Mögliche Fragestellungen zum Thema "Internetüberwachung" im Verfahren Mohamed M.[1]

[Vorbemerkung: Die Fragestellungen ergaben sich aus der Beobachtung der ersten drei Tage des Hauptverfahrens 3.,5.,6.3.08, insbesondere in Hinblick auf die Ausführungen des Beamten der SEO, der BVT und des Rechtsschutzbeauftragten und ohne Kenntnis der Akten und bisherigen Erhebungsmaterialien.]

Themenkreis: Internet-Überwachung bei ISP (Chello)

[Vorbemerkung: Der Internetverkehr wird durch sogenannte Datenpakete abgewickelt, die jeweils Sende- und Empfangs-IP-Adresse enthalten. Alle Datenpakete der verschiedensten Benutzer werden dabei über dieselbe Datenleitung geschickt. Um die Aufzeichnung des Datenverkehrs eines Benutzers zu erhalten, werden aus dem Gesamtdatenstrom die Daten bestimmter IP-Adressen gefiltert.]

- Erfolgte die Aufzeichnung des Internetverkehrs (der übertragenen Datenpakete) lückenlos oder besteht die Möglichkeit, dass einzelne Datenpakete verloren gingen bzw. nicht vollständig aufgezeichnet wurden?
- Wenn ja: Aus welchen Gründen kam es zu den Lücken (technische, organisatorische, ...)? Entstanden auf Grund dieser fehlenden Datenpakete Lücken in den Aufzeichnungen, die bei der vorgelegten Internetkommunikation (Chats, Mailverkehr, Internettelefonie, Forumseinträge) zu Fehlinterpretationen führen können (etwa bei Chats welcher Teilnehmer nun tatsächlich welchen Beitrag lieferte)?
- Wenn nein: Welche technischen Hinweise lassen erkennen, dass eine vollständige Aufzeichnung vorliegt? Mit welchen Maßnahmen wurde die Vollständigkeit der Aufzeichnung sichergestellt?

- Gibt es Hinweise bei der Datenaufzeichnung, dass auf Grund technischer Fehlfunktionen, Konfigurationsmängel oder sonstiger Gegebenheiten auch Datenpakete anderer Internetnutzer in die Aufzeichnung ganz oder teilweise übernommen wurden?
- Wenn ja: Welche Auswirkungen haben diese Datenpakete auf den Inhalt (Interpretierbarkeit) der Kommunikation des Angeklagten?

[Hintergrund der Fragestellung: aus technischer Sicht ist es ein durchaus häufiges Phänomen, dass Router oder vergleichbare Übertragungs- und Kopiereinrichtungen einzelne Datenpakete aus Kapazitätsgründen verlieren oder auch falsch gefiltert werden (Buffer Overflow). Dies kann, muss aber nicht, Auswirkungen auf die Verständlichkeit und den Inhalt der Datenpakete haben.]

- Welche der im Zusammenhang mit den Videos, Texten (u.a. "Testament", ...) und sonstigen Beiträgen wurden vom Angeklagten bloß downgeloadet? Welche Beiträge von ihm upgeloadet?
- Welche der upgeloadeten Beiträge wurden bloß im Rahmen privater Kommunikation (an einen einzelnen Empfänger) übertragen, welche an eine unbestimmte Zahl (veröffentlicht)?

1 Text siehe auch: **ftp://ftp.freenet.at/int/fragestellungen-prozess.pdf**

[Hintergrund: download=Datei aus Internet beziehen, upload=Datei über das Internet verbreiten, Unterschied, ob jemand extremistische Informationen konsumiert oder auch verbreitet hat]

THEMENKREIS: ONLINEÜBERWACHUNG DES COMPUTERS

- Erfolgte die Durchführung/Übertragung der Screenshots lückenlos (also regelmäßig alle 60 Sekunden) oder gab es Unterbrechungen?
- Wenn Unterbrechungen: Wie lange dauerten die Unterbrechungen und was waren ihre Ursache? Lassen sich für diese Unterbrechungen Rückschlüsse auf die Internet-Aktivitäten des Angeklagten ziehen? Welche Rückschlüsse?

