Expertengespräch der Enquete-Kommission Internet und digitale Gesellschaft zum Thema „Sicherheit im Netz“ am 28.11.2011

Erster Kriminalhauptkommissar Mirko Manske
Sachgebietsleiter des Bereiches der Operativen Auswertung Cybercrime
Bundeskriminalamt

Frage 1

Welche Straftaten werden typischerweise durch das oder im Internet begangen und welche statistischen Aussagen über die Entwicklung der Kriminalität können über diese Tatbestände (seit ihrem Inkrafttreten bzw. ihrer statistischen Erfassung) getroffen werden?

Der im allgemeinen Sprachgebrauch als „Internetkriminalität“ bezeichnete kriminelle Aktivitätsraum ist ein weites Feld. Zum einen sehen wir die „konventionellen“ und bereits seit vielen Jahrzehnten bekannten Modi Operandi, vornehmlich aus dem Betrugsbereich, bei dem die potentiellen Opfer heute etwa nicht mehr mittels postalischer Sendungen aus Afrika oder Spanien, sondern via E-Mail aufgefordert werden, Vorauszahlungen für seitens der Betrüger in Aussicht gestellte Erbschafts- oder Lotteriegewinnzahlungen in Millionenhöhe zu leisten. Hier nutzen die Täter die heute vorhandene technische Infrastruktur für ihre Zwecke – die Straftaten dahinter haben sich aber nicht wesentlich geändert. Das Internet ermöglicht es den Kriminellen heute jedoch, schneller und interaktiver mit ihren potentiellen Opfern zu kommunizieren und mit wenig Aufwand Webseiten scheinbar legitimer Firmen, Lotteriegesellschaften oder Anwaltskanzleien aufzubauen und in ihrem Sinne für das Social Engineering ihrer Opfer zu nutzen. Derartige Straftaten, und dazu gehören auch die „normalen“ Betrugsstraftaten im Online- oder Auktionshaushandel, bei denen nach Vorauskasse keine, minderwertige oder gefälschte Ware versandt wird, werden aus Sicht der Strafverfolgungsbehörden als „Cybercrime im weiteren Sinne“ verstanden – und sind in der Polizeilichen Kriminalstatistik (PKS) in aller Regel an dem Merker „Tatmittel Internet“ zu erkennen. Dieser ist jedoch nicht plausibilisiert und wird durch den Sachbearbeiter immer dann gesetzt, wenn in dem zugrundeliegenden Ermittlungsverfahren das Internet in irgendeiner Weise eine Rolle gespielt hat – so trägt zum Beispiel auch ein Tötungsdelikt den Merker „Tatmittel Internet“, wenn Täter und Opfer über das Internet kommuniziert haben.

In Abgrenzung dazu betrachten die Strafverfolgungsbehörden die Straftaten, die erst durch das Internet selbst ermöglicht wurden oder sich gegen das Internet selbst richten. Diese „qualifizierte Cybercrime“ sehen wir aktuell in den unterschiedlichsten Erscheinungsformen vom heute meist trojanerbasiertem digitalen Identitätsdiebstahl in jedweder Ausprägung, über das Einbrechen und den unberechtigten Zugriff auf gesicherte Systeme mit nachgelagertem Diebstahl dort vorhandener Daten bis hin zu digitaler Schutzgelderpressung, bei der Webseiten zunächst mittels DDoS-Angriffen für eine bestimmte Zeit lahmgelegt und die Inhaber sich dann kurze Zeit später finanzieller Forderungen der Täterseite zur Verhinderung erneuter Angriffe ausgesetzt sehen. Aber auch Echtzeitangriffe auf Onlinebanking-Vorgänge, die Manipulation von Wertpapierkursen mittels übernommener Aktiendepots oder – wie ganz aktuell Schadsoftwarebasierte Angriffe auf die neue

Generation der „smarten“ Mobilfunktelefone sowie malwarebasierte Attacken auf konkurrierende Unternehmen im Bereich der Wirtschaft gehören dazu.

