5 Jahre Kampf gegen Internet-Kriminalität

naiin Tätigkeitsbericht

(2000-2005)

Grußwort

Sehr geehrte Leserin, sehr geehrter Leser,

das Internet ist das Medium der globalen Kommunikation – ein Medium der grenzüberschreitenden Völkerverständigung. Dank der beständigen technischen Weiterentwicklung in der IT und der Telekommunikation wurde es in den vergangenen Jahren zu einem festen Bestandteil unserer heutigen Gesellschaft und der wirtschaftlichen Prozesse. Kein Wunder, dass es daher in zunehmendem Maße auch ins Visier Krimineller – Extremisten, Kinderpornografen, Betrüger geraten ist.

Als ich vor nun mehr fünf Jahren darum gebeten wurde, die Schirmherrschaft einer Initiative aus Wirtschaft, Politik und Gesellschaft zu übernehmen, die sich eben diesem Problem mit der Internet-Kriminalität annehmen sollte, wusste ich, dass wir mit diesem Anliegen Neuland betreten. Noch nie zuvor hatte sich eine Initiative mit dem Rückhalt aus allen Bereichen unseres gesellschaftlichen Zusammenlebens der umfassenden Bekämpfung von Internet-Kriminalität gewidmet.

So kann ich mich noch gut an die Euphorie der vielen Mitstreiter auf der Gründungsversammlung erinnern. Dieser Euphorie folgte in der Alltags-

arbeit schnell die Erkenntnis, dass die Bekämpfung von Internet-Kriminalität ein schweres Unterfangen sein wird. Unbeeindruckt dessen hat sich naiin in den vergangenen Jahren durch eine konsequente Arbeit und Fortentwicklung ihrer selbst, zu einer der schlagkräftigsten Einrichtungen gegen Cyber Crime entwickelt.

Einzigartig in ihren vielfältigen Maßnahmen, ihrer breiten Legitimation und ihren innovativen Ansätzen, ist es naiin gelungen Maßstäbe zu setzen. Ich freue mich daher besonders, dass die Initiative nun den Weg nach Europa beschreitet und ich bin mir sicher, dass sie – als grenzüberschreitende Initiative – auch auf dem gesamten Kontinent ihre Schlagkraft entfalten wird.

Für die Zukunft wünsche ich naiin noch mehr engagierte Unternehmen, die sich ihrer gesellschaftlichen Verantwortung bezüglich des Internets bewusst sind. Jeder, der vom weltweiten Datennetz profitiert – sei es wirtschaftlich, oder persönlich – sollte ein Interesse daran haben, dass dieses Medium nicht durch Kriminelle zweckentfremdet wird. Daher fordere ich an dieser Stelle alle wirtschaftlichen Kräfte, die im oder mit dem Internet arbeiten, dazu auf, sich unserem Anliegen anzuschließen.

Prof. Dr. Helmut Thoma
Schirmherr

Vorwort

Vor gut fünf Jahren hat sich die deutsche Internet-Wirtschaft mit Vertretern aus Politik und Gesellschaft an einen Tisch gesetzt, um ein Problem anzugehen, welches bis dahin noch nicht ins Blickfeld der Öffentlichkeit geraten war. Rechtsextremisten hatten strafbare Domain-Namen á la heil-hitler.de registriert und Pädokriminelle ihre Darstellungen von sexuell missbrauchten Kindern auf deutsche Server geladen.

Den Verantwortlichen in der deutschen Internet-Wirtschaft war der Gedanke fremd, die Infrastrukturen und Dienstleistungen ihrer Unternehmen für derartige kriminelle Machenschaften herzugeben. Sie reagierten prompt und gründeten im August 2000 die Initiative no abuse in internet (naiin). Der Auftrag von naiin war eindeutig: Bekämpfung von Internet-Kriminalität; Kampf dem Missbrauch im Internet.

Die Gründer von naiin haben schon frühzeitig die im Internet lauernden Gefahren erkannt und sich verantwortungsbewusst dazu bereit erklärt, diesen entgegen zu wirken. Nichts ahnend, dass die Zukunft noch weitere Arten von Kriminalität bereithält. Den Gründungstagen von naiin folgte die Wirtschaftskrise. Die dot.com-Blase platzte und naiin verlor einen Großteil seiner Mitglieder an den Insolvenzverwalter. Die Initiative

und ihre verbliebenen Mitstreiter ließen sich davon aber nicht entmutigen. Zu wichtig, war ihr Auftrag; zu erfolgreich, ihr Wirken.

Ich habe naiin als erster Vorsitzender durch diese von der Krise geprägten ersten Jahre begleitet. Es war nicht immer leicht, aber die konsequente Arbeit der engagierten Mitarbeiter und die beständige Weiterentwicklung ihrer selbst, hat es der Initiative und ihrem wichtigen Anliegen ermöglicht, die fragliche Zeit zu überdauern. Getreu dem Motto „Was einen nicht umbringt, macht einen stark" ist naiin gestärkt aus dieser Zeit herausgegangen. Die Initiative war den Kinderschuhen entwachsen und ihre Neuausrichtung Ende 2002 – kurz nach einer Auszeichnung durch die deutsche Bundesregierung – brachte die Wende.

Heute ist naiin eine Autorität im Kampf gegen das globale Cyber-Verbrechen, die größte Anlaufstelle für Internet-Nutzer, die sich mit den Gefahren im Netz konfrontiert sehen, und an Schlagkraft, Flexibilität sowie in der Einzigartigkeit ihrer Legitimation und ihren Maßnahmen nicht zu überbieten. Wie alle Unterstützer dieser Initiative bin ich froh ein Teil von naiin zu sein. Ich bin froh, zu wissen, dass es eine Einrichtung gibt, die die Werte, auf denen unsere Gesellschaft fußt – Werte wie Freiheit, Respekt, Verständigung, Miteinander und Menschlichkeit – im weltweiten Datennetz verteidigt.

Dieser Bericht wird Ihnen neben vielfältigen Informationen über naiin, auch einen Einblick in die Erfolge dieser Initiative gewähren. Überdies zeigt er die wichtigsten Entwicklungen in den einzelnen Kriminalitätsbereichen auf. Nach der Lektüre dieses Reports wird auch Ihnen bewusst

sein, dass es nicht zu unterschätzende Gefahren im Internet gibt. Dennoch sollten diese nicht darüber hinweg täuschen, dass das weltweite Datennetz ein „gutes" Medium ist und es sich lohnt, dieses Medium zu verteidigen!

Arthur Wetzel
Präsident

Inhaltsverzeichnis

1. Entstehung 11

2. Ziele 13

3. Arbeitsfelder & Maßnahmen 15

3.1. Information 15

3.2. Networking 16

3.3. Beschwerdestelle 17

3.4. Strategieentwicklung 17

3.5. Beratung 18

4. Organigramm 19

4.1. Standorte 20

5. Beschwerdestelle – netwatch 21

5.1. Vorgehen 21

5.2. Erfolg 22

5.3. Transparenz durch Live-Ticket-Verfahren 22

5.4. Erweiterung der Schwerpunkte 24

5.5. Problemstellung: Die Globalität des Internet 24

5.6. Indikator für künftige Entwicklungen … 25

5.7. Vorteile gegenüber Strafverfolgungsbehörden 26

5.8. Beschwerdestatistik 2000 – 2005 27

5.8.1. Beschwerden nach Kriminalitätsbereichen 28

6. Die relevantesten Kriminalitätsbereiche 29

6.1. Rechtsextremismus 29

6.1.1. Gemeinsam ist ihnen allen: Nationalismus und Hass 30

6.1.2. Server-Standort Deutschland 31

6.1.3. Entwicklungen 32

6.1.4. Tendenz 34
6.2. Linksextremismus 35
6.2.1. Linksextreme Publikationen: Digital statt Print! 35
6.2.2. Virtueller Kampf: Antifa vs. Nationaler Widerstand 36
6.2.3. Entwicklungen / Trends 37
6.3. Islamistischer Terrorismus 39
6.3.1. Al-Qaida-Drohungen via Internet 39
6.3.2. Islamisten im WWW: Ausbildung im Online-Lager 40
6.3.3. Entwicklungen / Trends 41
6.4. Kinderpornografie 43
6.4.1. Vorteile des Internet: Missbraucht durch Perverse 44
6.4.2. Die Tauschbörsen – Auch Kinderschänder kennen P2P! 44
6.4.3. Wonderworld: Chat im Zeichen der Kinderpornografie 46
6.4.4. Kindersexshops – Kindersex gegen Kreditkarte 48
6.4.5. Entwicklungen / Trends 50
6.5. Jugendschutz 51
6.5.1. Chats: Täglich werden Kinder sexuell genötigt 51
6.5.2. Auch „Kinder-Chats“ nicht sicher! 52
6.5.3. Entwicklungen / Trends 54
6.6. Internet-Piraterie 55
6.6.1. Tauschbörsen: Die Piraten in den p2p-Netzen 55
6.6.2. Organisierter Handel mit raubkopierten Filmen 56
6.6.3. Software-Diebstahl 58
6.6.4. Entwicklungen / Trends 58

1. Entstehung

Im August 2000 sah sich die deutsche Internet-Wirtschaft mit einem massiven Anstieg von Internet-Kriminalität konfrontiert. Die Registrierung der Domain heil-hitler.de bei der zentralen Registrierungsstelle für die deutsche Top Level Domain (TLD) „.de“, DENIC, war nur die Spitze des Eisberges. Schnell war klar: Das weltweite Datennetz findet nicht nur in rechtschaffenden Personen seine Anhänger, sondern übt auch auf Straftäter eine bis dahin ungeahnte Anziehungskraft aus.

