.

Haddon, Leslie; Livingstone, Sonia; EU Kids Online network (2011): EU Kids Online: National perspectives. Hg. v. EU Kids Online. Bristol. Online verfügbar unter http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/PerspectivesReport.pdf, zuletzt geprüft am 14.01.2013.

Hasebrink, Uwe; Lampert, Claudia; Schröder, Hermann-Dieter; Drosselmeier, Marius (2011): Jugendmedienschutz aus Sicht der Eltern. Kurzbericht über eine Studie des Zweiten Deutschen Fernsehens. Hg. v. Uwe Hasebrink. Hans-Bredow-Institut für Medienforschung an der Universität Hamburg. Hamburg. Online verfügbar unter http://www.unternehmen.zdf.de/fileadmin/files/Download_Dokumente/DD_Das_ZDF/Veranstaltungsdokumente/ZDF-Studie_Jugendmedienschutz_aus_Sicht_der_Eltern_2011.pdf, zuletzt geprüft am 14.01.2013.

Katzer, Catarina (2007): Gefahr aus dem Netz. Der Internet-Chatroom als neuer Tatort für Bullying und sexuelle Viktimisierung von Kindern und Jugendlichen. Dissertation. Universität zu Köln, Köln. Wirtschafts- u. Sozialwissenschaftliche Fakultät, zuletzt geprüft am 14.01.2013.

Kommission für Jugendmedienschutz (09.02.2012): KJM erkennt erstmals zwei Jugendschutzprogramme unter Auflagen an. Kommission für Jugendmedienschutz. Online verfügbar unter http://www.kjm-online.de, zuletzt geprüft am 14.01.2013.

Medienpädagogischer Forschungsverbund Südwest (2011): KIM-Studie 2010. Kinder + Medien, Computer + Internet. Hg. v. Medienpädagogischer Forschungsverbund Südwest. Stuttgart. Online verfügbar unter http://www.mpfs.de/fileadmin/KIM-pdf10/KIM2010.pdf, zuletzt geprüft am 14.01.2013.

National survey of American attitudes on substance abuse XVI: teens and parents (2011). Conducted by: QEV Analytics, Ltd. Knowlegde Networks. The national center on addiction and substance abuse at Columbia University.

Rüdiger, Thomas Gabriel: Cybergrooming in virtuellen Welten – Chancen für Sexualstraftäter?, 2/2012). In: Deutsche Polizei, 2/2012, S. 29–35. Online verfügbar unter http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&ved=0CEwQFjAD&url=http%3A%2F%2Finstitut-kreative-wissenschaft.com%2Fapp%2Fdownload%2F5780972045%2FCybergrooming%2Bin%2Bvirtuellen%2BWelten%2BDeutsche%2BPolizei%2B2_2012.pdf&ei=Nmf0UImhA8ntsgbe44GACg&usg=AFQjCNF

zQRMGqjYN4qY6hdA23_6iE8w1Rw&sig2=FLUS4IaQoqgeO1KTi1QC9w&bvm=bv.1357700187,d.Yms, zuletzt geprüft am 14.01.2013.

LBS-Kinderbarometer (29.10.2012): Kinder und Internet: Kontakte pflegen ja – neue Freunde eher nicht. Dr. Christian Schröder. Online verfügbar unter http://www.lbs.de/bremen/presse/initiativen/kinderbarometer/kinder-und-internet, zuletzt geprüft am 14.01.2013.

Schulz, Wolfgang; Held Torsten (2002): Regulierte Selbstregulierung als Form modernen Regierens. eine Studie im Auftrag des Bundesbeauftragten für Kultur und Medien (Endbericht). Hg. v. Hans-Bredow-Institut für Medienforschung an der Universität Hamburg. Hans-Bredow-Institut für Medienforschung an der Universität Hamburg. Hamburg (Arbeitspapiere des Hans-Bredow-Instituts Nr. 10, 10).

Spitzer, Manfred (2012): Digitale Demenz. Wie wir uns und unsere Kinder um den Verstand bringen. München: Droemer Knaur.

Unterhaltungssoftware Selbstkontrolle (2011): Grundsätze der Unterhaltungssoftware Selbstkontrolle (USK). Hg. v. USK. Online verfügbar unter http://www.usk.de/fileadmin/documents/Publisher_Bereich/USK_Grundsaetze_2011.pdf, zuletzt geprüft am 14.01.2013.

Unterhaltungssoftware Selbstkontrolle (2011): Leitkriterien der USK für die jugendschutzrechtliche Bewertung von Computer- und Videospielen. Hg. v. USK. Online verfügbar unter http://www.usk.de/fileadmin/documents/2011-06-27_Leitkriterien_USK.pdf, zuletzt geprüft am 14.01.2013.

Zu der Autorin

Ines Kawgan-Kagan wurde 1982 in Berlin geboren und studierte an der Fachhochschule für Verwaltung und Rechtspflege Öffentliche Verwaltungswirtschaft sowie an der Freien Universität Berlin Soziologie im Masterprogramm European Societies. Sie ist Mutter von vier Kindern und befasste sich bei der Deutschen Kinderhilfe bis Dezember 2012 unter anderem mit dem Bereich Jugendmedienschutz."

