Zeitschrift: Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie SAK = Criminologie / Groupe Suisse de Criminologie GSC = Criminologia / Gruppo Svizzero di Criminologia GSC

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 30 (2012)

Artikel: Ermittlungen und Überwachungsmassnahmen im Internet : Möglichkeiten und Grenzen

Autor: Weder, Bernhard

DOI: https://doi.org/10.5169/seals-1051475

Ermittlungen und Überwachungsmassnahmen im Internet – Möglichkeiten und Grenzen

BERNHARD WEDER
Dipl. El. Ing. HTL, Kantonspolizei Zürich,
Technische Ermittlungsunterstützung, Engineering Support

Inhaltsverzeichnis

Zusammenfassung 124
1. Grundlagen 124
2. Überwachungsstatistik 125
3. Echtzeitinternetüberwachung – wie funktioniert sie 127
   3.1 Festnetz 127
   3.2 Mobilfunknetz 127
4. Rückwirkende Teilnehmeridentifikation im Internet 128
   4.1 Festnetz – Internet 128
   4.2 Mobilfunknetz – Internet 129
5. Überwachbarkeit der Internetanwendungen 129
   5.1 Bedeutung 129
   5.2 Verschlüsselte Webseiten 130
   5.3 Proprietäre Protokolle 130
   5.4 Verschlüsselte Telefonie 131
   5.5 Transkription 132
   5.6 Komplexe Webseiten 132
   5.7 Internetprotokoll Version 6.0 134
   5.8 Nomadisierung 135
6. Echtzeit Internetüberwachung – Erfahrungen 136
7. Wie weiter? 137
   7.1 Reale – Virtuelle Raumüberwachung 137
   7.2 Government Software 138
   7.3 Funktion 138
   7.4 Online Durchsuchung 139
   7.5 Mythos Trojaner 139
8. Zukunft ohne Government Software 140

Zusammenfassung

Es werden die heutigen Möglichkeiten bei der Echtzeit Überwachung und der Rückwirkenden Teilnehmeridentifikation im Internet beleuchtet. Anhand der Statistik 2010 wird bewiesen, dass die Schweiz keineswegs – wie oft in den Medien behauptet – ein Überwachungsstaat ist. Auf die Schwierigkeiten der Ermittler, die sie bei der Auswertung der Überwachung antreffen, wird im Detail eingegangen. Heute sind viele Internetprotokolle nicht oder nur schwer überwachbar, weil sie verschlüsselt oder proprietär sind. Moderne Webseiten bestehen aus vielen Einzelteilen, die von den unterschiedlichsten Anbietern gefüllt werden. Betrachtet ein Überwachter solch komplexe Webseiten, wird die Ermittlungstätigkeit erheblich erschwert.

Die Erfahrungen bei der Auswertung von Echtzeitinternet Überwachungen zeigen, wie unterschiedlich Anwender das Internet nutzen. Ein Ausblick in die Zukunft führt zur Aussage, dass Government Software (GovWare) als einzig brauchbares technisches Überwachungsmittel übrig bleibt. Anhand der Unterschiede wird erklärt, wieso „GovWare" keine trojanische Software ist und welche Mittel bleiben, wenn der Einsatz der „GovWare" aus rechtlichen Gründen nicht mehr möglich ist.

1. Grundlagen

Seit Februar 2007 sind Internetüberwachungen in der Schweiz technisch möglich. Die rechtlichen Grundlagen dafür findet man im Bundesgesetz zur Überwachung des Post und Fernmeldeverkehrs (BÜPF). Eine Überwachungsmassnahme muss von den Untersuchungsbehörden beantragt werden. Die Staatsanwaltschaft muss diese geheime Überwachungsmassnahme verfügen und beim Zwangsmassnahmengericht des Kantons, respektive des Bundes bewilligen lassen.