Zum damaligen Zeitpunkt nutzten vor allem Rechtsextremisten und Pädokriminelle das Medium zur Verbreitung ihrer Propaganda beziehungsweise ihrer abscheulichen Bild- und Video-Dateien. Wie wir heute wissen, war dies erst der Anfang einer Entwicklung, die sich aufgrund der raschen Weiterentwicklung des Internets und der zunehmenden gesellschaftlichen Bedeutung des Mediums auch schnell auf andere Kriminalitätsbereiche ausdehnte.

Die Unternehmen der deutschen Internet-Wirtschaft erkannten bereits frühzeitig, dass ihre Dienstleistungen, Produkte und technische Infrastrukturen zur Verübung von Straftaten missbraucht werden. Um eben diesem Missbrauch entgegenzuwirken, gründeten sie zusammen mit Vertretern aus Politik und Gesellschaft am 18. August 2000 unter der Schirmherrschaft des ehemaligen RTL-Chefs, Prof. Dr. Helmut Thoma, die Initiative no abuse in internet (naiin).

naiin wurde in dem Bewusstsein geschaffen, dass die Bekämpfung von Internet-Kriminalität ein gesamtgesellschaftliches Engagement über die wirtschaftlichen Grenzen hinaus erfordert. Nur wenn alle politischen, wirtschaftlichen und gesellschaftlichen Kräfte zusammen mit den Strafverfolgungs- und Sicherheitsbehörden an einem Strang ziehen, kann es gelingen, dem Missbrauch des Mediums Einhalt zu gebieten.

2. Ziele

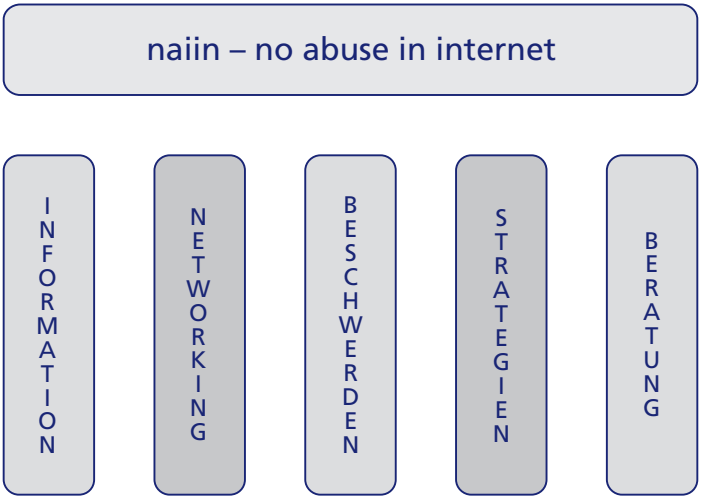
Das vorrangige Ziel von naiin ist die effektive und nachhaltige Bekämpfung von strafbaren Aktivitäten im Internet und damit die Erarbeitung entsprechender Gegenmaßnahmen.

Dabei versteht sich naiin als Selbstkontrolleinrichtung der gesamten Internet-Community. Denn nicht nur die Internet-Wirtschaft sollte sich für die Einhaltung gesellschaftlicher Regeln im Internet stark machen, sondern auch Gesellschaft und Politik sind gefordert, Eigenverantwortung im Umgang mit dem Medium zu zeigen.

Zugleich tritt die Initiative für die Verteidigung demokratischer Werte im weltweiten Datennetz ein – mit dem Ziel, es als freiheitliches Medium der Völkerverständigung zu erhalten. Zweck der Organisation ist darüber hinaus auch die Förderung der Kriminalprävention.

Die Umsetzung seiner Ziele verfolgt naiin mit Hilfe eines umfangreichen und breit gefächerten Maßnahmenbündels.

3. Arbeitsfelder & Maßnahmen



Die Tätigkeitsfelder von naiin sind vielseitig. Insgesamt fünf Pfeiler bilden das Fundament für die Arbeit der Organisation: Information, Networking, Beschwerdestelle, Entwicklung von Strategien und Beratung.

3.1. Information

naiin klärt durch öffentlichkeitswirksame Maßnahmen die Öffentlichkeit – vor allem Internet-Nutzer – über die missbräuchliche Nutzung des Internets auf. Ziel ist es, Internet-Nutzer für schädliche und illegale Inhalte zu sensibilisieren Und in die Lage zu versetzen, derartige Inhalte zu erkennen und zur Anzeige zu bringen.

Unter dem Gesichtspunkt des Jugendschutzes ist es notwendig im Rahmen der Öffentlichkeitsarbeit den Eltern minderjähriger Internet-User das notwendige Wissen (auch über Filtersoftware-Produkte) zu vermitteln, welches sie zwingend benötigen, um ihre Kinder vor jugendschutzrechtlich relevanten sowie rechtswidrigen Inhalten zu schützen.

Die Aufklärung der Öffentlichkeit erfolgt über die Presse-Arbeit, durch Informationen auf der Website, durch Newsletters, die an jeden Interessierten versendet werden, durch interne aber auch externe Initiativenübergreifende Arbeitsgruppen, Veranstaltungen, Vorträge und anderes.

3.2. Networking

naiin arbeitet mit Strafverfolgungs- und Sicherheitsbehörden sowie weiteren zuständigen Stellen auf urbaner, regionaler, nationaler und internationaler Ebene, auf das Internet spezialisierte Firmen und mit gleichgesinnten Initiativen, Institutionen und Organisationen zusammen, um effektive Maßnahmen zur Bekämpfung schädlicher und illegaler Inhalte zu erarbeiten und erfolgreich umzusetzen. Zugleich wird ein Informations- und Erfahrungsaustausch zwischen den gnannten Einrichtungen gewährleistet, von dem alle Beteiligten profitieren.

3.3. Beschwerdestelle

naiin betreibt seit November 2000 eine internationale Beschwerdestelle namens netwatch, bei der Internet-User schädliche und illegale Internet-Inhalte beanstanden können.

Beschwerden über derartige Inhalte können die Nutzer entweder über einen speziell ausgewiesenen Teil der Homepage via Formular oder direkt an netwatch@naiin.org der Beschwerdestelle der Initiative zukommen lassen.

Die beanstandeten Inhalte werden zunächst einer rechtlichen Prüfung unterzogen und falls notwendig werden Maßnahmen gegen diese ergriffen. Hierbei ist es naiin an einer intensiven Zusammenarbeit mit den jeweils zuständigen Strafverfolgungs- und Sicherheitsbehörden gelegen.

Es liegt im Interesse von naiin und wird von der Initiative angestrebt, Straftäter, die illegale Inhalte in das Internet einstellen, der Strafverfolgung und somit einer gerechten Strafe zuzuführen.

3.4. Strategieentwicklung

Auch die Entwicklung von Strategien unterschiedlichster Natur steht im Mittelpunkt der Arbeit von naiin. Anhand seiner Arbeit in den Bereichen Beschwerdestelle und als Ansprechpartner für die Internet-Nutzergemeinde greift naiin aktuelle Trends in der Internet-Kriminalität auf und versucht technische, gesellschaftliche und politische Gegenmaßnahmen zu entwickeln und umzusetzen.

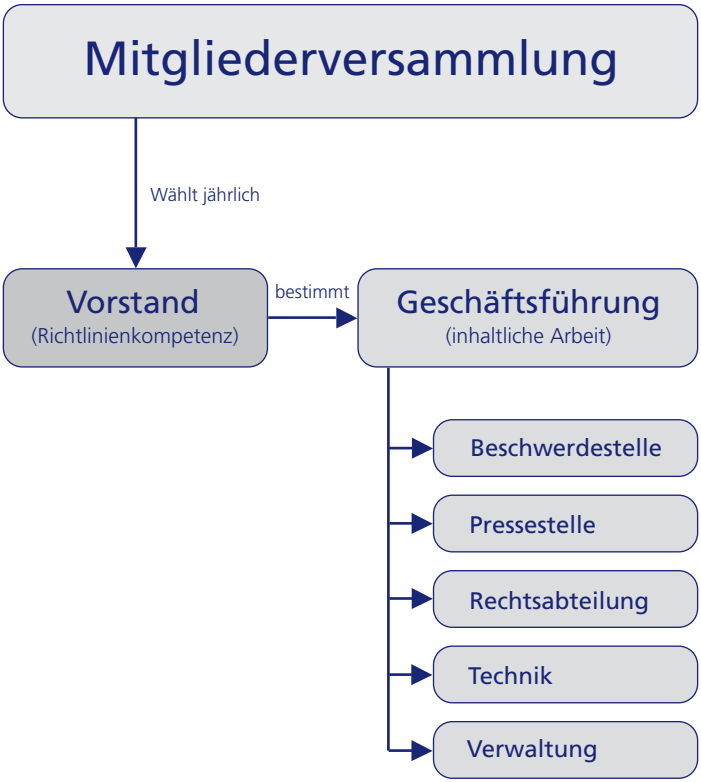
So mahnt naiin den Gesetzgeber zum Handeln auf; fordert beispielsweise die Verschärfung oder Einführung von Straftatbeständen. Weiterhin positioniert sich naiin zu politischen Vorhaben. Der Verein prüft diese und eruiert deren Erfolgsaussichten im Kampf gegen Cyber Crime. Dabei blickt naiin auch über die Ländergrenzen hinaus.