Die einschlägigen Strafrechtsnormen sind im Bereich der „Datendelikte“ zu finden, also dem Ausspähen und Abfangen von Daten inklusive der Vorbereitungshandlungen (§202a-c, StGB), der Veränderung von Daten (§303a StGB), der Computersabotage (§303b StGB), des Computerbetrugs (§263a StGB) aber auch der Geldwäsche (§261a StGB) – zumeist in der gewerbs- oder bandenmäßig qualifizierten Begehungsform.

Im Jahr 2010 weist die PKS insgesamt 246.607 erfasste Straftaten mit dem Merker „Tatmittel Internet“ aus – eine Steigerung von annähernd 20% im Vergleich zum Vorjahr. Qualifizierte Cybercrime wurde in 2010 mit 59.839 Straftaten (gegenüber 50.254 in 2009) und damit einer Steigerung von 19% erfasst. Allerdings sind diese Zahlen – wie alle PKS-Zahlen im Bereich der Cybercrime – nicht hinreichend aussagekräftig. Dies ist zum einen auf ein nach Einschätzung des BKA in diesem Phänomenbereich sehr großes Dunkelfeld zurückzuführen, da die überwiegende Anzahl der Straftaten durch das Opfer gar nicht bemerkt bzw. nicht bei den Strafverfolgungsbehörden angezeigt wird. Zum anderen können die Zahlen der PKS dem Phänomen nicht gerecht werden, da die PKS grundsätzlich Einzelstraftaten abbildet, ein Großteil der im Phänomenbereich Cybercrime einschlägigen Modi Operandi jedoch die Verkettung verschiedenster Straftaten darstellen. Dies lässt sich sehr anschaulich anhand eines Phishing-Angriffs auf einen Onlinebankingkunden darstellen: Nach der Datenveränderung (Einbringen des Trojaners) und dem Ausspähen von Daten (Abgreifen der Zugangsdaten) folgt dann schließlich die Manipulation der Transaktionsdaten (Computerbetrug) und die Umleitung der Überweisung auf das Konto eines sogenannten Finanzagenten (Geldwäsche). Je nach Sachbearbeiter wird hier eines der Delikte (meist der Computerbetrug oder die Geldwäsche) als – für die PKS – relevant deklariert – der Modus Operandi an sich kann jedoch nicht erfasst werden.

Festzuhalten bleibt, dass der vorstehend durch die PKS skizzierte stetige Aufwärtstrend von zuletzt etwa 20% jährlicher Steigerung im Bereich der Cybercrime durch die Auswertung des Schriftverkehrsaufkommens zwischen BKA und den Polizeidienststellen der Bundesländer bestätigt werden kann. Die Anzahl der durch die Bundesländer im Rahmen des polizeilichen Informationsaustauschs (Kriminalpolizeilicher Meldedienst, KPMD) an das BKA in 2011 gemeldeten Vorgänge wird nach momentanem Trend mehr als verdoppelt gegenüber den Eingängen des Jahres 2010. Unserer Einschätzung nach werden sich mit der weiter fortschreitenden Technisierung der Gesellschaft auch in den kommenden Jahren immer mehr Erscheinungsformen von Kriminalität ins Internet verlagern oder dort entstehen – und das hat vor allem auch mit dem für die Täter deutlich geringeren Entdeckungsrisiko im Internet zu tun.

Es sollten jedoch noch kurz die handelnden Personen, also Täter und Opfer beleuchtet werden. Dabei ist festzustellen, dass auch die im Phänomenbereich aktiven Täter einen weiten Bogen spannen. Wir sehen Jugendliche, teilweise sogar noch Kinder, die mit erheblichem technischen Verstand und beeindruckender Begabung gepaart mit einer großen Portion Neugier und teilweise auch krimineller Energie Trojaner und andere Schadsoftware konzipieren, entwickeln und einsetzen – häufig zunächst nur, um innerhalb der Szene an Ansehen, an „Standing“, zu gewinnen.