- Wurde im Überwachungszeitraum das Abspielen der so genannten "Tötungsvideos" festgestellt? Gibt es dazu Screenshots? Wurde das Abspielen sonstiger Videos festgestellt? Wurden diese Videos vollständig angesehen oder nur Teile? Wenn nur Teile, welche Teile?

[Hintergrund: Bisher scheint noch nicht ausreichend geklärt in welchem Umfang sich der angeklagte tatsächlich mit Propagandainhalten beschäftigt hat. Erfahrungen mit anderen Downloadern, etwa im Zusammenhang mit Musikdateien zeigen immer wieder, dass viele Internetnutzer ein vielfaches von dem downloaden, was sie sich tatsächlich ansehen.]

- Ist bei den Screenshots sicher gestellt, dass sie tatsächlich nur vom Computer des Angeklagten stammen? Mit welchen technischen Verfahren wurde das sicher gestellt?

[Hintergrund: Da der Manipulationsverdacht im Raum steht und Screenshots auch von beliebigen anderen Computern angefertigt werden können oder auch nachträglich verändert werden können, müssen entsprechende Zweifel ausgeräumt werden.]

- Wurden Teile des Textes (Euro2008/"Anschlagstext") downgeloadet oder wurde der gesamte Text vom Angeklagten erstellt?

- Lässt sich auf Grund der Tastaturanschläge/Screenshoots zweifelsfrei erkennen, dass bestimmte Texte, insbesondere der Text zur Euro2008 ("Anschläge") tatsächlich vom Angeklagten verschickt wurde?
- Wenn ja: Was wurde genau an wen verschickt?
- Wenn nein: Gibt es Hinweise, was mit dem Text tatsächlich passierte? Wurde er abgespeichert, wurde er gelöscht?

- Gibt es Hinweise, dass auf Grund von Computerabstürzen Texte, die mittels Screenshot/Tatstaturanschläge aufgezeichnet wurden, verloren gingen, vom Angeklagten nicht nochmals rekonstruiert wurden und daher nicht weiter vom Angeklagten verwertet wurden?

[Hintergrund: das vom Angeklagten verwendete Betriebssystem Windows XP ist relativ fehleranfällig und kann auch immer wieder abstürzen. Es ist denkbar, dass Entwürfe und Notizen, die vom Überwachungsprogramm zwar erfasst wurden, jedoch zu keinem Zeitpunkt tatsächlich verwendet/verwertet wurden.]

THEMENKREIS: BESCHLAGNAHMTER COMPUTER

FORENSISCHE VORGANGSWEISE / DATENSICHERUNG

- Welche Maßnahmen wurden gesetzt, um eine vollständige Datensicherung des Computers zu gewährleisten? Entsprechen diese Maßnahmen dem Stand der Technik?

- Welche Maßnahmen wurden gesetzt um bei späteren Auswertungen die vorsätzliche oder unabsichtliche Veränderung von Daten des beschlagnahmten Gerätes zu verhindern? Entsprechen diese Maßnahmen dem Stand der Technik?

[Hintergrund: Der Manipulationsverdacht könnte bei ausreichend sorgfältiger Vorgangsweise der Ermittlungsbeamten weitgehend ausgeräumt werden.]

- War der Computer zum Zeitpunkt der Beschlagnahme in Betrieb?
- Wenn ja: Welche Maßnahmen wurden gesetzt, um auch vom Arbeitsspeicher / von den laufenden Programmen ein getreues Abbild zu sichern?

[Hintergrund: Im Verfahren wurde bisher nicht ausreichend thematisiert, ob der Computer des Angeklagten freiwillig oder unfreiwillig als Server- bzw. Relay-Station für Dritte diente -> siehe unten. Wird ein laufender Computer beschlagnahmt, ist dass der bei weitem beste Zeitpunkt, Wirtsprogramme mit derartiger Funktionalität zu identifizieren.]

- Welche Update-Version hatte das Betriebssystem des beschlagnahmten Computers? Entsprach der Zustand der aktuellen Microsoft-XP-Version (war also der Computer auf dem letzten Aktualisierungsstand)?
- Wenn nein: Welche bekannte Sicherheitslücken waren auf dem Computer vorhanden? Gab es Schutzvorkehrungen gegen diese Sicherheitslücken? Gibt es Hinweise, dass diese Sicherheitslücken von irgendwelchen Programmen genutzt wurden?