Technical approaches for the detection of criminal activities in online environments

Prof. Dr.-Ing. habil. Ulrike Lucke

Abstract

This article is focused on the discussion on Cyber-Grooming from a technical perspective. After a short introduction to the phenomenon and its societal significance, relevant online environments are presented. Moreover, the activities to be recognized in such worlds are discussed in more detail, and targeted approaches for their detection are presented. In the following, a methodology to automatically detect suspicious activities ─ based on current mechanisms from computer science ─ is proposed. The article concludes with a summary of possible countermeasures for Cyber-Grooming, including the prerequisites, outcomes, and limitations of technical detection mechanisms.

1. Which problem do we address?

The EU has explicitly admitted to making the Internet a safer place for kids and minors [8]. From a technical point of view, the discussion in the EU on protecting children is finally focused on the question to just block or completely delete harmful websites. This is not targeted to current online environments (like virtual worlds, browser games, or online apps), but is stuck to an out-dated content-oriented (not: communication-oriented) view on classic Web pages with text, images, audio, or video.

Moreover, those static Web pages are not in the primary focus of minor users. Kids primarily explore the internet by starting to play games, not by surfing the Web [16]. Those online environments are especially attractive because of their possibilities to interact and communicate with other players (like shared game experience, chats, etc. to find and maintain friendship). There are certain offers in the Internet with a design and game mechanism that is particularly suitable for children, where they are especially exposed to enter close emotional relationships with others. Besides other legal issues, this is intensively exploited by pedo-criminals in a targeted manner [3]. Such initiations of sexual interactions with minors are called Cyber-Grooming [5][15].

Kids primarily explore the internet by starting to play games, not by surfing the Web.

This important, but not yet sufficiently covered topic was primarily addressed by the symposium “Protection of Children and Minors in the Internet – Perils of Virtual Worlds” on 19 September 2012 in Brussels [9]. Starting from a criminological overview of the phenomenon, aspects of law, society and IT for protecting kids and minors against Cyber-Grooming have been considered by respective experts, and first experiences with virtual police offices in an online game for kids have been presented. In the following, the political consequences have been discussed with representatives of EU commission and parliament. All participants agreed that the Internet is an important part of today’s media reality, and that providing related skills as well as an adequate protection of minors are a central goal of our efforts.

As a result, there were identified shortcomings of law, investigation, prosecution, and prevention; and a first catalog of possible countermeasures was gathered. Among others, a new age rating

Moreover, the development of technical means to detect and block suspicious activities in online environments were discussed, which need to be balanced between safety and privacy.

(age levels, criteria, and responsibilities), an adequate media-related instruction of kids as well as training of other involved players (teachers, police men, state attorneys, system providers), and a general sensitizing of the society for the perils of interaction and communication in the Internet were proposed. Moreover, the development of technical means to detect and block suspicious activities in online environments were discussed, which need to be balanced between safety and privacy. Further efforts to elaborate and implement the mechanisms mentioned above will follow in the near future.

This article presents a more detailed view on technical issues of how to detect and prevent criminal activities like Cyber-Grooming. In section 2, a short overview on covered systems is provided. Section 3 gives an impression of activities in those environments that can be automatically monitored. Section 4 presents some current mechanisms that can be facilitated to implement this, as well as an overall system architecture to realize detection and blocking of suspect activities. Finally, section 5 draws a conclusion of technical possibilities and necessary work.

2. Which platforms do we need to consider?

Public discussion on cases of Cyber-Grooming was mainly focused on specific platforms like Habbo Hotel[1] or Freggers[2]. They are explicitly designed for and offered to children. This comes along not only with special topics, stories, and designs, but also with simplified registration and authentication procedures that make it hard to lock out unwanted users.

In general, such online environments can be characterized as follows:

- Virtual worlds provide a more or less realistic copy of the real world, including places and typical activities to be carried out. Prominent examples are Second Life[3] (mainly targeted to adults), Habbo Hotel[1] (targeted to kids aged 12 to 18) or Panfu[4] (no age classification). They are accessed via browser interfaces or dedicated client software; the world models and interactions are buried on a central server. Virtual worlds do not offer a dedicated story or goal to their users, but are focused on the imitation of real-life activities and relationships. Users are present by means of their avatars, which are often far more different to their real-world counterpart than the world itself is. This opens up several possibilities for social interactions beyond traditional borders of ethnics, religion, age, or gender. This is of certain benefit for inclusion in settings like online learning [6], but can also be exploited by pedo-criminals to establish illegal contact with minors [5].
- Online games are associated with a specific story line, often based on a complex background philosophy, which requires the user to fulfill certain tasks or quests in order to reach a higher goal or level. Prominent examples are World of Warcraft[5] (scope: adventure, targeted to adults) or Oloko[6] (scope: farming, targeted to kids aged 6 to 12). Online games can also be played in the browser window or using dedicated client software; as in virtual worlds, the modeling and simulation of objects, avatars and interactions is realized on a central server. Because of the fictitious nature of a game, avatars are usually designed with lots of fantasy, hiding the real-life person behind it. While gameplay itself is headed towards a

1 http://www.habbo.com/

2 http://www.freggers.com/

3 https://secondlife.com/

4 http://www.panfu.com/

5 http://eu.blizzard.com/en-gb/games/wow/

6 http://www.oloko.com/

pre-defined goal (and therefore activities are usually restricted to this storyline), some platforms offer mechanisms for free interaction between users following a shared game experience. Again, this can be used for establishing unwanted or illegal contact between players [15].