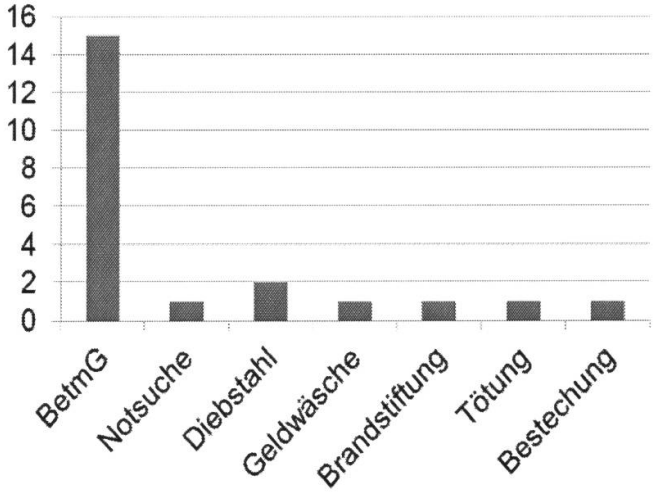
Zur Überwachung des Internetverkehrs sind die Internetzugangsanbieterinnen verpflichtet (Swisscom, Cablecom, Sunrise etc.). Durchgeführt wird die Massnahme organisatorisch und technisch vom Eidgenössischen Justiz und Polizeidepartement (EJPD). Der Dienst ÜPF (Überwachung des Post und Fernmeldeverkehrs) im Informatik Service Centre (ISC) des EJPD ist dafür zuständig.

Bis zum 1.1.2013 gilt eine Internetüberwachung als Spezialmassnahme und ist vom Goodwill der Fernmeldedienstanbieterin (FDA) abhängig.

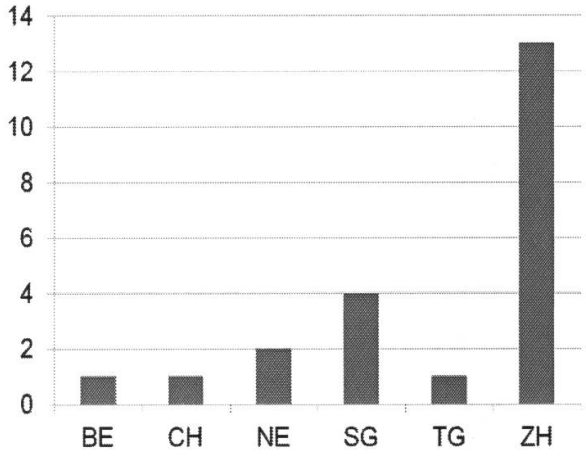
Einerseits sind die FDA zwar gemäss BÜPF dazu verpflichtet, da die geltende Verordnung VÜPF) aber keine Angaben über die Überwachung des Internetverkehrs enthält, kann der ÜPF den FDA keine Vorschriften machen, wie und wie schnell die Überwachung vollzogen werden muss. Die Verordnung VÜPF ist in einer teilrevidierten Fassung per 1.1.2012 in Kraft gesetzt worden. Allerdings wurde den FDA eine Übergangsfrist von einem Jahr zugestanden, so dass mit regulären Überwachungen erst per 1.1.2013 zu rechnen ist.

2. Überwachungsstatistik

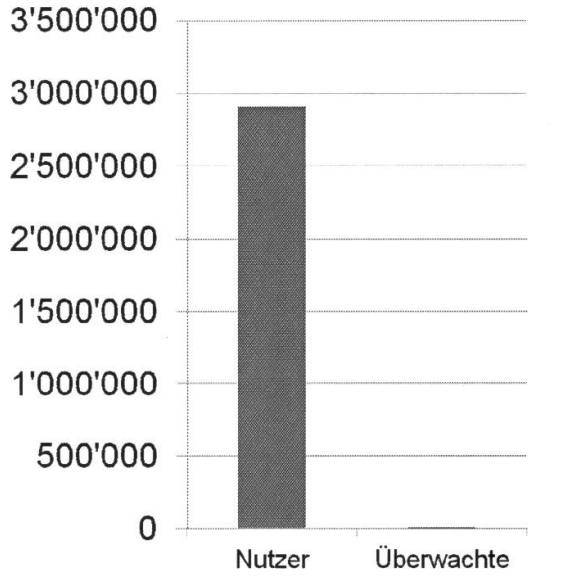
2010 gab es in der Schweiz rund 2,9 Mio. internetfähige Festnetzanschlüsse und 9,6 Mio. Mobilfunkteilnehmer mit der Möglichkeit, mobiles Internet zu nutzen[1)]. Von den insgesamt 12,5 Mio. potentiellen Internetanschlüssen können aus den genannten Gründen also gerade mal 23 % in einem Strafverfahren überwacht werden. Mehr als dreiviertel (77%) aller Anschlüsse entzogen sich der Strafverfolgung – eine massive Überwachungslücke.