3.5. Beratung

naiin steht nicht nur seinen Mitgliedsunternehmen, sondern auch allen Internet-Nutzern mit Rat und Tat zur Seite. Täglich gehen zahlreiche Anfragen per Post, Fax, E-Mail und Telefon zum Themenbereich Internet-Kriminalität bei naiin ein. Ob Fragen zum Jugendschutz, zur IT-Sicherheit, zum Umgang mit illegalen Web-Inhalten oder konkreten Hinweisen auf Straftaten, die naiin-Fahnder sind mit einer Themenvielfalt konfrontiert wie kaum eine andere vergleichbare Initiative.

Darüber hinaus steht naiin auch seinen Mitgliedsunternehmen mit seinem Know-How in der Bekämpfung von Cyber Crime zur Seite. Die Initiative fungiert dabei als Schnittstelle zwischen der Internet-Wirtschaft und den Strafverfolgungsbehörden, durchforstet Unternehmensserver nach illegalem Content, unterstützt die Umsetzung von Sicherheitsmaßnahmen und schützt die Unternehmen vor dem Missbrauch ihrer Infrastrukturen durch kriminelle Nutzer.

4. Organigramm



Die Mitgliederversammlung bestimmt jährlich einen Vorstand, der ihre Interessen und naiin in der Öffentlichkeit vertritt. Bestehend aus einem 1. Vorsitzenden (Präsident), 2. Vorsitzenden (Vize-Präsident), Schatzmeister und Schriftführer leitet er die Geschicke des Vereins. Der Vorstand übt dabei die sogenannte Richtlinienkompetenz aus. Er bestimmt die Ziele der Organisation und entwickelt entsprechende Projektideen sowie

Strategien. Für die Umsetzung der Vorgaben sowie der gesamten inhaltlichen Arbeit von naiin zeichnet die Geschäftsführung verantwortlich. Sie wird vom Vorstand des Vereins ein- und abgesetzt.

Der Geschäftsführung unterstehen neben der Beschwerdestelle ein Pressereferat, eine Rechtsabteilung, die Verwaltung sowie technische Sachverständige.

4.1. Standorte

naiin verfügt allein in Deutschland über zwei Standorte. Während die Organe des Vereins – Vorstand, Mitgliederversammlung – in Berlin den Kontakt zur Bundespolitik aufrechterhalten, unterhält die Geschäftsstelle ihren Sitz nahe der Medienmetropole Köln.

Vor allem die Nähe zum EU-Machtzentrum Brüssel war ausschlaggebend für den Umzug des operativen Geschäfts ins Rheinland.

5. Beschwerdestelle – netwatch

Zur Bekämpfung illegaler Inhalte im Internet hat naiin als Institution der freiwilligen Selbstkontrolle im November 2000 die Internet-Beschwerdestelle „netwatch“ installiert. Via Formular oder E-Mail können Internet-Nutzer ihrer Meinung nach illegale Internet-Inhalte bei „netwatch“ beanstanden. Primäres Ziel der naiin-Beschwerdestelle ist es, durch effektive technische und rechtliche Maßnahmen rechtswidrige Inhalte im Internet zu eliminieren.

5.1. Vorgehen

Die durch Internet-Nutzer beanstandeten Inhalte werden zunächst einer rechtlichen Prüfung unterzogen. Als fester Maßstab zur Beurteilung der beanstandeten Inhalte dient in erster Linie das bundesdeutsche Strafrecht, da es im Einklang mit dem Grundgesetz der Bundesrepublik Deutschland und den durch dieses garantierten Freiheiten steht. Dieser feste Maßstab verhindert ein willkürliches oder zensorisches Vorgehen der Beschwerdestelle.

Sind die Beanstandungen berechtigt und die gemeldeten Inhalte verstoßen gegen geltendes bundesdeutsches Recht, ergreift „netwatch“ unter Einschaltung der verantwortlichen Provider Maßnahmen zur Löschung der Inhalte. Bei Kenntnis der Identität oder Anhaltspunkten, die auf die Identität von Straftätern, die illegale Inhalte über das Internet verbreiten, schließen lassen, werden die ermittelten Daten an die zuständigen Strafverfolgungs- und Sicherheitsbehörden weitergeleitet.

5.2. Erfolg

Auf diesem Wege hat die naiin-Beschwerdestelle „netwatch“ seit ihrer Gründung bereits mehr als 126.100 Hinweise bearbeitet. Diese wurden in insgesamt 15.460 eingeleiteten Ermittlungsverfahren gebündelt. Die Bündelung erfolgt aufgrund von so genannten Mehrfachmeldungen, gezielten Operationen oder konkreten Tätergruppen.

5.3. Transparenz durch Live-Ticket-Verfahren

Da die Abgabe von Hinweisen durch die Internet-Nutzer an naiin einem Vertrauensbeweis gleichkommt, hat sich die Initiative auf ein Höchstmaß an Transparenz festgelegt. Mit seinem Live-Ticket-Verfahren setzt naiin europaweit Standards bei der Bearbeitung von Hinweisen auf illegale Internet-Inhalte. Keine andere Initiative in Europa gönnt sich ein solch hohes Niveau an Transparenz.

Das System erlaubt es Hinweisgebern den Bearbeitungsstatus ihrer Hinweise online einzusehen. Darüber hinaus können auch andere Internet-Nutzer – also die Öffentlichkeit – alle laufenden und abgeschlossenen Verfahren einsehen. Natürlich werden aus Sicherheits- und Datenschutzgründen keine inhaltlichen Informationen zur Einsicht bereitgestellt. Angezeigt werden neben dem Aktenzeichen eines eingegangenen Hinweises, der Kriminalitätsbereich, dem der Hinweis zugeordnet werden kann, sowie dessen Bearbeitungsstatus.

Aktenzeichen	Bereich	Status
070605-3	Kinderpornografie	geprüft
070605-2	Kinderpornografie	abgeschlossen
070605-1	Kinderpornografie	eingestellt
060605-3	Kinderpornografie	erfasst
060605-2	Kinderpornografie	erfasst
060605-1	Kinderpornografie	erfasst
050605-8	Kinderpornografie	erfasst
050605-7	Kinderpornografie	geprüft
050605-6	Rechtsextremismus	ruht
050605-5	Kinderpornografie	geprüft
050605-4	Kinderpornografie	geprüft
050605-3	Kinderpornografie	geprüft
050605-2	Kinderpornografie	eingestellt
050605-1	Kinderpornografie	geprüft
040605-4	Linksextremismus	eingestellt

Diese Maßnahme soll das Vertrauen der Nutzer in die naiin-Beschwerdestelle weiter stärken und zumindest eine begrenzte Überwachung der naiin-Aktivitäten bei der Bekämpfung von Internet-Kriminalität bieten. Insbesondere beim Handling von Fällen wie Kinderpornografie ist eine solche Transparenz als notwendig zu erachten und eine Frage der Glaubwürdigkeit.

5.4. Erweiterung der Schwerpunkte

Im 4. Quartal 2003 hat naiin auf die aktuellsten Entwicklungen im Bereich der Internet-Kriminalität reagiert, und seine Themenschwerpunkte erweitert. Während sich naiin seit seiner Gründung hauptsächlich der Bekämpfung von Rechtsextremismus und Kinderpornografie im Internet widmete, hat die Initiative Ende Oktober 2003 ihr Engagement auch auf weitere Internet-Kriminalitätsfelder ausgedehnt.

Hierzu gehören: Die Bekämpfung von Linksextremismus, Ausländerextremismus, sodomitischen Darstellungen, Gewaltpornografie, Spam, Online-Betrug, Musik-, Film- und Softwarepiraterie (Piraterie), Gewaltdarstellungen; weiterhin die Durchsetzung des Jugendschutzes im Internet sowie die Beobachtung von so genannten „Dark Sites" (Satanismus, Kannibalismus etc.) und Suizidforen.

Für die erfolgreiche Bekämpfung von Internet-Kriminalität ist es essentiell auf aktuelle Entwicklungen zu reagieren.

5.5. Problemstellung: Die Globalität des Internets

naiin macht anders als andere bundesdeutsche Einrichtungen ebenso wenig wie das Internet an den Grenzen der Bundesrepublik Deutschland halt. naiin wirkt international und trägt somit der Globalität des Internets Rechnung.

Die Hauptschwierigkeit dieses globalen Engagements ist, dass das bundesdeutsche Recht eben nicht weltweit Geltung hat. Um die jeweilige Rechtslage anderer Staaten ausreichend zu berücksichtigen, sind auf globaler Ebene drei Hauptkriterien von Relevanz:

1. Standort des Servers, auf dem die beanstandeten Inhalte liegen
2. Sprache, in der die beanstandeten Inhalte abgefasst sind
3. Aufenthaltsort derjenigen Person, die die beanstandeten Inhalte ins Internet eingestellt hat

Es bleibt gesondert zu erwähnen, dass im Rahmen der Bekämpfung von Kinderpornografie ein weltweit einheitlicher Standard angelegt wird.

5.6. Indikator für künftige Entwicklungen in der Internet-Kriminalität

Die naiin-Beschwerdestelle wirkt als wichtiger Indikator für künftige Entwicklungen in der Internet-Kriminalität. Anhand des Hinweisaufkommens sind aktuelle Trends ersichtlich. So konnte naiin bereits frühzeitig die Entwicklungen im Bereich des so genannten Phishings prognostizieren.