- Mobile apps are a category which can be seen as orthogonal to the previous ones. Today, several platforms are extended by a mobile component for access via smartphones or tablet PCs. This includes both, virtual world simulations as well as game-based approaches. Moreover, some apps do not require an internet connection. Thus, they are not vulnerable to mis-use of communication features. Prominent examples are Nighty Night[7] (scope: animal care, targeted to kids ages 1 to 4) or WordFeud[8] (scope: word puzzle, targeted to player aged 10 or higher). Mobile access simplifies connection to the online environment and strengthens the relationship between the users and his/her digital self. As in above categories, apps can include traditional forms of communication and content dissemination, like chats or forums.

Platforms as described above are attractive to large amounts of users, because they are apparently different to the real world and allow them to escape from their everyday routine or the problems of adolescence. Moreover, they offer some kind of persistency that allows them to create an authentic experience for a high degree of immersion.

From the providers' perspective, attracting users is crucial for financial success. However, there are different business models. Some products require payment to enter the system, either for getting the software (e.g. app download) or as a monthly fee. This hurdle is often avoided for solutions targeting kids, since payment can usually not be realized without knowledge of resp. support by parents. Other products are free to use, but players have to pay for advanced features like weapons, furniture, pets, or food. This payment model may expose kids to financial dependency from other players, e.g. when they got a virtual pet as a gift and don't have means to feed it [20].

This payment model may expose kids to financial dependency from other players, e.g. when they got a virtual pet as a gift and don't have means to feed it [20].

Considering these types and characteristics of online environments, technical mechanisms for monitoring of suspicious activities are restricted to server-based approaches for two reasons. First, stand-alone tools[9] do not support communication with other users and thus are not prone to mis-use for Cyber-Grooming. Second, governmental surveillance should keep away from private property and data of citizens (including their computers and software) [19], while commercial providers may be subject to regulation (e.g. for certification as a child-safe environment) and thus may be forced to install monitoring tools [22].

3. Which activities do we need to monitor?

This section provides a more detailed analysis of activities in online environments that should be subject of monitoring. The focus is on issues that allow for an automated detection. This implies that there may be other events or content elements that would not be rated as harmful by technical solutions, but should be from a more general perspective. That's why

7 http://www.goodbeans.com/products/nighty-night

8 http://wordfeud.com/

9 Theoretically, there is the third category of peer-to-peer applications, which is unequally harder to monitor. Those applications do neither rely on a central server nor do they reside on an single client, but they rather evolve from redundant, bilateral connections between nodes (clients) in a network. This architecture is well known from file sharing applications. However, there was not yet a case reported on illegal contact with children using such an approach.

accompanying approaches like virtual police officers in online worlds should be followed, additionally [13]. Moreover, automated detection implies a risk to find a supposed hit where no criminal or dangerous behavior took place. For this reason, technology can always just help to detect, to supply evidence, and to quickly react in questionable situations. However, technology can never judge on people. Personal rights, ethics and privacy are above any rating supposed by technology [10], and should be carefully considered during the design of a reporting system.

3.1 Text

The approach of using games theory addresses the inherent problem of predator and prey: Every action on one side causes the other party to adjust its strategy.

The most easy-to-monitor category of content elements is written or spoken language. (Spoken language can be translated into written text on-the-fly by voice recognition techniques [1]. Such systems have proven their maturity e.g. in telephony, in current game consoles and smartphones, or for supporting people with disabilities. Thus, spoken text can be automatically analyzed using the same methods as for written text.) If provided in written form, text can be searched for predefined patterns or any other irregularities that are used to classify if it contains unwanted content.

In general, an algorithm to monitor text messages and to rate them according to given threats [21] looks as follows:

1. if necessary, speech / character recognition
2. detection of bad words (and circumscriptions)
3. calculation of proximity measures
4. classification of message

The accuracy of results is determined by two variables, which come into play in steps 2 and 3 of this algorithm. First, the list of bad (i.e. unwanted) words needs to be defined, manually. This includes circumscriptions of these words (e.g. using so called ASCII art or wildcards) used by creative senders, e.g. "s3x" or "s_x" for the word "sex" [20]. That's why emphasis should be put on management of those lists of bad words, e.g. using community approaches (providers and/or users that mutually exchange new bad words). Second, the validity of used proximity measures has a strong impact on the accuracy (average ratio of false positives and false negatives compared to the whole amount of text) of an algorithm. Here, the combination of several independent characteristics can be used to increase the overall accuracy.

Available mechanisms for e-mail spam detection demonstrate that such mechanisms work well for specific areas of application. However, there is some ongoing research on this topic that might be of interest for the detection of Cyber-Grooming attempts, as well. The approach of using games theory addresses the inherent problem of predator and prey: Every action on one side causes the other party to adjust its strategy. This can be facilitated for innovative detection mechanisms to breakthrough this loop [4]. Another approach is to use ontologies in order to recognize semantics behind a text. This can help to detect if somebody is obviously not speaking about what's the primary meaning of his words, i.e. if there is an inconsistency in his message [7].