Im Jahre 2010 wurden insgesamt 22 Internetüberwachungen durchgeführt. 21 betrafen den Bereich Strafverfolgung, eine die Lokalisierung einer vermissten Person (Notsuche). 15 Internetüberwachungen fanden im Bereiche Betäubungsmittel, zwei im Bereiche Diebstahl und je eine im Bereiche Geldwäsche, Brandstiftung, Tötung und Bestechung statt [2)].



Am meisten Echtzeitinternetüberwachungen führte der Kanton Zürich (13) durch, der Kanton St. Gallen vier, Neuenburg zwei und Bern, Thurgau und Fedpol (Bund) je eine. Die Gründe für diese Verteilung sind nicht erforscht. Generell gilt jedoch: Internetüberwachungen sind personell aufwendig, erfordern spezifisches Wissen und entsprechende finanzielle Mittel.

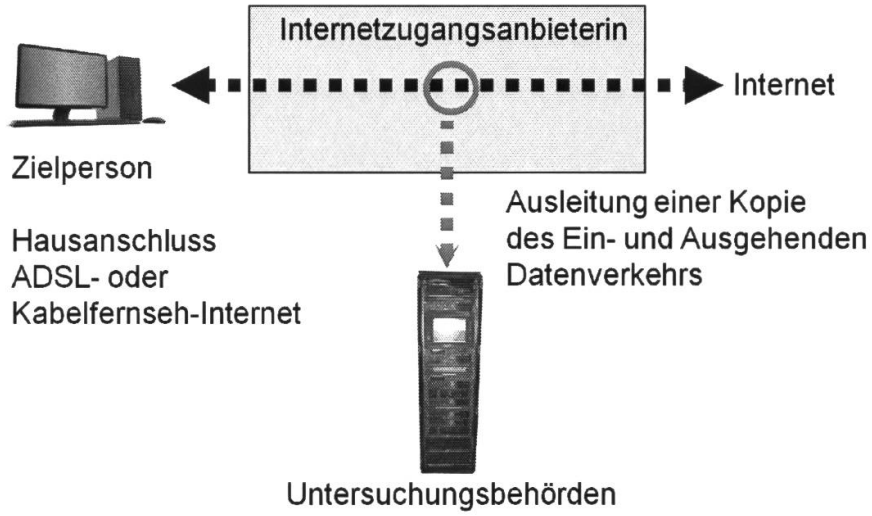


Von den maximal 2,9 Mio. überwachbaren Festnetzinternetanschlüssen wurden 0.00075 % überwacht. Mobile Internetnutzer wurden keine überwacht, schlicht deshalb, weil die technische Ausrüstung bei den Fernmeldedienstanbieterinnen fehlt. Die Angst vor einer flächendeckenden Überwachung der Bürger ist unbegründet – die Schweiz ist definitiv kein Überwachungsstaat.

3. Echtzeitinternetüberwachung – wie funktioniert sie

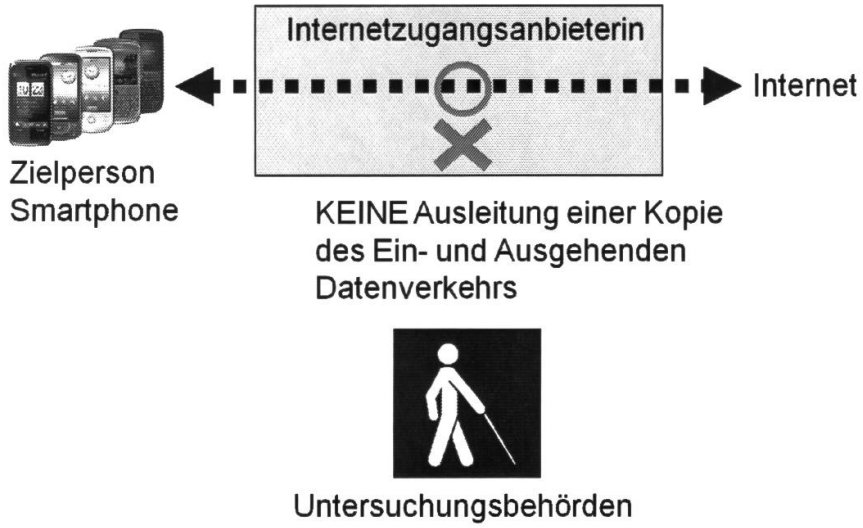
3.1 Festnetz

Die Zielperson (zu überwachende Person) verbindet sich über seine Internetzugangsanbieterin mit dem Internet. Die Internetzugangsanbieterin leitet eine vollständige Kopie des Ein- und ausgehenden Datenverkehrs der Zielperson an das ISC-EJPD ÜPF aus. Dort wird der Datenverkehr entgegengenommen und aufgezeichnet. Die Untersuchungsbehörden können auf der Anlage des ÜPF den Datenverkehr auswerten.