Ein weiterer wesentlicher Bestandteil der Arbeit der naiin-Fahnder ist neben der Entgegennahme und Bearbeitung von Hinweisen der Beschwerdestelle auch die Beobachtung der einzelnen Kriminalitäts-bereiche im Internet. Ähnlich wie der Verfassungsschutz beobachtet naiin beispiels-

weise Diskussionsforen der rechtsextremistischen Szene. Aber auch die Pädophilen-Szene, terroristische Plattformen sowie linksextremistische Kommunikationsportale stehen unter intensiver Beobachtung.

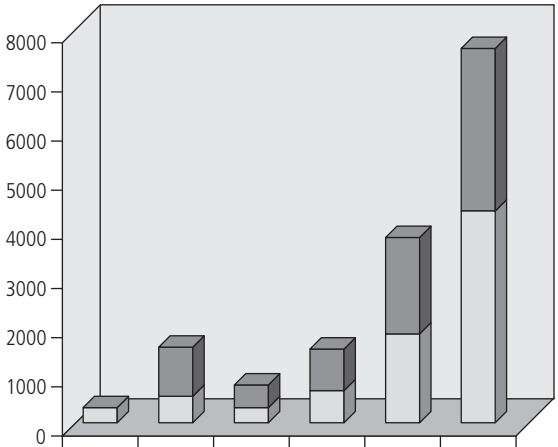
Mit Hilfe der gewonnen Erkenntnisse ist es naiin möglich, regelmäßig Analysen aktueller Bedrohungsszenarien durchzuführen. Dies ist erforderlich, um Maßnahmen und Strategien anzupassen.

5.7. Vorteile gegenüber Strafverfolgungsbehörden

naiin hat im Rahmen seiner Arbeit entscheidende Vorteile gegenüber den Sicherheits- und Strafverfolgungsbehörden. Vor allem in der grenzüberschreitenden Arbeit ist naiin besser positioniert. Die Initiative muss sich beispielsweise nicht an existierende Rechtshilfe-abkommen halten.

Persönliche Kontakte zu ausländischen Strafverfolgungsbehörden ermöglichen so die schnelle Weiterleitung von aktuellen Verfahren an die jeweils zuständigen Behörden weltweit. naiin leistet damit seinen Teil zur globalen Verfolgung von Straftätern im Internet.

5.8. Ermittlungsverfahren 2000 – 2005



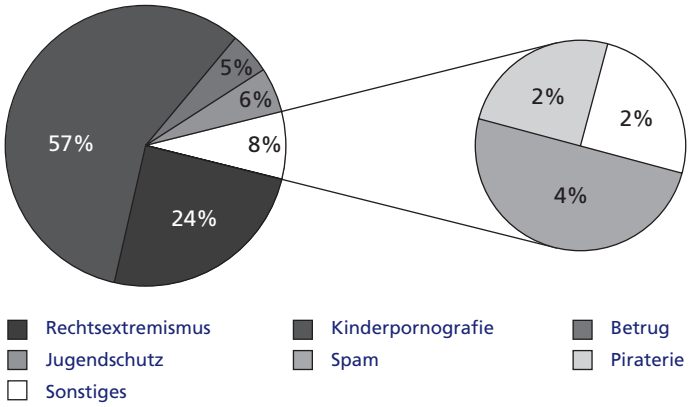
	2000	2001	2002	2003	2004	2005
Eingestellt	0	1022	491	865	1958	3282
Abgeschlossen	290	503	264	627	1807	4351

In den Jahren 2000 – 2005 hat die naiin-Beschwerdestelle netwatch 15.460 Ermittlungsverfahren geführt, die aus mehr als 126.100 Hinweisen hervorgegangen sind. Dabei konnte allein in den Jahren 2004 und 2005 74 Prozent des Verfahrensaufkommens verzeichnet werden. Dies ist zum einen auf den zunehmenden Bekanntheitsgrad von naiin; zum anderen auf das steigende Sicherheitsbewusstsein der Internet-Nutzergemeinde zurückzuführen.

Zugleich hat in den vergangenen Jahren die Fähigkeit der Internet-Nutzer zugenommen, zwischen strafbaren und legalen Inhalten unterscheiden zu können. Stellten sich in den Jahren 2001 und 2002 noch 67 bzw.

65 Prozent der eingegangenen Hinweise als unbegründet heraus, nahm dieser Anteil bis zum Jahr 2005 bei einem überproportionalen Anstieg des Hinweisaufkommens deutlich ab. Im vergangenen Jahr wurden nur noch 39 Prozent der Hinweise als „unbegründet“ eingestuft.

5.8.1. Beschwerden nach Kriminalitätsbereichen



6. Die relevantesten Kriminalitätsbereiche

6.1. Rechtsextremismus

Schon seit den Anfangstagen des weltweiten Kommunikationsnetzes – Internet – nutzen rechtsextreme Organisationen und Personen dieses Medium zur Verbreitung ihrer Propaganda. Politische Agitation, Verabredung zu Demonstrationen, Versandhäuser für Skinheadbedarf, Chat-Rooms, Kontaktbörsen, Hasslisten, Internetradio und Internetfernsehen etc., alles was technisch möglich ist, wird von Rechtsextremisten genutzt, und das qualitativ und quantitativ weiterhin zunehmend.

Damit ködern sie vor allem junge Leute, die ja bekanntermaßen eine besondere Affinität zum Internet haben. Das Internet ist zu einem der wichtigsten Kommunikations- und Propagandainstrumente der rechtsextremen Szene geworden. Vor allem in der Professionalität unterscheidet sich der Rechtsextremismus damit deutlich von anderen extremistischen Positionen.

Es gibt Menschen, die der Meinung sind, dass das Internet anders als alle anderen Medien völlig frei und unreglementiert sein soll. Das Grundgesetz ist jedoch auch eine Art von Reglementierung. Es ist sehr hochwertig, erfolgreich und erhaltenswert. Das Denken und Handeln der Rechtsextremisten läuft implizit oder sogar direkt ausgesprochen auf eine Abschaffung des Grundgesetzes hinaus.

6.1.1. Gemeinsam ist ihnen allen: Nationalismus und Hass

Der Rechtsextremismus umfasst nicht nur offline ein breites Spektrum. Auch online repräsentieren sich die unterschied- lichsten Gruppierungen des Rechtsextremismus auf verschiedenste Art und Weise.

Von Skinheads, über Parteien, Versandhäusern, die Tonträger, T-Shirts (bzw. „T-Hemden"), Fahnen, Anstecker etc. anbieten, über radikale Band-Sites, Holocaust-Leugnern bis hin zu Sekten, Kontaktbörsen, rechtsextremen Spiele-Clans und Sites über Mythologie sowie Heidentum mit rechtsextremer Tendenz umfassen das Spektrum.

Das Weltbild aller rechtsextremen Strukturen im Internet ist dennoch nahezu identisch. Gemeinsam ist ihnen: Der Hass gegen Ausländer, Juden, Homosexuelle, gegen die Demokratie, die Bundesrepublik, die EU, die UNO, gegen Amerika, Linke, Schwarze, Christen, Moslems. Die Liste der Feinde ist lang.

Man kann sagen, die Rechtsextremisten sind hochgradig paranoid. Sie fühlen sich von Feinden umstellt und brauchen dies aber genau zu ihrem Selbstverständnis: Sie fühlen sich als die einzig Aufrechten und Verfolgten in einer Welt voller Feinde.

Sie kämpfen gegen „die Lügen der Politik", gegen „die Verschwörungen der Juden", gegen Zensur (NPD-Verbot, „Auschwitzlüge" usw.), gegen „Überfremdung" und vieles mehr. Diese Selbststigmatisierung verschafft ihnen Identität und Attraktivität, gerade bei Jugendlichen.

6.1.2. Server-Standort Deutschland

Um seine Inhalte im Internet verfügbar zu machen, muss man diese auf einem Server unter einer bestimmten Internet-Adresse (URL) zugänglich machen. Das ist das Geschäft der sogenannten Hostprovider – auch Webhoster genannt –, die einerseits Domainnamen vergeben, andererseits Webspace – sprich: Speicherplatz im Internet – gegen eine Kostenpauschale zur Verfügung stellen.

Diese Hostprovider sind nicht zu verwechseln mit den Accessprovidern (zu Deutsch: Zugangsanbietern) wie beispielsweise „AOL", die den Zugang ins Internet bereitstellen. Die Hostprovider in Deutschland achten inzwischen darauf, dass sie möglichst keine rechtsextremistischen Seiten mit strafbaren Inhalten hosten. Sobald ihnen solche Seiten bekannt werden, entfernen sie diese umgehend von ihren Servern.

Das hatte zur Folge, dass der Server-Standort Deutschland für die Betreiber von Seiten mit illegalen rechtsextremen Inhalten in den vergangenen Jahren zunehmend an Attraktivität verlor. Dementsprechend wanderten die meisten Anbieter rechtsextremer Inhalte ins Ausland ab und speisen in Ländern wie den USA ihre Inhalte in das World Wide Web ein.

USA: Freedom of Speech

Bei der Wahl der ausländischen Server-Standorte spielt dabei die in den einzelnen Ländern im Vergleich zur Bundesrepublik Deutschland

unterschiedliche Rechtslage eine wesentliche Rolle. So ist in den USA das Recht auf freie Meinungsäußerung (Freedom of Speech) garantiert durch den „First Amendment of the U.S. Constitution" (deutsch: 1.Verfassungszusatz der Verfassung der Vereinigten Staaten von Amerika) fast unbeschränkt.

Es darf jeder Naziparolen verbreiten, Hasslisten veröffentlichen oder den Holocaust leugnen. So etwas wie Volksverhetzung gibt es im US-amerikanischen Strafrecht nicht und wird es wohl auch in naher Zukunft nicht geben, weil dazu die amerikanische Verfassung geändert werden müsste.

