(ADMF) und zu dem normalerweise nur spezielles sicherheitsüberprüftes Personal Zugang hat. Dieses gibt nun die entsprechenden Daten in das System ein, welches die Daten dann entsprechend aufbereitet an die jeweils zuständigen Netzknoten übermittelt. Das können Fest- und Mobilfunkvermittlungsstellen sein, Router, oder andere, je nach verwendeter Technologie.

Dabei werden sämtliche Tätigkeiten in gesicherten Logfiles aufgezeichnet, um später jederzeit nachverfolgen zu können, wer beim Netzbetreiber wann welche Eingaben und Abfragen im System getätigt hat. Damit soll auch einem eventuellen Missbrauch vorgebeugt werden.

Im Netzknoten werden nun alle anfallenden Kommunikationsdaten einer überwachten Verbindung dupliziert. Da heute alle solche Netzknoten digital arbeiten, ist der Vorgang des Duplizierens technisch völlig unproblematisch und beschränkt sich in der Regel auf das Duplizieren der zu übertragenden Datenbits. Diese werden über die entsprechend vorkonfigurierte Verbindung ausgeleitet, ebenso die in der vermittlungstechnischen Software gesammelten Rufdaten. Bevor aber CC und IRI an den oder die Bedarfsträger geschickt werden (ein Ziel kann auch gleichzeitig von mehreren Bedarfsträgern überwacht werden), werden sie allerdings noch an ein ebenfalls beim Netzbetreiber befindliches System geleitet, die sog. Delivery oder Mediation Function (DF). Hier werden herstellerspezifische Protokolle, Formatierungen und/oder Codecs in genormte Formate umgewandelt beziehungsweise auch länderspezifische Anpassungen vorgenommen.

Mit wenigen Sekunden Verzögerung, bedingt durch die beschriebene Nachbearbeitung, landen dann alle Informationen bei den Bedarfsträgern, in speziellen Auswerte- und Überwachungssystemen. Diese werden auch als Monitoring Center bezeichnet, engl. *Law Enforcement Monitoring Facility*, abgk. LEMF. Hier werden alle eingehenden Daten sicher abgespeichert, zusammengeführt und anschließend Analysten oder Auswertern zugewiesen. Die Analyse erfolgt heute auch intensiv softwareunterstützt. So werden etwa automatisch Benutzerprofile nach verschiedensten Kriterien erstellt, etwa Bewegungsprofile **(siehe Abbildung 2)**, Korrelationen mit Daten aus anderen Quellen ermittelt **(siehe Abbildung 3)** und Sprachanalysen durchgeführt.

Einige Besonderheiten gilt es noch im Bereich des Mobilfunks zu erwähnen. Sind von zu überwachenden Mobiltelefonen Daten wie die Rufnummer (MSISDN), die internationale Kennung (IMSI) oder die eindeutige Gerätenummer (IMEI) bekannt, so kann die Überwachung ohne weitere Probleme in der Mobilfunkvermittlungsstelle vorgenommen werden, egal, ob es sich dabei um GSM, UMTS, oder andere Mobilfunksysteme handelt.

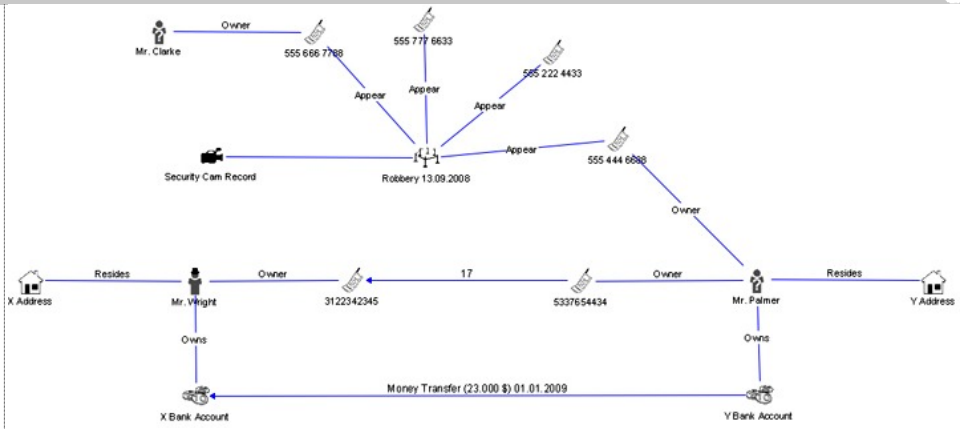

Abbildung 3: Beispiel einer Korrelationsanalyse (Quelle: [1])

Wird jedoch eine anonyme Wertkarte verwendet und alle oben beschriebenen Identitäten sind (vorerst) noch unbekannt (z.B. wegen neuem Mobiltelefon), so kommt ein spezielles Gerät zum Einsatz, der sog. IMSI-Catcher. Dieses Gerät nützt die Eigenschaft von GSM aus, dass sich zwar das Mobiltelefon gegenüber dem Netz authentifizieren muss, nicht aber das Netz gegenüber dem Mobiltelefon. Der IMSI-Catcher gaukelt nun dem zu überwachenden Mobiltelefon vor, eine Zelle im Netz zu sein, die die beste Empfangsqualität bietet, dem eigentlichen Mobilfunknetz präsentiert er sich als Mobiltelefon. Damit kann nun das im IMSI-Catcher unverschlüsselt vorliegende Gespräch überwacht werden, außerdem lassen sich so alle wichtigen Kenndaten (MSISDN, IMSI, IMEI) für eine reguläre Überwachung ermitteln.