Das entgegen gesetzte Ende dieser Skala wird durch den hochkriminellen Intensivtäter beschrieben, der das Internet als allumfassenden Aktionsraum jedweder (meist mit unmittelbarer Vermögensrelevanz) strafrechtlich relevanter Aktivitäten begreift. Und gerade hier stellen wir in den letzten Jahren eine weiter zunehmende Professionalisierung und ein stetig ausgebautes arbeitsteiliges Vorgehen fest.

Lag in den Jahren 2006-2008 zum Beispiel im Bereich des Phishings zum Nachteil von Onlinebankingkunden noch der gesamte Tatstrang (Beschaffen der Malware, Infektion der Opfer-PC, Rekrutieren und Führen der Finanzagenten, Manipulation der Transaktionen, Aussteuern der Gelder ins Ausland, Rückfluss nach Deutschland oder in andere Staaten in Form von anonymisierten Zahlungsmitteln) im wesentlichen in der Hand einer Tätergruppierung („Modell ‚von der Wiege bis zur Bahre'"), so sehen wir heute verschiedene, von einander losgelöste Tätergruppierungen, die einzelne Bausteine für mehrere, unterschiedliche Täter(gruppen) als buchbare Dienstleistung anbieten.

Dabei ist es dem kriminellen Dienstleister, der z.B. Finanz- und Warenagenten bereitstellt, egal, für welche Phishing- oder Cardinggruppierung er seine Dienstleistung erbringt. Teilweise werden die gleichen Finanz- oder Warenagenten auch unterschiedlichen Tätergruppierungen zeitgleich oder in engem zeitlichem Zusammenhang angeboten.

Die verschiedenen Täter oder Tätergruppierungen kennen sich nicht persönlich und kommunizieren in aller Regel über anonymisierte Kommunikationswege (ICQ, Skype, Jabber), die retrograd so gut wie keine und im Zuge von Echtzeitmaßnahmen auch nur sehr eingeschränkt erfolgsträchtige Ermittlungen ermöglichen. Die Cyberkriminellen von heute sind auf einem globalen Markt angekommen, auf dem Daten, Tatmittel und Infrastruktur weltumspannend gehandelt werden. Die Währungen, in denen diese Geschäfte legalisiert werden sind webmoney, liberty reserve, ukash und auf Zypern emittierte und anonym ausgegebene PrePaid Kreditkarten von VISA und MasterCard.

Dieser globale Markt und die durch ihn bestehende Möglichkeit, sich die zur Tatbegehung notwendigen Mittel bei unterschiedlichsten Anbietern zu verschaffen, ermöglichen stetig wechselnde Konstellationen bei den Tatbegehungen. Die Gruppierungen von heute sind in Netzwerken zusammengeschlossen und dabei annähernd gleichberechtigt. Geliefert wird, was bestellt und bezahlt wird, der schlussendliche Verwendungszweck des gelieferten Guts spielt dabei für die Dienstleister keine wesentliche Rolle mehr.

Hier zeigen sich Vorboten einer aus unserer Sicht zu erwartenden dramatischen Entwicklung, die sich wie folgt darstellen könnte:

a) Vollständiger Verlust der digitalen Identität von Internetnutzern aufgrund der immer weiter zunehmenden Infektion der mit dem Internet verbundenen Endgeräte

b) Sukzessive Erschließung/Entwicklung neuer Verwertungsmechanismen in Abhängigkeit von den beim Opfer abgegriffenen Arten digitaler Identitäten

c) Weitergehender Ausbau der bestehenden Trojanerfunktionalitäten um Angriffsmethoden für neue Sicherungsverfahren im Online-Kreditkartengeschäft (zum Beispiel auf das 3DSecure-

Verfahren als Sammelbegriff für MasterCard's SecureCode und „Verified by VISA“).