Daher sind dort inzwischen die meisten rechtsextremen deutschsprachigen Homepages gehostet. Unter dem Eindruck der Terroranschläge vom 11. September 2001 ist die Bereitschaft vieler amerikanischer Provider zur Abschaltung extremer Webseiten zwar gestiegen. Zugleich gibt es aber auch viele amerikanische Rechtsextremisten – darunter der US-amerikanische Nazi Gerhard Lauck –, die als Provider auftreten und ihren deutschen Gesinnungsgenossen gern ihre Dienste anbieten.

6.1.3. Entwicklungen

In den vergangenen fünf Jahren konnte ein signifikanter Rückgang von rechtsextremistischen Websites mit strafbaren Inhalten verzeichnet werden.

Die Strategie einer konsequenten Sperrung derartiger Angebote – auch über Ländergrenzen hinweg – sowie die Erfolge der Strafverfolgungsbehörden trugen demnach Früchte. Das Gefahrenpotential ist damit aber nicht gesunken. Die Nutzung des Internets als Medium zur Kommunikation, Nachwuchsrekrutierung und Selbstdarstellung ist in der rechtsextremen Szene unverändert hoch.

Die Szene verzichtet aber mittlerweile darauf, ihre Websites – die zum größten Teil auch wieder in der Bundesrepublik Deutschland gehostet werden – mit strafbaren Inhalten auszustatten. Stattdessen greift sie auf szene-interne Codes und Schlagwörter zurück. Die Ideologie bleibt jedoch unterschwellig vorhanden. Vor allem Diskussionsforen erfreuen sich großer Beliebtheit in der Szene. In diesem Bereich werden inzwischen auch die meisten Straftaten verübt. In der Annahme, auf fremden Diskussionsplattformen relativ anonym zu kommunizieren, werden Hetzschriften, Bombenbauanleitungen, strafbare Kennzeichen wie das Hakenkreuz u.ä. publiziert. Darüber hinaus dienen diese Plattformen auch der Verabredung zu Demonstrationen oder Treffen zu geheimen Veranstaltungen wie nicht angemeldeten Neonazi-Konzerten.

Auch der Handel mit Nazi-Devotionalien oder verbotenen rechtsextremen Tonträgern floriert im Internet. Über kleine aber auch große, etablierte Internet-Auktionshäuser versuchen rechtsextremistische Internet-Nutzer immer wieder ihre zum großen Teil illegale Ware an den Mann zu bringen.

6.1.4. Tendenz

Es ist auch künftig mit einer weitreichenden professionellen Nutzung des Internets durch Rechtsextremisten zu rechnen. Darüber hinaus kann davon ausgegangen werden, dass die Zahl der rechtsextremistischen Websites mit strafbaren Inhalten nach dem zu verzeichnenden Rückgang in den kommenden Jahren wieder ansteigen wird. Als Hauptgrund für diese Annahme ist vor allem das nachlassende öffentliche Interesse an dem Thema anzuführen. Der Druck durch die Medien auf Politik, Wirtschaft, Strafverfolgung und Gesellschaft ist deutlich gesunken. Themen wie die Bekämpfung des internationalen Terrorismus haben die Auseinandersetzung mit dem Rechtsextremismus merklich abgeschwächt.

Durch diesen Umstand schwindet auch der Verfolgungsdruck, den das öffentliche Interesse vor allem in der Jahren 2000 und 2001 auf die Szene ausgeübt hat. Infolgedessen werden zunächst wieder deutschsprachige Anbieter zur Verbreitung strafbarer rechtsextremistischer Propaganda missbraucht werden. Nach einsetzender Strafverfolgung wird die Szene dann wieder auf ausländsche Anbieter ausweichen.

6.2. Linksextremismus

Auch wenn nicht so ausgeprägt wie der Rechtsextremismus, sind linksextremistische Strukturen im Internet aber ebenso präsent. Die linksextremistischen Seiten sind zum großen Teil aber designtechnisch nicht so anspruchsvoll gestaltet, sondern eher unauffällig – teils textlastig mit wenigen Grafiken.

Die Besucherzahlen halten sich zwar in Grenzen, aber dennoch haben es die dort publizierten Texte ebenso in sich wie beim Rechtsextremismus. Gewaltverherrlichung und -Aufrufe, verfassungswidrige Propaganda, Bombenbauanleitungen und viele weitere strafbare Inhalte gehören mitunter zum Repertoire linksextremistischer Websites.

Gewaltbereitschaft und Demokratiefeindlichkeit werden in der Präsenz des Linksextremismus im weltweiten Datennetz genauso deutlich wie beim Rechtsextremismus. Und das Kommunikationsmedium Internet hat zweifelsohne auch in der linksextremistischen Szene eine wichtige Rolle eingenommen.

6.2.1. Linksextreme Publikationen: Digital statt Print!

Nach dem Scheitern der herkömmlichen Agitationsorgane – Zeitungen und Publikationen in Print-Form – verlagerten sich viele linksextremistische Publikationen ins weltweite Datennetz.

So konnten linksextremistische Gruppierungen ihre Zeitschriften aufgrund mangelnder Nachfrage nicht mehr finanzieren. Das Internet bot Abhilfe: Hier lässt sich kostengünstig ein zahlenmäßig großes Publikum unkompliziert erreichen. Nahezu das gesamte linksextremistische Publikationsangebot ist daher im Internet vertreten. In der Regel stehen auf den Seiten auch ganze Archive mit Beiträgen der früheren – auch Print-Ausgaben – zur Verfügung.

Durch die Websites, die die Publikationen begleiten, erhöht sich zugleich auch die Aktualität der Informationen. Während Printmedien aus Kostengründen nur vierzehntägig, monatlich, quartalsweise oder gar halbjährlich erscheinen konnten, ist es nun möglich eine täglich aktualisierte Informationsplattform bereitzustellen. Ein Tatbestand, der auch der Mobilisierung der Szene für beispielsweise kurzfristig organisierte Internet-Aktionen, Demonstrationen oder Gegendemonstrationen (z.B. zu rechtsextremen Aufmärschen) zu Gute kommt.

6.2.2. Virtueller Kampf: Antifa vs. Nationaler Widerstand

Das Internet stellt für Links- und Rechtsextremisten nicht nur eine globale Plattform für Agitation, Vernetzung und Mobilisierung dar, sondern ist auch ein Schauplatz im Kampf zwischen den beiden Positionen – gar eine virtuelle Kampfarena. Angefangen von der Veröffentlichung von Steckbriefen „politischer Feinde", die zuvor ausspioniert werden, beleidigt man sich gegenseitig in Gästebüchern und Diskussionsforen des jeweiligen Gegners.

Weder Antifa (Häufiger Bestandteil der Namen linksextremistischer Vereinigungen) auf der einen Seite noch Nationaler Widerstand auf der anderen Seite nehmen sich in ihren verfassungsfeindlichen Einstellungen viel. Beide Parteien sprechen sich gegenseitig die durch die Verfassung gegebenen Grundrechte – insbesondere das Existenzrecht (nicht nur das politische) – ab.

So kursierte in der linksextremistischen Internet-Szene eine Publikation namens „Das Schlachten eines Faschisten für den menschlichen Verzehr – Eine Schritt-für-Schritt-Anleitung für die Zerlegung eines Faschisten in servierbare, vorzügliche Stücke Fleisch". An dieser gegenseitigen Menschenverachtung ändert letztlich auch nicht die Tatsache, dass man zeitweilig gar dieselben Ansichten (siehe Krieg gegen den Irak) vertritt.

6.2.3. Entwicklungen / Trends

Die Nutzung des Internets durch linksextremistische Gruppierungen blieb in den vergangenen Jahren auf hohem Niveau. Mit in der Programmiersprache Flash programmierten Online-Spielen sprach die Szene auch zum Teil gezielt jugendliche Nutzer an. Diese hohe Nutzung des Mediums durch den Linksextremismus wird auch in den kommenden Jahren konstant bleiben.

6.3. Islamistischer Terrorismus

Spätestens seit den Terroranschlägen vom 11. September 2001 ist der Öffentlichkeit bewusst, dass Terroristen und ausländerextremistische Strukturen das Internet intensiv nutzen. So steht fest, dass die Rolle des Internet in Zusammenhang mit den Anschlägen auf das World Trade Center und das Pentagon keine unbedeutende war.

Darüber hinaus sind nahezu alle in der Bundesrepublik Deutschland präsenten islamistischen Organisationen mit eigenen Web-Auftritten im Internet vertreten. Sie verwenden das Internet vor allem zu Selbstdarstellungs- und Propagandazwecken, aber zunehmend auch zur Kommunikation, die sie mit diversen Methoden verschlüsseln.

6.3.1. Al-Qaida-Drohungen via Internet

Nach den Terror-Anschlägen vom 11. September 2001 in den USA stellt das Kommunikationsnetzwerk Internet oftmals nur noch die einzige Möglichkeit für Terror-Organisationen wie „Al-Qaida“, die für die Anschläge in New York und Washington DC verantwortlich zeichnet, dar, sich zu artikulieren.

So ist spätestens seit Ende 2002 eine verstärkte Agitation der Organisation und ihres Anführers Osama Bin Laden über das Medium zu verzeichnen. Al-Qaida verbreitete und verbreitet Drohungen über das Internet – darunter auch ein Video, in dem die Bundesrepublik Deutschland erstmals als eines der Feindbilder der Terrororganisation Erwähnung fand.