There are some alternatives to automated text classification that should be considered. If all communication (e.g. chat) is moderated by a human supervisor, sending of each message requires approval. This is realized for common office hours in some games like Panfu. Another option is to allow only pre-defined text blocks for messages, which should work for limited scenarios like sending friendship requests and status updates. Both mechanisms can be combined, e.g. only pre-defined text blocks as long as chat is not moderated. However, these mechanisms make sense only in small user groups, and they require the provider to pay some additional effort.

3.2 Graphics

While textual content is comparatively easy to analyze, visual information is harder to classify. This includes static images as well as dynamic media objects like animations or videos. Again, the latter, more complex types can be reduced to single, static scenes (so called frames) for analysis. This may not be necessary for every single frame, since modern video encryption is typically based on a number of intermediate frames containing only partial information derived from previous or following frames [14]. Thus, for reasons of performance video analysis may be restricted to so called i-frames containing complete scenes (e.g. one per 0,5 seconds in MPEG-1 and -2 videos, one per 10 seconds in MPEG-4 videos) without loss of precision.

As for textual content, a general algorithm for analyzing visual content may look as follows:

1. comparison with rated content
2. calculation of similarity measures
3. classification of image
4. if necessary, repeat this for single frames

Again, the quality of results is determined by two aspects. First, the specificity of predefined images has a strong impact. A database of very typical images of unwanted content is required. Second, calculation of similarities between these images and the current content object is crucial. Objects may vary in size, color, direction, perspective, etc. – that's why several possible operations for transforming visual content (like scale, rotate, skew, distort, dye, shade, etc.) have to be applied and combined in order to test if any similarity to previously rated content can be created. The accuracy of results increases with the amount of rated content to compare, and with the complexity of comparisons to be carried out. However, the available time for processing is limited by the given ratio of frames to analyze, so a trade-off is necessary. Currently, a lot of research on visual computing is done, so new and improved algorithms will be available in the future [18]. Anyway, porn blockers have proven that these mechanisms can already work quite well.

Besides analyzing the content represented by an image or video, more simple (yet effective) means can be applied to the names and locations of these objects. For example, the name of a file may in some cases give a hint on its content, and it is much easier to analyze using the approaches presented in the previous section. Moreover, sites that are known to deliver un-wanted content can be handled in a similar manner, like successfully exploited for email spam detection (so called black or grey lists of hosts under suspect). Images or videos may only be subject of enhanced visual analysis if they successfully passed these simple tests.

While textual content is comparatively easy to analyze, visual information is harder to classify. This includes static images as well as dynamic media objects like animations or videos.

There are some alternatives to automated verification of visual media, as for textual content. First, upload or linking of graphics may require approval by a moderator. Second, users can be forced to use predefined image libraries that are restricted to "safe" content. Again, a combination of these approached is possible, e.g. beyond office hours the use of individual content may be prohibited.

3.3 Complex activities

The most complex types of activities to be detected are those consisting of individually un-suspicious elements that unfold their risk potential only in its entirety. Unfortunately, this corresponds to the most dangerous type of Cyber-Groomers who's patiently establishing a personal relationship to his later victim [20]. Thus, stream-based detection mechanisms as described above cannot help here. Rather, data on all interactions between users has to be logged in order to have it available for later analysis – a very critical approach in terms of privacy.

Obviously, it is not feasible to continuously transmit data on all activities of all users in all virtual worlds to a central law enforcement agency, even if limitations of national law were resolved. Besides respecting private interactions between users, the pure amount of incurring data will forbid this approach. Several means may help to cope with these problems:

- Suspicious activities follow typical patterns. This may be to send similar messages to a number of other users in short time, to repeatedly send messages to the same person by using different accounts, or to unilaterally finance the virtual belongings of another user. Not all aspects of interactions need to be logged, but only the elements of those patterns.
- For detection of those patterns, it is not necessary to know the exact identities of related users, but just to differentiate between several accounts and user classifications like age-range and gender. Thus, identities of users can be hidden by assigning pseudonyms[10] which can be resolved only by the providers of virtual worlds. This can be compared to masking the origin of a computer by an IP address, which can be resolved by the responsible internet provider.
- Finally, information on users and their interaction should remain inside the platform of the provider as long as possible in order to avoid misuse. Accumulated reports can be transmitted to law enforcement agencies, which in turn can request to fully log data on relevant users and their interactions in order to collect evidence.

Thus, identities of users can be hidden by assigning pseudonyms which can be resolved only by the providers of virtual worlds.

However, this requires the discovery of typical activity patterns of Cyber-Groomers as well as their formal description.

Additionally, established community mechanisms like report-buttons for users can help to collect relevant information. Users can provide hints on suspicious behavior with just a few clicks. This creates valuable data for automated detection mechanisms, since preceding activities can act as training data, too.

3.4 Putting it all together

The combination of all methods described above leads to a multi-level approach for the detection of suspicious online activities. The following diagram provides a graphical representation of these mechanisms, using the notation of a process model. Logging all communications and item-based interactions, as well as analyzing communications are parallel processes, accompanied by optional human moderators and virtual policemen. Please note that the focus of the presented process model is on monitoring tasks, i.e. common activities of users or providers of online environments are displayed only as long as they are relevant for the detection of suspicious activities.

10 Please note that users of online environments typically act under a user name, so later assignment of pseudonyms to these user names is yet a second step to hide their identity.