Bei UMTS ist die Vorgangsweise etwas komplizierter, da sich hier erstmals auch das Netz gegenüber der Mobilstation identifizieren muss *(mutual entity authentication)*. Hier wird ein *Man-in-the-Middle*-Angriff durchgeführt, mit dessen Hilfe das Mobiltelefon anschließend in den GSM-Modus gezwungen wird, wonach genauso wie oben verfahren werden kann.

Der Betrieb eines IMSI-Catchers ist allerdings auch mit etlichen Problemen und Nachteilen verbunden, die hier kurz erwähnt werden sollen. So muss etwa der Netzanbieter des Ziels schon im Vorfeld ermittelt werden. Je nach Signalstärke des IMSI-Catchers befinden sich mehrere Mobiltelefone im Einzugsgebiet, die vom IMSI-Catcher zwar abgewiesen werden, aber dann trotzdem nicht auf das eigentliche Netz zugreifen können. Er verursacht daher eine lokale Störung im Mobilfunknetz, die (zumindest theoretisch) vom Netzbetreiber im Nachhinein festgestellt werden kann. Auch können nur ausgehende Anrufe mitgehört werden, außerdem scheint das abgehörte Gespräch nicht auf der Telefonrechnung des Teilnehmers auf. Die Überwachungsmaßnahme kann also von aufmerksamen Anwendern zumindest begründet vermutet werden. Abgesehen davon erklärt die Beschränkung auf ausgehende Anrufe auch, warum ein IMSI-Catcher nicht geeignet ist, um Lawinenopfer zu lokalisieren – die gesuchte Person ist in der Regel nicht mehr in der Lage, selbst einen Notruf abzusetzen!

Auf eine detailliertere technische Beschreibung muss hier aus Platzgründen verzichtet werden, eine grundlegende Einführung in das Thema, wenngleich etwas veraltet, findet sich unter.[2] Eine exzellente Seminararbeit über die genaue Funktionsweise von IMSI-Catchern bei UMTS ist.[3] Die Beschreibung der Funktionsweise des IMSI-Catchers ist auch gut nachzulesen in Wikipedia.

Erwähnt werden soll hier auch noch die Vorratsdatenspeicherung (VDS), die aber mit Lawful Interception sowohl technisch als auch konzeptuell nur indirekt verwandt ist. So erfolgt LI nur bei begründetem Verdacht auf richterliche Anordnung, während die VDS präventiv durchgeführt wird. Da bei der VDS Rufdaten aller Teilnehmer und Teilnehmerinnen erfasst werden, kann das Sammeln dieser Daten nicht analog zu LI von der vermittlungstechnischen Software durchgeführt werden, da dies viel zu viel Aufwand bedeuten würde. Die sinnvolle LI-Überwachungskapazität einer Vermittlungsstelle liegt im niedrigen einstelligen Prozentbereich aller aktiven Verbindungen. Bei VDS werden bis auf wenige Ausnahmen (zum Beispiel E-Mail-Header) hauptsächlich Daten abgegriffen, die der Betreiber zu Abrechnungs- oder Dokumentationszwecken sowieso erstellen muss, und dann entsprechend ergänzt und abgespeichert. Außerdem findet bei VDS die Aufbewahrung der gesammelten Daten direkt beim Netzbetreiber statt und die Behörde greift auf diese nur bei Bedarf zu.

Dementsprechend groß ist auch das Speichervolumen, das die Netzbetreiber hier vorhalten müssen. Ein größerer Telekommunikationsanbieter etwa, der auch ein Mobilfunknetz betreibt und zugleich ISP ist, muss hier durchaus mit benötigten Kapazitäten rechnen, die ein Petabyte (1 PB = 1.000 TB = 1.000.000 GB = 10^{15} Byte) deutlich überschreiten können.

Wenn man über Überwachung der Telekommunikation spricht, so muss man auch fragen, wie es um dem Unterschied zwischen dem gesetzlich legitimiertem Abhören *(Lawful Interception)* und dem in letzte Zeit durch alle Medien geisternden großflächigem Abhören von Telekommunikation durch Geheimdienste (engl. *Signal Intelligence*) bestellt ist. Nun, formal existieren

Abbildung 2: Beispiel eines Bewegungsprofils (Quelle: [1])