Stichwort: Psychologische Kriegsführung

Mit ihren Verlautbarungen drohen sie nicht nur, sondern betreiben auch psychologische Kriegsführung. Sie rechtfertigen im Nachhinein ihre Attentate (z.B. den Anschlag auf Djerba), vereinnahmen Anschläge für sich (u.a. die Geiselnahme von Moskau Ende Oktober 2002) und wollen Sympathisanten mobilisieren. Drohungen gegenüber dem „Westen" wurden dabei mehrfach wiederholt und sogar ausgeweitet.

6.3.2. Islamisten im WWW: Ausbildung im Online-Lager

Die Server, über die die Propaganda islamistischer Extremisten in das World Wide Web eingestellt werden, sind nicht nur in Ländern des Nahen Osten oder Asiens, sondern in nicht wenigen Fällen auch in den USA beheimatet, was im ersten Augenblick hinsichtlich der Terroranschläge vom 11. September 2001 sicherlich verwundert. Dort sind viele Inhalte trotz der Anschläge nach wie vor durch die Meinungsfreiheit gedeckt und anonymes Webhosting ist möglich. So gestaltet sich die Suche nach den Urhebern der Websites meist sehr schwierig.

Nach außen hin scheinen die meisten Websites islamistischer Extremisten zunächst harmlos, doch beim näheren Studium erweisen sie sich aber häufig als Verlautbarungs-Propaganda. Demgegenüber stehen aber auch Websites, deren Betreiber von vornherein keinen Hehl aus ihrer Ideologie machen. Auf diesen findet man Animationen, die beispielsweise den

Al-Qaida-Führer Osama bin Laden zeigen, wie er ein Sturmgewehr auf US-Präsident George W. Bush jr. richtet und abdrückt.

Gar das Eintauchen in ein ehemaliges Ausbildungslager der Terroristen in u.a. Afghanistan ist online möglich. Gezeigt wird, wie Anschläge trainiert werden und der Nutzer darf auch selbst ans Gewehr: Über Internet-Spiele kann geübt werden, ranghohe Politiker zu liquidieren. Hinter den teils anspruchsvollen Animationen, Online-Spielen etc. stehen meist junge technisch versierte Menschen, die ein Interesse an diesen Themen haben.

Die Quintessenz der in zahlreichen Sprachen gestalteten Seiten ist im Wesentlichen gleich: Die Gegenüberstellung des „verdorbenen, zum Untergang bestimmten Westens" und des „heilbringenden Islams".

6.3.3. Entwicklungen / Trends

Die Zahl der Diskussionsforen und Chat-Rooms, die der weltweiten Kommunikation von Anhängern islamistisch-terroristischer Organisationen dienen, ist in den vergangenen Jahren ebenso stark angestiegen wie die unzähligen Websites, die sich dem Thema widmen.

Zudem offenbaren sich gewisse ideologische Verbindungen zum Rechtsextremismus. Der Antisemitismus und Anti-Amerikanismus führt zum Teil zu erstaunlichen Zusammenschlüssen. So verlinken sich nicht wenige islamistische und rechtsextremistische Websites bereits untereinander.

Es ist davon auszugehen, dass das Internet auch bei den jüngsten Eskalationen hinsichtlich der Auseinandersetzung mit den Mohammed-Karrikaturen eine wesentliche Rolle gespielt hat. So hatten Islamisten Ende Januar 2006 angekündigt, den Server der dänischen Tageszeitung „Jyllands Posten“ attackieren zu wollen.

Tendenz

Es ist damit zu rechnen, dass islamistische Terroristen das Internet künftig noch stärker nutzen werden. Auch ein gezielter terroristischer Anschlag auf die Infrastruktur des Internets ist in naher Zukunft nicht auszuschließen. Aufgrund der wirtschaftlichen Bedeutung, die dem weltweiten Datennetz heutzutage bereits zukommt, würde ein solcher Anschlag – abgesehen von seinem Symbolgehalt – hohe finanzielle Schäden verursachen.

6.4. Kinderpornografie

Der sexuelle Missbrauch von Kindern ist zweifelsohne eines der abscheulichsten Verbrechen. Derzeit kursieren mehrere Millionen kinderpornografische Bilddateien, die den sexuellen Missbrauch an Kindern dokumentieren, im weltweiten Datennetz – dem Internet. Hinzu kommen noch zahlreiche Videos und andere Dateiformate kinderpornografischer Natur.

Der Handel mit Kinderpornografie über das Internet nimmt bei den verhältnismäßig sehr wenigen Ermittlungserfolgen dramatisch und rasant zu. Und wie ausgeprägt dieser Online-Handel ist, zeigen polizeiliche Ermittlungen: Denn ist eine kinderpornografische Datei erst einmal im Umlauf, verschwindet sie nicht mehr vom Markt.

Trotz bereits stattgefundener Thematisierung in der Öffentlichkeit sind „Kindesmissbrauch" und „Kinderpornografie" nach wie vor zu den Tabuthemen unserer Gesellschaft zu zählen. Ziel muss es sein in Kooperation mit Initiativen, Vereinen, Behörden und der Wirtschaft national sowie international die Öffentlichkeit für diese Thematik zu sensibilisieren und Kindesmissbrauch sowie den Handel mit Kinderpornografie im Internet aktiv zu bekämpfen.

6.4.1. Vorteile des Internets: Missbraucht durch Perverse

Kinderpornografie ist an sich kein neues Phänomen. Relativ neu ist allerdings die Verbreitung dieser über das Internet. Technische Neuerungen, die das „neue Medium" begleiten, kommen dem Handel mit Kinderpornografie sehr entgegen.

Das Internet ermöglicht, dass sich Perverse und Kinderschänder grenzüberschreitend an Bildmaterialien aller Art ergötzen können. Sie tauschen unter anderem Reisetipps zu Wallfahrtsstätten von Pädophilen in Asien, Südamerika oder Osteuropa aus und treffen sich zur gemeinschaftlichen Folter von Kindern via Webcam.

Zudem ist der Handel mit Kinderpornos im Internet von einer gewissen Professionalität gekennzeichnet, die von der unterschiedlichen Rechtslage weltweit und auch von den technischen Möglichkeiten des Internet (dezentrale Struktur / Anonymität) profitiert.

6.4.2. Die Tauschbörsen – Auch Kinderschänder kennen P2P!

Über sogenannte Tauschbörsen im Internet tauschen pädokriminelle Internet-User im Sekundentakt weltweit große Datenmengen an kinderpornografischem Material.

Einschlägige Suchbegriffe aber auch vermeintlich harmlose „Keywords“ – wie die Eingabe der Namen von Größen des internationalen Pops – führen in den peer-to-peer-Netzwerken, die von Millionen von Internet-Usern genutzt werden, zu kinderpornografischen Bildern und Videos.

Ungewollter Download von Kinderporno

Die Zahl der Fälle, in denen sich peer-to-peer-Nutzer auf der rechtswidrigen Suche nach aktuellen Musik-Hits und Kinofilmen ungewollt härteste Kinderpornografie auf den Rechner ziehen, steigt. Oft stehen die Betreiber dieser Musiktauschbörsen dem Treiben selbst machtlos gegenüber. Peer-to-peer-Netzwerke sind nämlich ebenso wie das Internet dezentral strukturiert. Das heißt, dass diese Netzwerke ohne einen zentralen Server auskommen.

Hinzu kommt, dass die für den Dateitausch notwendige Software wie zum Beispiel „Kazaa“ oder „Limewire“ neben dem Austausch von gewöhnlichen Dateiformaten auch die Weitergabe von Bild- und Videodateien ermöglicht.

6.4.3. Wonderworld: Chat im Zeichen der Kinderpornografie

Der Handel mit Kinderpornografie im Internet findet unter anderem in geschlossenen Nutzergruppen statt. Die Ermittlung und Strafverfolgung der diesen Gruppen angehörenden Internet-Nutzer ist in der Regel gemeint, wenn in den Nachrichten von der Sprengung von sogenannten Internet-Kinderporno-Ringen die Rede ist.

Die Mitglieder dieser geschlossenen Nutzergruppen, in dessen Rahmen vorwiegend der Tausch kinderpornografischer Materialen denn der kommerzielle Handel mit derartigem Material im Mittelpunkt steht, machen sich u.a. die „Chat"-Technologie zu Nutze.

Die Vorteile des Internet-Chats liegen auf der Hand:

::: Kommunikation in Echtzeit

Eine Vielzahl von Nutzern weltweit kann zeitgleich miteinander kommunizieren.

::: Ein gewisses Maß an Anonymität

Wahl eines Pseudonyms, wobei der Internet-User gegenüber anderen Chat-Nutzern weitgehend anonym bleibt. Lediglich der Administrator ist in der Lage den jeweiligen Nutzer ohne großen Aufwand zu reanonymisieren – sprich dessen IP-Adresse zu ermitteln.

::: Möglichkeiten der Abschottung

In den Online-Chats ist es jedem Nutzer möglich einen eigenen sogenannten Chat-Room unter einem von ihm bestimmten Titel zu eröffnen. Der Zugang kann dabei mit einem Passwort geschützt werden, so dass Gleichgesinnte unter sich bleiben können. D.h. die Aktivitäten in diesen Räumen sind für Nutzer, die nicht über das Passwort verfügen, nicht sichtbar.