[Hintergrund: Verspätete Updates / bekannte Sicherheitslücken sind beliebte Angriffsziele für Bot-Net-Betreiber, dass sind Einrichtungen, die fremde Rechner unter ihre Kontrolle bringen. Die bisherigen Ausführungen haben nicht ausgeschlossen, dass der Computer des Angeklagten mit oder ohne sein Wissen als Relay-Station von Dritten genutzt wurde -> siehe unten]

BEURTEILUNG DER ABGESPEICHERTEN DATEIEN / DOWN- UND UPLOAD VON DATEIEN

- In welchen Bereichen des Dateisystems wurden die verschiedenen anklagerelevanten Dateien, insbesondere von Texten, Bildern, Videos und Tondokumenten gefunden?
- Sind es Bereiche, die von Programmen automatisiert angelegt/verwaltet werden (z.B.: "Temporary Internet Files", ...) oder die der Benutzer selbst anlegen musste bzw. die er selbst kontrolliert?
- In welchem Verhältnis (mengenmäßig / inhaltlich) stehen die automatisiert angelegten Dateien und die bewusst gespeicherten Dateien?

[Hintergrund: Um etwa eine Webseite mit Bildern betrachten zu können, müssen zuerst alle Bilder als Dateien downgeloadet werden und werden - abhängig vom verwendeten Browser - automatisiert in Verzeichnisse gelegt. Bei Microsoft

Internet Explorer, den auch der Angeklagte verwendete, ist es u.a. "C:\Dokumente und Einstellungen*username*\Lokale Einstellungen\Temporary Internet Files" Da ein Internetnutzer den Inhalt einer Seite vor Betrachten nicht kennt, kann aus der Existenz derartiger Dateien keinesfalls geschlossen werden, dass man sich mit den Inhalt der Dateien identifiziert. Die meisten Internetnutzer kennen diese Dateibereiche ihres Computers nur unzureichend, sodass derartige Dateien auch noch lange nach dem Seitenaufruf vorhanden sind. Ein Rückschluss, dass man sich deswegen mit dem Inhalt identifiziert wäre unzulässig. Will jemand bewusst eine entsprechende Datei aufbewahren, legt er einen eigenen Ordner an oder er verwendet Ordner wie "C:\My Documents", "C:\Dokumente und Einstellungen*username*\Eigene Dateien\Eigene Bilder" usw. Zur Beurteilung, ob sich der Angeklagte mit entsprechenden Inhalten überhaupt beschäftigt hat bzw. damit identifiziert hat, ist es unerlässlich zwischen diesen beiden Speicherarten zu unterscheiden. Das bloße vorhanden sein von Dateien auf dem Computer ist nicht ausreichend.
Gleiches gilt für die Videos. Diese werden meist in sogenannten downloadbaren Formaten ".wmv" oder ".flv" bereit gestellt. Das heißt die Videos müssen downgeloadet werden, bevor sie angesehen werden bzw. sie werden downgeloadet, auch wenn sie nicht vollständig angesehen werden. Das Vorhandensein von Videos auf der Festplatte bedeutet somit nicht automatisch, dass sie auch angesehen wurden.]

- Welche der Dateien wurden vom Angeklagten downgeloadet, welche von ihm selbst erzeugt bzw. auch tatsächlich upgeloadet (verbreitet)?

[Hintergrund: Nur bei den vom Angeklagten verbreiteten Dateien wird man von einer (Mit-)Beteiligung an Delikten sprechen können.]

Server- und Relayinstallationen am Computer

- Haben sich auf dem beschlagnahmten Gerät Hinweise auf Installationen von Server- und Relaydiensten gefunden? Eventuell frühere Installationen die zum Zeitpunkt nicht mehr aktiv waren?
- Wenn ja: Welche Installationen? Welche Funktionalität haben diese Dienste? In welchem Ausmaß wurden sie verwendet? Welche Auswirkungen haben Sie auf die Onlineüberwachung (Screenshots/Tatstatureingaben)? Welche Auswirkungen haben Sie auf auf den Internetverkehr (bzw. dessen Aufzeichnungen)? Gibt es Hinweise, dass die Installation vom Angeklagten erfolgte oder durch Dritte (etwa automatisierte Installationen im Rahmen eines Wurms/Virus oder eines anderen Schadprogrammes)? Gibt es Hinweise auf Installationen / Installationsversuche von Außen ("Hacker")?