3.2 Mobilfunknetz

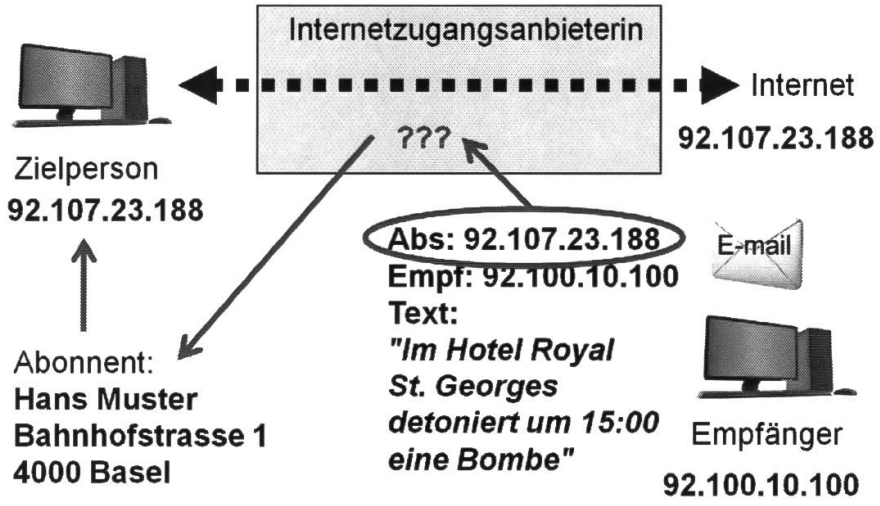
Über das Mobilfunknetz der Anbieter Swisscom, Sunrise und Orange mit dem Internet verbundene Internetfähige Handys (Smartphone) können nicht überwacht werden, weil die Fernmeldedienstanbieterinnen zurzeit technisch noch nicht dazu in der Lage sind. Mit dem Ablauf der Übergangsfrist zur Umsetzung der teilrevidierten VÜPF per 1.1.2013 sollten sie dann zumal in der Lage sein. Die Untersuchungsbehörden können heute also keine Internet Kommunikation über Smartphone überwachen. Kommunikation über viel genutzte Apps wie MMS, Whatsapp, Viber, Facebook und Skype sind nicht überwachbar. Die Straftäter sind sich durch Medienberichte der Situation bewusst und nutzen diese Lücken gezielt aus [3)].