IRC – Internet Relay Chat

Diese Eigenschaften begünstigten die Entwicklung von nationalen und internationalen Online-Chats zu Treffpunkten der Kinderschänder-Szene maßgeblich. Zu diesen Treffpunkten ist unter anderem auch der größte internationale Chat-Bereich, der „Internet Relay Chat" (IRC), zu zählen. Jeder Nutzer kann dort einen eigenen Bereich – einen sogenannten „Kanal" – eröffnen. An manchen Tagen laufen auf diese Weise bis zu 20.000 IRC-Kanäle gleichzeitig.

Der harte Kern der internationalen Szene der Kinderporno-Händler trifft sich hier, um Erfahrungen, Bilder, Videos aber auch Kinder zu tauschen. Man verabredet sich, macht einen „Kanal" auf, tauscht und verschwindet wieder.

6.4.4. Kindersexshops – Kindersex gegen Kreditkarte

Neben einer Vielzahl von Pädophilen, die „privat" ihre kinderpornografischen Materialen über Newsgroups, Mail, Tauschbörsen und Online-Chats untereinander kostenfrei austauschen, gibt es Geschäftsleute und Banden, die einen hochprofessionellen Handel mit Kinderpornografie betreiben.

Sie haben sowohl die Vorteile des Internets als globale Plattform als auch den großen und gewinnbringenden Markt für Kinderpornografie erkannt. Zu den Vorteilen des weltweiten Netzes gehört zweifelsfrei, dass Inhalte aus allen Ländern – darunter auch Länder, in denen Handel, Herstellung und Besitz von kinderpornografischem Material nicht strafbar sind oder zumindest nicht verfolgt werden – eingespeist werden können.

Aufbau der Kindersex-Seiten

Diese Geschäftsleute eröffnen professionelle Sexshops, die kennwortgeschützt nur durch registrierte Nutzer betreten werden können. Für diese Kunden stehen Datenbanken mit Fotos, Zeichnungen, Videos und Texte kinderpornografischer Natur uneingeschränkt zur Verfügung. Und der Kunde zahlt per Kreditkarte. Der Aufbau dieser kinderpornografischen Sexshopseiten ist oftmals gleich. In der Regel stehen auf der Startseite, auf der bereits mit „free pics" (dt.: kostenlosen Bildern) eifrig Kundenfang betrieben wird, drei Bereiche zur Auswahl: „Free Tour" oder „Preview", „Members"und „Join".

Im Rahmen der „Free Tour“ wird mit ausgesuchten Bildern geworben, um den potenziellen Kunden zu einer meist sehr teuren Mitgliedschaft zu überreden. Neben einzelnen Fotos gibt es auch kommerzielle kinderpornografische Webangebote, die auch mal eine ganze Galerie nackter, missbrauchter Kinder oder das ein oder andere Video selbiger Natur zur kostenfreien Einsicht zur Verfügung stellen.

Die „Free Tour“ besteht in der Regel aus zwei oder drei Seiten. Danach landet der Besucher automatisch im Bereich „Join“. Dort findet der Surfer dann den Preis, den er zahlen muss, um Zugang zu erhalten, sowie ein Formular zur Registrierung. Abgerechnet wird in der Regel ausschließlich über Kreditkarte.

Nach seiner Registrierung bekommt der Nutzer dann die Bestätigung samt Zugangsdaten für den „Member“-Bereich per Mail zugesandt. Damit erhält er uneingeschränkten Zugriff auf das gesamte Angebot des jeweiligen Kindersexshops. Obwohl der Händler sowie der Provider, der das Angebot hostet, in den einigen Fällen identifiziert werden können, gelingt es meist schwer oder überhaupt nicht derartige Sexshops „schließen“ zu lassen.

Grund: Händler und Provider sitzen häufig im „sicheren Ausland“ – sprich: In Ländern, in denen die Rechtslage derartige Geschäfte zulässt beziehungsweise in denen massive Defizite auf dem Gebiet der Strafverfolgung existieren. Die Betreiber derartiger Kindersexshops haben dabei nicht viel Mühe Webhost-Unternehmen zu finden, für die Geld bedeutender ist als Moral, Verantwortung und Menschlichkeit.

6.4.5. Entwicklungen / Trends

Trotz Fahndungserfolgen seitens der Strafverfolgungsbehörden – bei der Operation „Marcy“ im September 2003 wurden auf einen Schlag weltweit 38 kinderpornografische Zirkel im Internet gesprengt und knapp 26.500 Tatverdächtige identifiziert – und ein konsequentes weltweites Vorgehen der Internet-Wirtschaft gegen kinderpornografisches Material ist mit einer deutlichen Abnahme derartiger Cyber-Verbrechen in den kommenden Jahren nicht zu rechnen. Zu sehr verfestigt hat sich die mit einem hohen Organisationsgrad ausgestattete mafia-ähnlich strukturierte Kinderporno-Industrie. Vor allem die Politik ist hier gefragt, ein Umfeld zu erzeugen, in dem ein weltweites Engagement gegen derartige Verbrechen möglich ist.

6.5. Jugendschutz

Das weltweite Datennetz birgt Gefahren für Kinder und Jugendliche. Nicht selten kommt es vor, dass sich Kinder online sexuellen Attacken seitens pädophiler Internet-Nutzer ausgesetzt sehen.

Sowohl die Politik als auch die Wirtschaft haben reagiert: Schärfere Jugendschutzbestimmungen, die Kinder vor unter anderem pornografischen, extremistischen und gewaltverherrlichenden Inhalten schützen sollen, sind seit dem 1. April 2003 in Kraft und Unternehmen arbeiten intensiv an der Entwicklung von Filterprogrammen und Altersverifikationssystemen.

Rechtliche und technische Maßnahmen können jedoch nicht die elterliche Aufsicht ersetzen, auf die Kinder und Jugendliche beim Surfen angewiesen sind und die den effektivsten Schutz der jüngsten Internet-Nutzer vor schädlichen und illegalen Internet-Inhalten darstellt.

6.5.1. Chats: Täglich werden Kinder sexuell genötigt

Das Chatten stößt insbesondere bei Kindern und Jugendlichen auf große Begeisterung. Das wissen aber auch pädophile Internet-Nutzer. Getarnt hinter harmlosen Nicknames geben sie sich in privaten Zwiegesprächen – eine Eigenschaft der Chat-Technologie – als gleichaltrig aus und belästigen Kinder und Jugendliche sexuell.

Derartige sexuelle Übergriffe auf Kinder in Chat-Rooms sind alltäglich, wie eine US-Studie belegt. Von 1000 befragten Teenangern weiblichen Geschlechts wurden 30 Prozent im Internet schon einmal sexuell belästigt. Jedes fünfte Kind wird zudem online zu sexuellen Handlungen aufgefordert.

Auch in Deutschland sind derartige Fälle keine Seltenheit. naiin sah sich bereits mehrfach mit derartigen Fällen konfrontiert und rät beunruhigten Eltern, Strafanzeige gegen die Täter zu erstatten. naiin bemüht sich in solchen Fällen stets schnellstmöglichst in Zusammenarbeit mit den Chat-Betreibern die Daten der Täter zu sichern, um diese der Strafverfolgung zuzuführen.

6.5.2. Auch „Kinder-Chats" nicht sicher!

Oftmals treiben sich pädophile Nutzer in speziell für Kinder ausgewiesenen Chats herum und suchen dort ihre Opfer. Zu diesen bauen sie dann systematisch eine Beziehung auf, versuchen persönliche Daten in Erfahrung zu bringen und drängen auf ein persönliches Treffen.

Wie ernst die Lage ist, zeigte unlängst ein Ermittlungserfolg der Schweizer Polizei. Deren Beamte haben 17 homosexuelle Pädophile im Alter von 28 bis 56 Jahren, die im Juli 2002 in einem Chat-Room sexuelle Kontakte zu Jungen im Schutzalter gesucht hatten, überführt. Die Polizeibeamten gaben sich dabei als 14-Jährige aus. Die 17 Männer wurden dann an Treffpunkten in Zürich, Basel und im Kanton Zug festgenommen, wo sie ihre vermeintlichen Opfer zu sexuellen Kontakten treffen wollten.

Ein weiteres Beispiel: Ein 33-Jähriger aus dem Landkreis Nürnberger Land lernte im Sommer 2004 in einem Internet-Chatroom eine 14-Jährige aus Hamburg kennen. Er veranlasste das Mädchen, sich auszuziehen und sexuelle Handlungen an sich vorzunehmen. Ohne zu wissen, dass ihr Gegenüber diese Handlungen aufzeichnet, spielte das Mädchen bereitwillig mit. Der 33-Jährige, der zuvor bereits einschlägig in Erscheinung getreten war, verschickte den so gedrehten Film übers Internet.

Beispiel No. 2: Im Zusammenhang mit dem Mord an einem 15-jährigen Schüler aus dem Donau-Ries-Kreis hat die Polizei im August 2004 zwei Tatverdächtige festgenommen. Die aus der homosexuellen Szene stammenden Verdächtigen sollen ihr späteres Opfer via Internet kontaktiert haben.

Der 15-Jährige, der im Internet offenbar homosexuelle Bekanntschaften gesucht hatte, habe, so die Polizei, vermutlich mit seinen Mördern ein „Blind-Date" via Chat vereinbart. Die beiden Täter erstachen ihn zur „Befriedigung ihres Geschlechtstriebs".

Auch die britische Regierung hat den Ernst der Lage erkannt und initiierte eine 1,5 Millionen Pfund teure Kampagne um über Chat-Risiken aufzuklären. In Deutschland laufen derzeit ähnliche Aktionen – u.a. initiiert vom Bundesfamilienministerium und den Landesmedien-Anstalten (klicksafe.de).