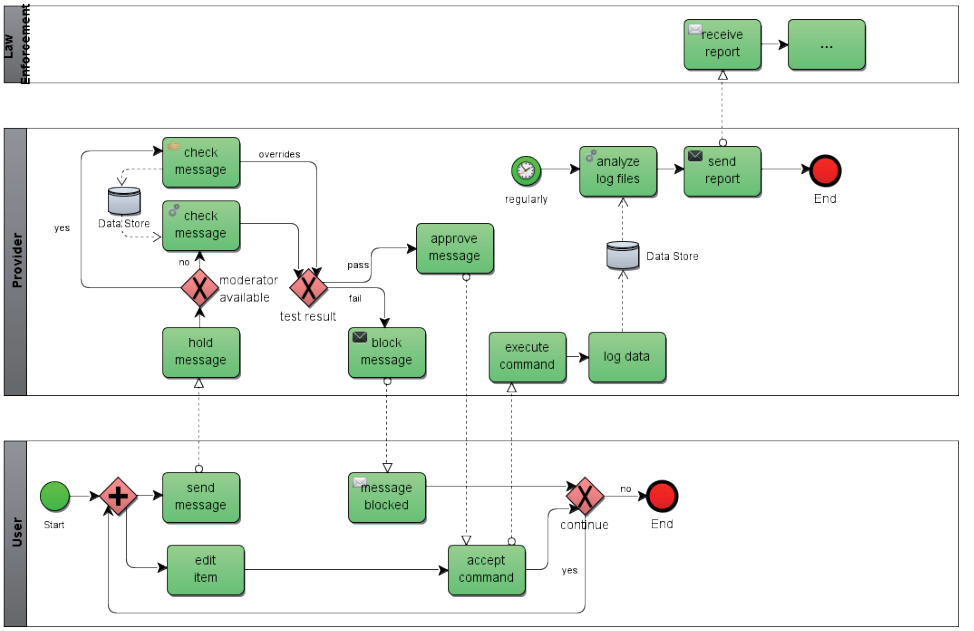

Figure 1 Communication between users can be subject of continuous monitoring. Moreover, all interactions can be logged and analyzed regarding suspicious activity patterns.

The process of automatically checking a message (including textual and visual content) is now explained in more detail in the following diagram.

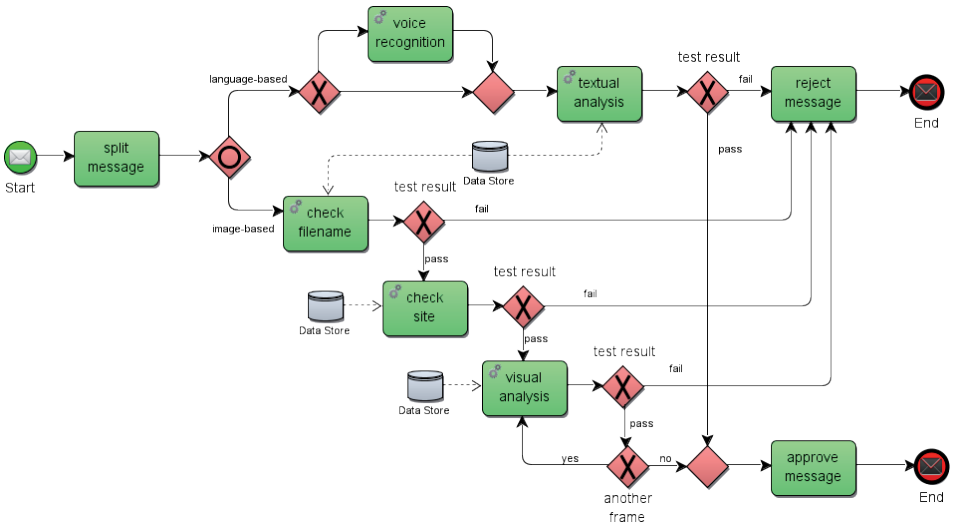

Figure 2 A message is split into textual and visual components, which are subsequently analyzed. Finally, a message will pass or fail these tests.

Up to now, the description of algorithms to analyze textual or visual content elements was rather vague. The next section provides in introduction to technical possibilities for this analysis.

4. Which mechanisms can we use for detection?

The description of image analysis revealed that a tradeoff between performance and accuracy of detection algorithms may become necessary, given the limited time for analyzing and rating messages in a stream. Moreover, technology asks for another tradeoff between accuracy and transparency, since transparent detection algorithms (i.e. those who come along with a reason for their rating) tend to be rather error-prone, and vice-versa. The next two sections present relevant approaches at either ends of this scale, followed by a third section describing a system architecture that integrates such algorithms and tools into a complete framework.

For the field of Cyber-Grooming, extensive empirical studies will be necessary in order to make pattern of offenders and victims explicit, before automated detection based on such rules can be applied.

4.1 Rule sets

Rule-based systems are a well-studied approach to make knowledge of human experts explicit and interpretable by automated processing. Such an expert system defines a set of conditions on how to handle incoming data [12]. For this purpose, it consists of two kinds of machine-readable information:

- A knowledge base contains a set of information that was proven to be true.
- An interference engine describes a set of operations how this knowledge as well as incoming data can be transformed.

The expert system tries to infer new statements from this basis, with the final goal to conclude with a statement on approval or rejection of the message to be classified.