d) Adaption bestehender krimineller Infrastrukturen auf neue Verwertungsmodelle und neue Opfermärkte sowie

e) weitergehender Ausbau und Perfektionierung der Social Engineering Methoden

Auch die Opferstrukturen sind von großer Diversität geprägt. Die Bandbreite reicht vom unbedarften Internetnutzer, der seinen Rechner aus dem Karton des Discounters nimmt und direkt an das Internet anschließt bis zu aufwändig gesicherten Industrie- und Sicherheitseinrichtungen. Mit Blick in die Zukunft wird hier sicherlich auch die Tatsache bedeutsam, dass insbesondere die Internetnutzung durch ältere Menschen nach wie vor stark zunimmt. Im Jahr 2010 nutzten 65% der 55-64-jährigen und 41% der 65-74jährigen das Internet.

Gerade mit diesen lebensälteren Usern drängen eine Vielzahl von sogenannten „Newbies“, von unerfahrenen aber mit viel Neugier, Zeit und vor allem in aller Regel nicht unerheblichem finanziellen Potenzial ausgestatteten Usern in das Internet, ohne dabei jedoch ausreichend über die Risiken des Webs und der modernen Technologie informiert und aufgeklärt zu sein.

Frage 2

Welche Schwierigkeiten und welche neuen Möglichkeiten ergeben sich bei der Sicherstellung von Beweismitteln zur Verfolgung von Straftaten, die typischerweise durch das oder im Internet begangen werden (verglichen mit anderen Ermittlungsverfahren)?

Die Internationalität des Internets, sein in ihm selbst liegender grundsätzlich globaler und netzwerkartiger Ansatz ist vermutlich der größte Schutzfaktor, den die heute im Phänomenbereich der Cybercrime aktiven Täter gezielt ausnutzen. Im Bereich der Cybercrime gibt es heute kaum noch Ermittlungsverfahren, die nur mittels nationaler Aktivitäten und Informationsquellen erfolgreich geführt werden können. Auslandsermittlungen – und sei es nur die Anfrage bei einem ausländischen Internetserviceprovider oder Zahlungsdienstleister zu IP-Logs und Verbindungsdaten – sind an der Tagesordnung und bedingen in aller Regel justizielle Rechtshilfeersuchen, die (wenn sie denn gestellt werden) den Ermittlern die benötigten Informationen nur mit erheblichen Zeitverzögerungen zur Verfügung stellen.

Dieser Zeitverzug ist insbesondere vor dem Hintergrund der Flüchtigkeit der Daten und der nicht mehr gegebenen Mindestspeicherungsfristen eines der entscheidenden Probleme bei der Bekämpfung der internationalen Cybercrime: Bis das BKA in den USA eine tatrelevante IP-Adresse zum Beispiel zu einem LogIn in ein kompromittiertes E-Mail-Konto erhalten hat, kann diese in Deutschland durch den zuständigen Provider keinem Anschluss mehr zugeordnet werden – weitere Ermittlungen sind damit häufig ebenfalls unmöglich.

Dies ist umso kritischer zu bewerten, als es dem BKA damit nicht möglich ist, hunderttausende Opfer von Straftaten, deren Rechner mit Trojanern oder Botsoftware infiziert sind und die jeden

Tag einen weiteren Teil ihrer digitalen Identität verlieren, zu informieren und dafür zu sorgen, dass ihre Rechner bereinigt und ihre Passwörter gewechselt werden. So wurden dem BKA im April 2010 durch Interpol Luxemburg etwa 230.000 deutscher IP-Adressen von mit Schadsoftware infizierten Systemen mitgeteilt, die sich zu einem in Luxemburg befindlichen Steuerungsserver verbunden hatten. Die Zeitstempel der übermittelten IP-Adressen stammten aus dem November des Jahres 2009. Keines der Opfersysteme konnte mehr identifiziert werden.