4. Rückwirkende Teilnehmeridentifikation im Internet

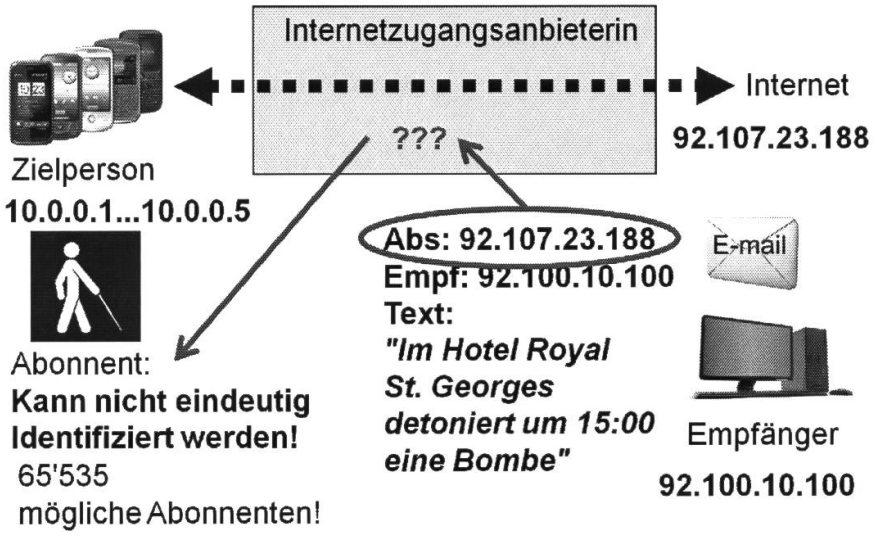
4.1 Festnetz – Internet

Kommuniziert eine Zielperson mit dem Festnetz über das öffentliche Internet, erhält sie von ihrem Internetzugangsanbieter eine eindeutige öffentliche IP Adresse (z.B. 92.107.23.188). Verschickt sie ein E-Mail an eine andere Person, so sieht der Empfänger diese Absender IP Adresse im Kopffeld des eintreffenden E-Mails. Die Strafverfolgungsbehörden können diese IP Adresse bei der zuständigen Internetzugangsanbieterin abklären lassen. Die Internetzugangsanbieterin kann den Abonnenten des Festnetzinternetanschlusses identifizieren.



4.2 Mobilfunknetz – Internet

Kommuniziert eine Zielperson mit dem Mobilfunknetz über das Internet, erhält sie von ihrem Internetzugangsanbieter eine interne, private (10.0.0.1) und eine öffentliche IP Adresse (z.B. 92.107.23.188). Verschickt sie ein E-Mail an eine andere Person, so sieht der Empfänger die öffentliche Absender IP Adresse im Kopffeld des eintreffenden E-Mails. Die Internetzugangsanbieterin kann den Abonnenten des Festnetzinternetanschlusses jedoch nicht eindeutig identifizieren, weil aus technischen Gründen bis zu 65´535 Endgeräte dieselbe IP Adresse verwenden. Die Internetzugangsanbieterinnen wären gemäss BÜPF zur Identifikation verpflichtet. Umgesetzt wird diese Pflicht jedoch nicht.



5. Überwachbarkeit der Internetanwendungen

5.1 Bedeutung

Die konventionelle Telefonie wird in zunehmendem Masse durch die internetbasierende Telefonie ersetzt. Telefoniert man heute über einen Kabelfernsehanschluss, so wird die Sprache im Voice Over IP Protokoll (VoIP) abgewickelt. Auch moderne und "billigere" Festnetz Telefonangebote wie z.B. "Click and Call" von Sunrise oder "Trio Casa" von Swisscom verwendet internetbasierende Technik. Über kurz oder lang wird die klassische, leitungsvermittelte Telefonie – wie man sie von früher kennt – verschwinden. In naher Zukunft wird daher die klassische Festnetztelefonüberwachung obsolet und die Internetüberwachung immer wichtiger.

5.2 Verschlüsselte Webseiten

Nicht alle Internetprotokolle sind überwachbar. Gängige und öffentlich publizierte, unverschlüsselte Protokolle können decodiert werden. Verschlüsselte Protokolle hingegen können nicht decodiert werden.

Fast alle Webseiten, bei denen man etwas bezahlen, bestellen oder buchen kann, setzen standardmässig die sichere HTTPS (Hypertext Transfer Protocol Secure) Technik ein. Einige Beispiele dafür sind Fluggesellschaften, Transportunternehmen, Banken, Finanzinstitute, Hotelbuchungsportale, Reiseportale und Kreditkartenfirmen. Zunehmend verwenden "konventionelle" Webseiten ebenfalls diese Technik. Selbst die zurzeit bekannteste Suchmaschine "Google" bietet seit geraumer Zeit eine auf HTTPS basierende Suche an. Suchresultate, die auf der verschlüsselten Website https://www.google.com gefunden werden, können nicht decodiert werden.

Bei verschlüsselten Webseiten bleibt als einziges ermittelbares Resultat die IP Adresse des Servers, der den Service ausgeliefert hat. Man erfährt also, mit welchem Dienstleister im Internet die Zielperson Kontakt hatte. Mittels einer sogenannten „Whois"-Abfrage findet der Ermittler nur noch die Firma oder den Dienstleister, der die Domäne registriert hat. Die Namen der Firmen sagen allerdings nicht viel aus. Es sind zusätzliche, aufwendige Recherchen notwendig, um herauszufinden, welcher Service dahinter steht. Was genau angeboten wird, lässt sich allerdings vielmals nur vermuten (Bsp. aus einer realen Überwachung):