The benefits of such a solution are that every decision (in our case: on approval or rejection of a message to be classified as suspicious or not) can be justified in terms of the rules that have been applied. Moreover, there is experience from several application fields that are dealing with rule-based systems for several years.

However, there are some weak points. First of all, the success of this approach depends on the precision and completeness of given rules. This requires explicit modeling of knowledge in the respective field, which is a challenge where empirical data is still missing or not yet valid enough. For the field of Cyber-Grooming, extensive empirical studies will be necessary in order to make pattern of offenders and victims explicit, before automated detection based on such rules can be applied. Finally, complex rule sets make high demands on processing power. Current research on answer set programming [11] will help to tackle this problem.

These pro's and con's make rule-based systems more appropriate for textual analysis in the detection process described above.

4.2 Artificial neural networks

At the contrasting end of the scale, a well-known computational approach inspired by nature is available. Artificial neural networks imitate the structure and behavior of a brain in order to make a decision [2]. A number of switching elements (neurons) are arranged in a multi-layered architecture. They are connected with some preceding and subsequent switches following a given topology. Each connection is associated with a certain weight in order to strengthen or weaken the transmitted signal. Moreover, every switch has its own scheme to derive an output signal from the set of incoming signals. The overall output is calculated by the switches in the last layer. A network functions as follows:

- In an introductory learning phase, the artificial neural network is confronted with training data and the desired results of processing. The switching elements adjust the weights along their interconnections as well as their internal calculation schemes.
- In the working phase, the network can be confronted with new data that has to be classified.

Such an approach can be applied even to complex data or problems, since there is no direct equivalent of the problem description in the structure of the system. Thus, no explicit definition of rules is required, and the network (as well as processing time) will not necessarily grow with the complexity of the problem. Provided that a sufficient set of training data is available, proper functioning of the network can be established without expert knowledge. All calculations are available within few computational steps necessary for propagating the input data through the neural network structure.

At the other hand, the success of this approach heavily depends on the quality of training data and the training process. Thus, empirical data is required to some extent also for this approach. The main drawback of neural networks is that they do not provide any justification for their decisions. Thus, they can be used to prepare a recommendation or to generate short-term warnings, but not to create or collect evidence.

These pro's and con's make artificial neural networks more appropriate for visual analysis in the detection process described above.

4.3 Detection architecture

Following the discussions on how to analyze different types of content, how to handle private data, and how to integrate into the existing hardware / software structure of online environments, the following system architecture is proposed.

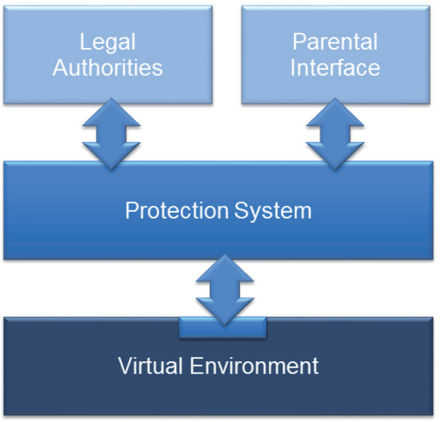

Figure 3 The proposed system architecture decouples police work and law enforcement from technological issues of single online worlds, while keeping privacy of users. Additional benefit is provided for parents to monitor their kids' online activities.

Besides technical issues on where to handle which types of data, this layered architecture provides a strong benefit in decoupling legal authorities from system providers. Officials from police, law enforcement, etc. do no longer need to tightly keep pace with technological progress. Rather, they can focus on monitoring, analyzing, and tracking criminal behavior. A dedicated interface allows them to enter new case descriptions (i.e. patterns derived from their investigations) that are used to analyze upcoming activities in several online environments, independently from their technical connection.

On the other side of the system, interfaces to providers are established in order to integrate different online environments into the monitoring system. Currently, engagement like this is voluntary and very limited. Legal initiatives should force providers of online environments to integrate a plug-in of the monitoring system into their services in order to get a certificate as a child-safe place.

Officials from police, law enforcement, etc. do no longer need to tightly keep pace with technological progress. Rather, they can focus on monitoring, analyzing, and tracking criminal behavior.

Another feature of the proposed system is an optional parental interface. Here, parents can get some possibilities to request reports on the activities of their kids. Of course, privacy should be considered, i.e. reports should be accumulated, and detailed information on dedicated activities should be given only in case of severe warnings.

Another added value from the cooperation of these parties is to integrate automated mechanisms for learning by feedback. Such an additional input can be decisions on messages by moderators, assessment of complex situations by law enforcement, and others more. Automated detection mechanisms must be able to improve their capabilities, as human supervisors would do. Such mechanisms of machine learning are subject of current research [17].

It should be noticed that the generic approach described here is not specific to Cyber-Grooming, but can be transferred to several fields of crime, like economics, terrorism, sedition, and so on.

Another issue that technology cannot solve is to reason about the goal of a user. Does he/she act with criminal intent? Questions like these will always require human judgement.

5. Conclusion

Computer science provides several means to automatically monitor and assess user activities in online environments. This article presented a rough overview, but further work is necessary to implemented the presented concept and mechanisms.