Auch die fortschreitende Anonymisierung im Internet macht es den Strafverfolgungsbehörden heute oftmals unmöglich, Täter und Tatorte zu entdecken und somit die Orte zu finden, an denen weitere, beweisrelevante Daten gesichert und damit objektive Tatbeweise erhoben werden können. VPN-Dienstleister, durch Kriminelle übernommene Endkonsumenten-PC, die als Proxies missbraucht werden sowie Anonymisierungsdienste wie TOR oder Anonymouse machen es den Strafverfolgungsbehörden zusätzlich schwer, etwaig gefundene Tat-Täter-Zusammenhänge zu verifizieren und zu personalisieren.

Die für die im Rahmen der Beweissicherung zwingend notwendigen forensischen Spezial-dienststellen sind ob der schnell um sich greifenden Relevanz des Internet für immer mehr Phänomenbereiche – insbesondere auch im Bereich des polizeilichen Staatsschutzes – zunehmend überlastet. Gleichzeitig nimmt das Volumen der auf den Rechnern von Beschuldigten und damit im Rahmen der Asservatenauswertung zwingend zu sichtenden gespeicherten Daten ständig zu.

Hierin liegt gleichwohl auch ein gewisser Vorteil für die Strafverfolgungsbehörden: Beweismittel liegen häufig in einer komprimierten Form vor und sind, wenn sie denn gefunden werden und lesbar sind, in aller Regel beweiskräftig dokumentiert und unmittelbar aussagekräftig. Als weiteren Vorteil, den das Internet für die Polizei mit sich gebracht hat, sind die heute bestehende Möglichkeiten der OpenSource-Abklärungen und Ermittlungen zu nennen. Über diese Instrumentarien bieten sich heute Ermittlungsmöglichkeiten und Informationsgewinne, die früher nicht in der Form realisiert werden hätten können.

Polizei, Forschung, Dienstleister, Handel, Banken – die Gesellschaft an sich ist auf dem Weg in eine neue Zeit. Diese neue Zeit wird bestimmt werden, durch die immer stärker werdende Notwendigkeit, Ressourcen der verschiedenen Player über die Grenzen zwischen Staat, Forschung und Wirtschaft hinaus zu bündeln. Das Bundeskriminalamt ist aktuell dabei, diesbezüglich mit der Einrichtung einer Nationalen Kontaktstelle Cybercrime-Bekämpfung (institutionalisiertes Public Private Partnership) einen Beitrag zu leisten. Diese sieht vor, dass die Hauptakteure der Internetwirtschaft bzw. der Wirtschaftszweige, deren Geschäftsmodelle ganz oder erheblich von der Funktionsfähigkeit, der Verfügbarkeit und der Integrität des Internets abhängen, wie z.B. Provider, Logistikunternehmen, Versicherer, Banken etc. eine Non-Profit-Einrichtung bilden, in der Verfahren, Techniken und Standards gemeinsam entwickelt werden, die dazu beitragen, dass das Internet als Wirtschafts- aber auch als gesellschaftlicher Raum möglichst frei von Kriminalität und Organisierter Kriminalität erhalten bleibt.

Frage 3

Welche Schwierigkeiten und welche neuen Möglichkeiten ergeben sich bei der Verfolgung von Straftaten, die typischerweise durch das oder im Internet begangen werden und bei denen deutsche Ermittlungsbehörden mit Behörden im Ausland zusammenarbeiten?

Wie vorstehend bereits dargelegt, bedingen fast alle Fälle der Cybercrime heute Ermittlungen im Ausland und damit sehr häufig (wenn auch nicht immer) justizielle Rechtshilfeersuchen. Die durch das BKA sowie Dienststellen der Bundesländer in der Vergangenheit gestellten außereuropäischen Rechtshilfeersuchen, insbesondere in die USA, wohin aufgrund der technischen Gegebenheiten des Internets ein besonders starker Bezug gegeben ist, aber auch in die Ukraine und die Russische Föderation, wo häufig Täterspuren zu finden sind, haben im günstigsten Falle eine Laufzeit von wenigstens drei Monaten gezeigt.