6.5.3. Entwicklungen / Trends

Als Reaktion auf das Schulmassaker in Erfurt trat der Jugendmedienschutz-Staatsvertrag (JMStV) am 1. April 2003 in Kraft. Zeitgleich wurde die Kommission für Jugendmedienschutz (KJM) als Aufsichtsbehörde für den privaten Rundfunk und das Internet geschaffen. Eine wirkliche Besserung der Situation im Bereich des Jugendschutzes konnte diese Maßnahme des Gesetzgebers bislang nicht bewirken.

Es ist grundsätzlich zu bezweifeln, ob die Jugendschutz-Bestimmungen der Bundesrepublik Deutschland überhaupt je Früchte tragen werden.

Die Regelungen sind zum Teil nicht an das Medium Internet angepasst. So ist es angesichts der Globalität des Datennetzes überaus fragwürdig, Gefahren für Kinder und Jugendliche auf Ebene der Bundesländer entgegenwirken zu wollen. Zu leicht können Jugendschutzmaßnahmen durch ein simples Ausweichen auf ausländische Angebote umgangen werden. Zu leicht können sich deutsche Anbieter den hiesigen Jugendschutz-bestimmungen durch das Abwandern ins Ausland entziehen.

Das in Deutschland sehr hohe Schutzniveau im Bereich des Jugendmedienschutzes wird darüber hinaus auch internationalen Bestrebungen hinsichtlich einer staatenübergreifenden Lösung des Problems im Wege stehen. Es ist anzuraten, die deutschen Konzepte im Bereich des Jugendmedienschutzes zu überdenken. Ein „Weiter so“ und das beständige gegenseitig auf die Schulter Klopfen der deutschen Jugendmedienschützer ist dem wichtigen Anliegen des Online-Jugendschutzes nicht dienlich.

6.6. Internet-Piraterie

Der Schutz geistigen Eigentums ist in Zeiten des Internet schlichtweg eine schier unüberwindbare Aufgabe. Insbesondere für die Industrie-Zweige, die durch Verstöße gegen bestehendes Copyright weltweit Milliarden an Umsatz einbüßen müssen, ist die Bekämpfung derartiger Delikte eine große Herausforderung.

Auch der Staat, dem durch den illegalen Handel mit raubkopierter Ware ebenfalls Unmengen an Steuergeldern, die er bei den Originalen im Handel über die Mehrwertsteuern erhalten hätte, entgehen, hat ein Interesse am Schutz von Urheberrechten.

Insbesondere kleineren Unternehmen, die auf den Verkauf ihrer Produkte angewiesen sind, sind durch Software-, Musik- und Film-Piraterie oder ähnlichen Formen der Urheberrechtsverletzungen in ihrer Existenz bedroht.

6.6.1. Tauschbörsen: Die Piraten in den p2p-Netzen

Begonnen hat alles mit der Tauschbörse „Napster". Sie hatte sich schnell zu einem unüberschaubaren Umschlagplatz von u.a. raubkopierter Musik aber auch Filmen entwickelt, bis ihr die amerikanische Musikindustrie vertreten durch die „Recording Industry Association of America" (RIAA) 1999 den Kampf angesagt hat. Die Bekämpfung von „Napster" war erfolgreich, jedoch traten mehr als 130 P2P-Tauschbörsen an ihre Stelle.

Der einfache Umgang mit den p2p-Netzen macht die Tauschbörsen auch für den „normal", technisch nicht versierten Internet-Nutzer attraktiv. Da der Download von u.a. Raubkopien dadurch zum Kinderspiel wird, greifen viele Internet-Nutzer einfach kostenlos zu, statt sich ihre Wunschmusik oder -Film im Handel käuflich zu erwerben.

6.6.2. Organisierter Handel mit raubkopierten Filmen

Neben dem Tauschhandel von raubkopierten Filmen in den peer-2-peer-Netzwerken oder dem Direkt-Download von Homepages sowie FTP-Servern eröffnen sich den Filmpiraten noch viele weitere Möglichkeiten, um im Internet an billige Duplikate von Kinofilmen, die in vielen Fällen noch nicht einmal angelaufen sind, zu gelangen.

Umsatzeinbußen von bis zu 20%

Denn einige Raubkopierer betreiben im Internet ein recht profitables Geschäft mit raubkopierten Filmen, mit dem sie die Filmindustrie allein in Deutschland jährlich um schätzungsweise 20 Prozent ihres Gesamtumsatzes bringen.

Nicht nur über Auktionshäuser bieten sie ihre „heiße" Ware an, sondern auch via Spam-Mail und Homepage. Im Vorfeld fertigen sie sich Dutzende oder gleich Hunderte von Video-CDs in ihren geheimen Press-

Werken, die in Kellern oder Garagen des eigenen Hauses untergebracht sind, an, um sie dann per Post an ihre im Internet geworbenen Abnehmer zu versenden.

Herkunft der Kopiervorlagen

An die Originale gelangen die Kopierer nicht selten durch Unterstützung von Filmjournalisten, Mitarbeitern von Filmkonzernen oder Agenturen aber auch Jurymitgliedern. So kursierten bereits vor der Veröffentlichung Raubkopien des Kinofilms „Herr der Ringe – Die zwei Türme" in bester Qualität im Web. Anhand des alle 15 Minuten aufblinkenden Schriftzugs „Zu Ihrer Verwendung" konnte der Übeltäter schnell ermittelt werden: Ein Vertreter der Oscar-Jury.

Sollten derartige Kontakte jedoch nicht vorhanden sein, werden die Filmpiraten kreativ und rüsten sich für die Filmpremieren bereits mit Videokameras aus und kopieren den Kinofilm von der Leinwand. Die Qualität derartiger Aufnahmen lässt jedoch zu wünschen übrig. Nicht selten sind Köpfe oder Hände von anderen Kinobesuchern zu sehen. Experten wissen jedoch: Umso länger ein Film im Kino läuft, desto besser wird die Qualität der Raubkopien.

6.6.3. Software-Diebstahl

Nicht nur Musik und Filme werden im Internet illegal gehandelt, sondern auch Raubkopien von Software – darunter Computeranwendungen und -spiele. EU-weit verursacht diese Art des Diebstahls geistigen Eigentums einen Schaden von mehr als 12 Milliarden US-Dollar jährlich.

Und Deutschland befindet sich auf Platz 2 der europäischen Länder. Denn in der Bundesrepublik entsteht der Software-Industrie mit circa 1,9 Milliarden US-Dollar der zweithöchste Schaden innerhalb Europas. Frankreich führt das Ranking in der EU an. Die EU rangiert im weltweiten Vergleich auf Platz 1 – noch vor Asien. Damit übertrifft der Staatenbund selbst die Vereinigten Staaten um einiges.

6.6.4. Entwicklungen / Trends

Nicht nur der Skandal um den aggressiven XCP-Kopierschutz auf den Musik-CDs des Labels Sony BMG sowie die Enthüllungen von fragwürdigen Fahndungsmethoden der „Gesellschaft für Urheberrechtsverletzungen" (GVU) führen die Bemühungen der Musik- und Filmbranche im Kampf gegen Raubkopien ad absurdum. Auch eine Beschneidung des Rechts auf Privatkopie wird wohl eher als Angriff auf die zahlende Kundschaft gesehen werden.

Trotzreaktionen, die zu einem weiteren Anstieg von Piraterie im Internet führen werden, sind die Folge. Die jüngsten Pannen der Musik- und Film-

branche im Kampf gegen die Internet-Piraterie schüren Unverständnis bei den Verbrauchern für die Rechte der Urheber. Dies kann nicht im Interesse der Rechteinhaber sein.

Der Erfolg groß angelegter Aufklärungskampagnen ist zudem in Frage zu stellen. Die Nutzer wissen zwar aufgrund der Kampagnen, wie es um die Rechtslage hinsichtlich der Raubkopien bestellt ist, nehmen illegale Angebote aber weiterhin in Anspruch. Auch die Tatsache, dass viele legale Online-Angebote noch unzureichend sind, begünstigt die weitere Entwicklung im Bereich der Internet-Piraterie.

Viele Online-Music-Stores, die seitens der Wirtschaft viel zu spät als legale Alternative zum illegalen Download errichtet wurden, weisen noch heute erhebliche Mängel bei der Angebotsvielfalt oder den technischen Spezifikationen der käuflichen Dateien auf.

Hinweis

Diesen Bericht finden Sie online unter www.naiin.org/de. Dort können Sie auch die Mitgliedschaft bei naiin beantragen, unseren Newsletter abonnieren oder sich in unseren Presse-Verteiler eintragen. Engagieren Sie sich für / bei naiin und helfen Sie uns, das Internet sicherer zu machen. Sagen auch Sie: Ja zu naiin!

Kontakt

naiin – no abuse in internet e.V.
Einsteinpalais
Friedrichstraße 171
D-10117 Berlin

Tel.: 030 / 46 999 37 58
Fax: 030 / 46 999 37 59
E-Mail: info@naiin.org
Web: www.naiin.org

Kontakt für die Presse:

Tel.: 02266 / 44 000 91
E-Mail: presse@naiin.org
Weitere Informationen finden Sie online in unserem Presse-Center.

Impressum

Herausgeber: naiin – no abuse in internet e.V.
Einsteinpalais
Friedrichstraße 171
D-10117 Berlin

Autor: Dennis Grabowski

Hinweis: Dieser Tätigkeitsbericht ist auch über das Internet abrufbar: www.naiin.org

Druck: impress media GmbH
Mönchengladbach
www.impress-media.de