5.1 What we need

A basic requirement for all approaches presented above is the availability of observable behavioral patterns of offenders and victims with related probabilities of a criminal suspect. This must be specific for certain criminal activities as well as for certain national law. Thus, sophisticated empirical research in criminology (in relation to sociology and/or psychology) is necessary.

Another condition for successful realization of the solution presented above is the availability of interfaces to virtual environments, where plug-ins to the monitoring system can be entered. Since providers will not have intrinsic motivation to provide such interfaces, public pressure or regulations by law may force them to actively participate in protection of minor users.

5.2 What we can provide

As soon as detection mechanisms are installed, they can provide alerts on suspicious activities. They can be presented directly to player, but also to their parents, to providers of online environments, as well as to law enforcement.

Moreover, a monitoring system can help to collect evidence in case of a suspect or later trial. This can be information on the date, time and (virtual) place of an activity, on the person(s) involved, as well as on details on these activities. Given an official criminal investigation, these data can be forwarded from providers to law enforcement.

5.3 What we cannot detect

Independently of the technical implementation and surrounding conditions, there are some aspects that technology can hardly (if at all) provide. One of these is identity: Is a user the one he/she claims to be? The internet is based on the virtualization of identities. While biometrical data is reliable in local settings, digital transmission of identifying information is prone to manipulation. This is even harder is case of minor users. There are some mechanisms (like post-ident) to ensure that a user is above a certain age, e.g. for adult offers. These solutions are not capable to ensure that a user is below a certain age, since children typically to not have identifying documents. At least, their identity can easily be stolen by related persons. Another issue that technology cannot solve is to reason about the goal of a user. Does he/she act with criminal intent? Questions like these will always require human judgement.

References

M. A. Anusuya, S. K. Katti: „Speech Recognition by Machine, A Review", Int. Journal of Computer Science and Information Security (IJCSIS) 06/03, Dezember 2009, S. 181-205.

C.M. Bishop: "Neural Networks for Pattern Recognition", Oxford: Oxford University Press, 1995.

S. W. Brenner: "Is There Such a Thing as 'Virtual Crime'?", 4th California Criminal Law Review, 2001, pp. 105-11.

M. Brückner, C. Kanzow, T. Scheffer: „Static Prediction Games for Adversarial Learning Problems", Journal of Machine Learning Research (JMLR), Vol. 13, 2012, S. 2617-2654.

K.-K. R. Choo: "Online child grooming. A literature review on the misuse of social networking sites for grooming children for sexual offences", Australian Institute of Criminology, 2009.

F. Collins, D. McCormick: "Digital Selves: Lessons from Second Life", in Proc. World Conf. on Educational Multimedia, Hypermedia and Telecommunications (Ed-Media) 2011, S. 3405-3411, Chesapeake, VA, USA : AACE, 2011.

X. Deng, V. Haarslev, N. Shiri: "Measuring Inconsistencies in Ontologies", in Proc. 4th Europ. Conf. on The Semantic Web: Research and Applications (ESWC '07), Berlin : Springer, 2007, S. 326-340.

Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Official Journal of the European Union, L 335/1, 17.12.2011.

G. Ehrmann, U. Lucke, M. Mulder, T.-G. Rüdiger, T. Schulz-Spirohn, J. Storbeck, D. Woidke: "Protecting Children and Minors in the Internet: Perils of Cyber-Grooming in Virtual Worlds", Position Paper, October 2012. http://apache.cs.uni-potsdam.de/de/profs/ifi/mm/positionpaper-CyberGrooming-EN.pdf

European Convention on Human Rights, ETS 5; 213 UNTS 221, Rome, 4 November 1950.

M. Gelfond: «Answer sets», in: "Handbook of Knowledge Representation", Elsevier, 2008, pp. 285-316.

A. Gupta, C. Forgy, A. Newell, and R. Wedig: "Parallel algorithms and architectures for rule-based systems", SIGARCH Comput. Archit. News, Vol. 14, No. 2, May 1986, pp. 28-37.

S. Jacobsen, M. Mulder: „Dutch police, vision on youth and internet", in this issue.

R. Koenen (Ed.): "Coding of Moving Pictures and Audio", ISO/IEC JTC1/SC29/WG11, Moving Picture Experts Group, März 2002.

C. Krebs, T. Rüdiger: „Gamecrime und Metacrime: Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Welten", Verlag für Polizeiwissenschaft, Dezember 2010.

S. Livingstone, L. Haddon, A. Görzig, K. Ólafsson: „EU Kids Online", Final Project Report, 2011.

M. Mohri, A. Rostamizadeh, A. Talwalkar: "Foundations of machine learning", Cambridge, MA : MIT Press, 2012.

T. Morris: "Computer Vision and Image Processing", Palgrave Macmillan, 2004.

Andreas Pfitzmann: „Contra Online-Durchsuchung", Informatik Spektrum 31/01, Februar 2008, S. 65-69.

T.-G. Rüdiger: „Sexualtäter in virtuellen Welten", in this issue.

N. Spirin, J. Han: "Survey on Web Spam Detection: Principles and Algorithms", ACM Explorations on Knowledge Discovery and Data Mining (KDD) 13/02, 2011, S. 50-64.

Jörg Ziercke: „Pro Online-Durchsuchung", Informatik Spektrum 31/01, Februar 2008, S. 62-64.