Die so erlangten Daten sind dann, wenn sie schließlich bei der ermittlungsführenden Dienststelle in Deutschland angekommen sind, in aller Regel bereits inaktuell und „kalt".
Als weiterer Problempunkt sind zweifelsohne auch die unterschiedlichen Rechtssysteme der verschiedenen, regelmäßig von Ermittlungen und damit auch Rechtshilfemaßnahmen betroffenen Staaten insbesondere im Bereich Cybercrime-naher Delikte zu nennen. Insbesondere im Bereich des Ausspähens von Daten und dessen Vorbereitung (zum Beispiel durch die Programmierung von Schadsoftware) sind zwischen West- und Osteuropa erhebliche Unterschiede in der Strafbarkeit etwaiger Täterhandlungen festzustellen. Aber auch stark differierende Speicherfristen ermöglichen effiziente und erfolgreiche Ermittlungen im Ausland häufig nur unter erheblichen Einschränkungen und Schwierigkeiten.

Als Vorteil der schon fast zwingenden internationalen Ermittlungen im Phänomenbereich Cybercrime kann angeführt werden, dass immer mehr in der Verfolgung der Cybercrime involvierte und aktive Staaten erkennen, dass neue Arten der Zusammenarbeit, die effektiver und vor allem schneller als der klassische Weg über die Interpol-Zentralstellen sind, gefunden werden müssen. Diese Erkenntnis hat über die vergangenen fünf Jahre beim BKA zum Aufbau eines mittlerweile weltweiten Netzwerkes von im Phänomenbereich der Cybercrime eingesetzten Spezialisten geführt – Kollegen in Washington, Pittsburgh, Seoul, Bangkok, Kiew, Moskau oder Riga, zu denen persönliche Kontakte bestehen, sind nur noch einen Telefonanruf oder Jabber-Chat entfernt. Diese Kontakte tragen und ermöglichen es immer wieder auch, die Widrigkeiten der verschiedenen Rechtssysteme und der zwingenden Rechtshilfemaßnahmen im Rahmen des rechtlich Möglichen zu minimieren. Gegenseitige Hospitationen und gemeinsame Taskforces sind dabei ein weiterer Ausdruck der in den vergangenen Jahren deutlich gestiegenen internationalen Kooperationen – und gleichzeitig auch der wachsenden Bedeutung, die das Thema Cybercrime in einer Vielzahl von Staaten heute einnimmt.

Gerade in diesem Kontext ist das unter den Unterzeichnern der „Convention on Cybercrime" akzeptierte und gegenseitig zugesicherte Instrument der Vorabsicherung, der sogenannten Preservation Order, als erfolgskritisch hervorzuheben. Die Datenvorabsicherungen versetzen einen anfragenden Staat in die Lage, im Ausland befindliche technische Beweismittel (z.B. ein E-Mail-Postfach, einen Server oder einen kompromittierten Rechner) durch die im Zielland zuständigen

Behörden über eine Verpflichtung des jeweiligen Providers ohne bereits vorliegendes Rechtshilfeersuchen sichern zu lassen und damit in einem sehr tatnahen Zustand vor weiterer Veränderung zu schützen. Dadurch wird der ersuchende Staat in die Lage versetzt, die Daten auch nach mehreren Monaten im Rahmen der Rechtshilfe in dem Zustand für das nationale Verfahren zu erheben, wie sie im Moment der erkannten Beweisrelevanz vorlagen. Diese Methode ist jedoch nicht geeignet, die aus der Rechtshilfe resultierenden Zeitverluste zu kompensieren, da eine Nutzung der Daten zu weiteren Ermittlungsschritten auch in diesen Fällen erst nach Erledigung der Rechshilfe möglich ist. – Gleichwohl ist sie ein wirksames Instrument, einer Veränderung / Löschung von Beweismitteln durch Täter oder auch Dritte entgegenzuwirken. In der Bundesrepublik Deutschland ist dieses Instrument, obgleich die „Convention on Cybercrime“ unterzeichnet und auch ratifiziert worden ist, bisher nicht in nationales Recht umgesetzt worden.