[Hintergrund: In Frage kommen u.A. Webserver, Mailserver, Chatserver, Anonymisierungsserver, ftp-Server, ... Es ist für kriminelle Internet-Aktivitäten eine beliebte Vorgangsweise die entsprechenden Aktivitäten nicht über den eigenen Rechner, sondern über Bot-Netze mit ferngesteuerten Fremdrechnern abzuwickeln (sogenannte Zombie-Rechner). Laut Bundeskriminalamt waren 2006 weltweit 1450 Command&Control-Server bekannt, die derartige Netze steuerten. Es ist denkbar, dass Gruppen/Personen mit denen der Angeklagte Kontakt hatte sein Gerät für derartige Zwecke nutzten, insbesondere da er als "vertrauenswürdig" eingestuft wurde.]

- Haben sich auf dem beschlagnahmten Gerät Hinweise auf Installationen von Spyware (abgesehen von der Installation der SEO) gefunden? Eventuell frühere Installationen die zum Zeitpunkt nicht mehr aktiv waren?
- Wenn ja: Welche Auswirkungen haben diese Installationen auf das Erstellen, Verändern und Verschicken von Texten und anderen Dateien?

[Hintergrund: wie oben]

THEMENKREIS: ALLGEMEINE FRAGESTELLUNGEN

[Dieser Themenkreis umfasst Fragen, die sich aus dem Zusammenwirken der verschiedenen Überwachungsmaßnahmen ergeben.]

ZEITLICHE SYNCHRONISATION

- Wie wurde sicher gestellt, dass die zeitlichen Abläufe des Lauschangriffs, der Online-Überwachung, der Überwachung beim Internet-Service-Provider und die zeitlichen Zuordnung von Aktivitäten am später beschlagnahmten Computer tatsächlich ausreichend genau synchronisiert wurden?
- Wenn keine ausreichende Synchronisation: Gibt es Hinweise, dass fehlende Synchronisation zu Fehlinterpretationen in der zeitlichen Abfolge von wesentlichen Vorgängen geführt haben (etwa Missinterpretationen, was tatsächlich Up- und Downgeloadet wurde, wer welche Nachricht empfangen/verschickt hat, ob tatsächlich Nachrichten verschickt wurden, ...)?

[Hintergrund: Weder das Internet, noch einzelne Computer verfügen über verbindliche Zeitaufzeichnungen (Kalender bzw. Uhr). Abweichungen von mehreren Minuten bis mehreren Stunden sind üblich, fallweise gehen Datumswerte überhaupt verloren oder werden von Benutzern irrtümlich/absichtlich verstellt. Damit lassen oft Abläufe, wer nun tatsächlich etwas verschickt/verbreitet hat und wer bloßer Empfänger ist, nicht ausreichend klar zuordnen.]

- Gibt es Hinweise auf Internetaktivitäten ausgehend vom Rechner des Angeklagten auch in Zeiten außerhalb der Anwesenheit des Angeklagten?
- Wenn ja: Welche Aktivitäten sind das? Gibt es Hinweise, dass es sich um Server- bzw. Relay-Aktivitäten handelt (ein- und ausgehender Datenverkehr)?

[Hintergrund: Internetaktivitäten außerhalb der Anwesenheit sind starke Indizien, dass der Rechner von Dritten genutzt wird. Diese Nutzung durch Dritte könnte auch in der Zeit während der Anwesenheit des Angeklagten erfolgen, ist aber wesentlich schwerer nachzuweisen.]

EURO2008-TEXT / "ANSCHLAGSTEXT"

- Für den Fall, dass es keine eindeutigen Hinweise aus der Onlineüberwachung gibt, dass dieser Text vom Angeklagten erstellt und verschickt wurde, lassen sich aus dem zeitlich synchronisierten Internetverkehr Anhaltspunkte für ein Upload des Textes oder alternativ für ein Download des Textes finden?