94.245.120.189	=	Microsoft Limited, Software Updates für Windows
173.241.240.7	=	Openx Technologies Inc, Werbefirma, verkauft Online Werbung auf Webseiten
31.186.225.24	=	Internap Network Operations, Rechenzentrum für kommerzielle Webserver
46.137.77.20	=	Amazon Data Services Ireland, Online Buchhändler
93.184.220.33	=	Edgecast Networks Inc, Inhaltsanbieter, für z.B. Deutsche Telecom, EMI, Walt Disney

5.3 Proprietäre Protokolle

Zunehmend werden zudem firmeneigene Protokolle im Internet eingesetzt, die sich nicht an öffentliche Standards halten, sondern von Firmen für ihre Angebote neu erfunden werden. Ein Beispiel dafür ist das Microsoft Messenger Protokoll (MSN), aber auch „Social Media" Anwendun-

gen wie Facebook verwenden spezielle Protokolle. Diese Protokolle werden von den Anbietern nicht öffentlich publiziert, sondern als Firmengeheimnisse betrachtet. Da sich die Anwendungen stetig weiter entwickeln, werden die Protokolle auch entsprechend oft geändert. So ist es für die Hersteller von Überwachungssoftware schwierig "Up to date" zu bleiben. Der Aufwand für das Reverse Engineering der nicht öffentlichen Protokolle ist immens. Kann ein Protokoll endlich decodiert werden, kann es sein, dass der Anbieter das Protokoll bereits wieder geändert hat und die Decodierung dann schon nicht mehr funktioniert. Die Strafverfolger werden also immer hinterher hinken.

Heute werden bereits viele spezielle Anwendungen verwendet, um miteinander zu kommunizieren. Die Verbreitung sog. „Flatrate“ Abonnemente (unlimitierter Datenverkehr für einen fixen Betrag pro Monat) für das Festnetz-Internet und auch das Mobilfunk-Internet bewirken, dass die Benutzer vermehrt auf Applikationen umsteigen, die Telefonie, Meldungsdienste und Videokonferenzen über das Internet anbieten, da deren Nutzung keine zusätzlichen Kommunikationskosten verursachen.

Die meisten Applikation sind sowohl für fix installierte PC's und auch für moderne Smartphone erhältlich. Besitzen beide Gesprächspartner dieselbe Software, kann darüber bequem und unentgeltlich kommuniziert werden. Einige heute populäre Anwendungen sind „Whatsapp“, „Viber“, „Facebookchat“, „Facetime“, „GoogleTalk“ und „ICQ“. Es existieren aber noch zahlreiche andere Anwendungen. Viele neue werden in Zukunft auf den Markt kommen und alte verschwinden.

5.4 Verschlüsselte Telefonie

Skype ist eine verschlüsselte Telefon und Videokonferenz Software die ursprünglich in Estland entwickelt worden ist. Neuerdings ist Microsoft der Besitzer. Nebst der Verschlüsselung verwendet die Software auch noch die sog. Peer to Peer Technik. Das heisst, dass nicht mehr ein zentraler Server existiert, der den Service anbietet, sondern dass der Service auf alle Benutzer der Technik im Internet aufgeteilt wird. Es kann also keine Überwachung mehr an einem zentralen Ort erfolgen.

Straftäter nutzen die Technologie von Skype explizit, weil sie wissen, dass Skype Telefonate nicht abhörbar sind. Eine Strafverfolgungsbehörde hat ein konventionelles Handygespräch von zwei mutmasslichen Wirtschaftsdelinquenten abgehört. Die beiden Angeschuldigten telefonieren nur noch um miteinander abzusprechen, wann sie auf „Skype“ gehen. Die

deliktischen Gespräche finden dann nur noch mittels Skype statt – ausserhalb des Zugriffs der Strafverfolgungsbehörden.

5.5 Transkription

Da die meisten überwachten Personen nicht in einer Landessprache kommunizieren, fällt für die Dolmetscher viel Arbeit an. So muss zum Beispiel jeder Chatbeitrag zuerst übersetzt werden. Vielfach ist es auch nicht einfach, einen vertrauenswürdigen Dolmetscher zu finden, der die Sprache so gut versteht, dass auch verklausulierte Kommunikation verständlich übersetzt werden kann. Straftäter kommunizieren meistens sehr konspirativ und erwähnen die Sache, um die es geht nicht offen, sondern umschreiben sie. Es ist daher essentiell, dass immer der oder dieselbe Dolmetscherin den Fall während der gesamten Überwachungsdauer übersetzt, damit die logischen Bezüge zu bereits erfolgter Kommunikation hergestellt werden kann. Die übersetzte Kommunikation wird in schriftlichen Protokollen festgehalten. Diese müssen im Strafverfahren der angeschuldigten Person vorgelegt und durch einen anderen, bis dahin unbeteiligten Übersetzer wieder zurück in die originale Sprache übersetzt werden. Dies verdoppelt die Kosten für die Strafverfolger.