About the author

Ulrike Lucke is Professor of Computer Science and head of the Complex Multimedia Application Architectures group at the University of Potsdam. Her areas of research are heterogeneity and interoperability of network-based architectures, including aspects of mobile and pervasive computing, especially in the field of E-Learning. Moreover, she is Chief Information Officer (CIO) of the University of Potsdam and thus responsible for strategic IT issues.

Kinder- und Jugendschutz im Netz: Gefahren des Cyber-Grooming in virtuellen Welten

Georg Ehrmann, Deutsche Kinderhilfe e.V.
Ulrike Lucke, Universität Potsdam
Manuel Mulder, Polizei der Niederlande
Thomas-Gabriel Rüdiger, FH der Polizei Brandenburg
Thomas Schulz-Spirohn, Staatsanwaltschaft Berlin
Jürgen Storbeck, ehem. Leiter Europol
Dietmar Woidke, Brandenburgischer Innenminister

Die EU hat sich ausdrücklich zum Schutz von Kindern und Jugendlichen im Internet bekannt[1]. Die Diskussionen zum Kinderschutz sind in der EU jedoch letztlich fokussiert auf die Frage, ob gefährliche Webseiten nur gesperrt oder komplett gelöscht werden sollen. Dies ist nicht zielführend in Online-Umgebungen (wie virtuellen Welten, Browser-basierten Spielen oder Online-Apps), sondern einer veralteten, inhalts-orientierten (nicht: kommunikations-orientierten) Sichtweise verhaftet. Annähernd jedes Kind beginnt das Internet durch Online-Spiele für sich zu entdecken[2]. Diese Online-Umgebungen werden insbesondere durch die Interaktion und Kommunikation mit anderen Spielern (z.B. gemeinsame Spielerlebnisse, Chats) attraktiv. Hier gibt es spezielle Angebote mit kindgerechtem Design und Spielemechanismus, in denen Minderjährige besonders leicht emotionale Bindungen zu anderen Spielern eingehen. Dies wird von Pädokriminellen gezielt ausgenutzt[3]. Eine derartige Anbahnung von sexuellen Interaktionen mit Kindern und Jugendlichen wird als Cyber-Grooming bezeichnet[4].

Diesem wichtigen und bislang nicht hinreichend beachteten Thema widmete sich erstmals die Veranstaltung „Protection of Children and Minors in the Internet – Perils of Virtual Worlds“ am 19. September 2012 in Brüssel. Ausgehend von einem kriminologischen Abriss des Phänomens wurden juristische, gesellschaftliche und technische Aspekte des Schutzes von Kinder und Jugendlichen vor Cyber-Grooming von Fachexperten erörtert sowie erste Praxiserfahrungen mit virtuellen Polizeiwachen in einem Online-Kinderspiel präsentiert. Der politische Rahmen wurde anschließend mit Vertretern von EU-Kommission und -Parlament diskutiert. Alle Beteiligten stimmten darin überein, dass das Internet ein wichtiger Bestandteil der heutigen Medienrealität ist und daher die Vermittlung von Medienkompetenz und der Schutz von Minderjährigen ein zentrales Anliegen darstellen.

Im Ergebnis wurden Mängel an Gesetzgebung, Aufdeckung, Strafverfolgung und

1 Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates. Amtsblatt der Europäischen Union, L 335/1, 17.12.2011.

2 S. Livingstone, L. Haddon, A. Görzig, K. Ólafsson: „EU Kids Online“, Final Project Report, 2011.

3 C. Krebs, T. Rüdiger: „Gamecrime und Metacrime: Strafrechtlich relevante Handlungen im Zusammenhang mit virtuellen Welten“, Verlag für Polizeiwissenschaft, Dezember 2010.

4 M. Arnsperger: „Cyber Grooming im Chat: Gefährliche Anmache im Internet“, stern, Dezember 2008.

Prävention aufgezeigt sowie ein erster Katalog möglicher Gegenmaßnahmen erarbeitet. Als nötig wurden u.a. angeregt: eine überarbeitete Alterseinstufung von Online-Spielen (Altersstufen, Kriterien und Verantwortliche), eine adäquate Medienerziehung von Kindern bzw. Schulung von allen anderen Beteiligten (Erzieher/Lehrer, Polizisten und Staatsanwälte, Betreiber) sowie eine generelle Sensibilisierung der Gesellschaft für die Interaktions- und Kommunikationsrisiken des Internet. Zudem wurde die Einrichtung technischer Erkennungs- und Sperrmechanismen in Online-Umgebungen diskutiert, die sich im Spannungsfeld zwischen Sicherheit und Datenschutz bewegen. Weitere Aktivitäten zur Ausarbeitung und Umsetzung der vorgeschlagenen Maßnahmen werden folgen.

Impressum

Herausgeber: Rainer Grieger,
Präsident der Fachhochschule der Polizei des Landes Brandenburg

Redaktionelle und inhaltliche Gestaltung: Thomas-Gabriel Rüdiger, M.A.

Fachhochschule der Polizei des Landes Brandenburg,
Bernauer Straße 146, 16515 Oranienburg
Tel. 03301-850-2501
Fax 03301-850-2509
E-Mail fachhochschule@polizei.brandenburg.de

ISSN 1865-1062

Druck: Fachhochschule der Polizei des Landes Brandenburg

Redaktionsschluss: 30. April 2013