5.6 Komplexe Webseiten

Heut zu Tage bestehen die Webseiten nicht mehr nur aus einem einfachen HTML Code. Vielfach sind sie aus verschiedensten Teilen zusammengesetzt, die von unterschiedlichen Anbietern geliefert werden. Vielfach werden auch Erweiterungen der ursprünglichen Webseitensprache HTML angewendet, wie zum Beispiel Java, Flash und Silverlight. Was für den Benutzer wie eine einzige Webseite wirkt, besteht in Wirklichkeit aus vielen Einzelteilen, die nicht vom selben Anbieter stammen müssen.

Als Beispiel soll die die „Blick“ Webseite dienen. Am rechten Rand ist ein Inserat von „Navyboot“ zur Weihnachtszeit eingeblendet. Installiert man in seinem Browser (z.B. Firefox) eine Erweiterung (z.B. Firebug) so lässt sich herausfinden, dass das Inserat nicht von einem Server des Blicks stammt, sondern von einer komplett anderen Firma, im konkreten Beispiel von der Firma „Adtech“.

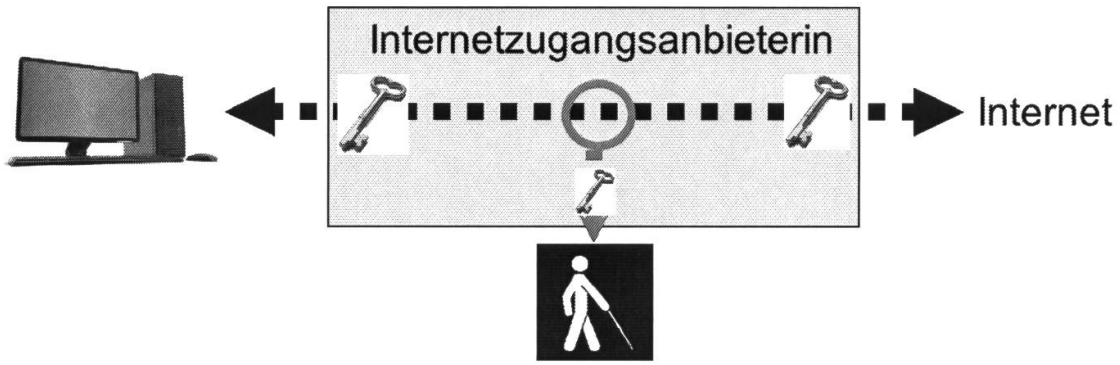
Dies ist eine Partnerfirma des Blicks, die die Werbung situativ auf die Blickseite bringt. Welche Werbung eingefügt wird, hängt davon ab, wo und wann der Benutzer die Webseite liest. So wird für einen Schweizer Benutzer andere Werbung eingeblendet, wie für einen Leser im Ausland. Auch ist es so, dass die Werbung je nach Zeit variiert. Ist gerade Weihnachtszeit, wird Werbung für diese Zeit eingeblendet. Ist der Benutzer dem Werbeanbieter bekannt, blendet er noch stärker personalisierte Werbung ein. So kann die Zielgruppe ganz genau ausgewählt werden (Frau, Mann, Alter, Vorlieben etc.). Realisiert wird dies, indem der Werbeanbieter sogenannte "Cookies" in den Rechner des Benutzers hinterlegt, mit denen der Benutzer eindeutig identifiziert werden kann. In den Datenbanken der Werbefirmen, ist festgehalten, was der Benutzer schon einmal angeklickt hat und welche Vorlieben er hat.

Komplexe Webseiten bedeuten für die Ermittler eine grosse Erschwerung der Auswertearbeit.

Da die Rekonstruktionssoftware die Webseite nicht so, wie sie die Zielperson sah darstellen kann, findet der Auswerter sämtliche übertragenen Dateien dieser Webseite nur in zeitlicher Reihenfolge als Einzeleintrag vor. Er muss sich durch jeden Eintrag durcharbeiten und das dekodierte Resultat einzeln beurteilen. Benutzt die Website noch zusätzlich Java, Flash, Silverlight – Skriptsprachen, so kann der decodierte Code beim Betrachten nicht ausgeführt werden, da die Auswertesoftware aus verständlichen Gründen nicht wie der Browser (Internet Explorer, Firefox, Safari, Opera, Chrome) der Zielperson direkt ins Internet zugreifen darf. Der Bildschirm des Ermittlers wird dann regelrecht mit Fehlermeldungen zugepflastert.

5.7 Internetprotokoll Version 6.0

IP V6.0 ist der Nachfolger des heute verwendeten IP V4.0 Internetprotokolls. Da bereits alle IP Adressen in der V4.0 vergeben sind, wurde der Standard V6.0 notwendig. Eine Analogie gab es mit der Abschaffung der 01 – Telefonnummern Vorwahl für Zürich. Weil alle Telefonnummern vergeben waren, musste auf zwei neue Vorwahlen (043 und 044) umgestellt werden.



Zusätzlich ist es mit IP V6.0 einfach möglich, den gesamten Internetverkehr zu verschlüsseln. Dann nützt es auch nichts mehr, Kopien des Datenverkehrs beim Internetzugangsanbieter auszuleiten. Dieser Verkehr ist dann selbst für ihn nur noch verschlüsselt sichtbar. Ab dann benötigen die Untersuchungsbehörden die Mitarbeit der Provider nicht mehr und das BÜPF ist im Bereiche Internetüberwachung obsolet. Wie schnell sich der neue Standard durchsetzt, kann heute noch nicht mit Sicherheit vorausgesagt werden. Es ist jedoch festzustellen, dass neue Netzwerkkomponenten (Geräte) ausnahmslos alle mit IP V6.0 Fähigkeit ausgeliefert werden. Über kurz oder lang wird daher der Internetverkehr ausschliesslich in IP V6.0 stattfinden.

5.8 Nomadisierung

Moderne, mobile Internet Endgeräte (Post PC's) unterstützen eine Vielzahl von Technologien, die den Zugriff auf das Internet ermöglichen. Mit Smartphone, Laptops, IPads kann via „WirelessLan" (WLAN, WiFi, drahtloses Internet) gesurft werden – man ist nicht mehr nur auf den Fernmeldedienstanbieter seines Mobilfunknetzes angewiesen. Zu Hause greift man über das eigene WLAN, oder über das „offene WLAN" eines Nachbarn" auf das Internet zu und spart so die Kommunikationskosten, die sonst bei seinem Fernmeldedienstanbieter anfallen. Für öffentliche Restaurants, Kaffees, Shops, Shoppingcenters, Kommunen, Kasernen, Postbusse, Transportunternehmen, Hotels, Flughäfen etc. gehört es heute bereits selbstverständlicher Weise zum Grundangebot, kostenloses „WiFi" (=drahtloses Internet) anzubieten – wer dies nicht anbietet, tut sich schwer im Markt und setzt sich einem nicht gewünschten Wettbewerbsnachteil aus. „WiFi" ist ein „Must" geworden. Begünstigt wird diese Entwicklung durch die zunehmend notwendige und geforderte Mobilität der Arbeit-

nehmer in der globalisierten Welt. Pendler, die ihren Computer-Arbeitsplatz schon während der Reisezeit zu ihrem physischen Arbeitsort in Betrieb nehmen, treiben die Verbreitung von „Free WiFi" an.

Für die Strafverfolger bedeutet dies, dass sie keine vollständige Überwachung der Internetkommunikation mehr erhalten können. Benutzt die Zielperson nicht mehr nur den Internetzugang seines Mobilfunkanbieters, sondern die kostenlosen „WiFi" Verbindungen, die er auf seiner Reise antrifft, so ist schlichtweg unmöglich, lückenlos die Kommunikation des mutmasslichen Straftäters zu überwachen. Dazu müssten alle Anbieter von „WLAN" verpflichtet werden können, den Internetverkehr an das ÜPF auszuleiten (auch der „Nachbar" mit seinem offenen WLAN). Sie würden dann zum „Internetzugangsanbieter" die dem Fernmeldegesetz zu unterstellen wären. Dies ist schlichtweg unrealistisch und daher wohl nicht praktikabel.

6. Echtzeit Internetüberwachung – Erfahrungen

Die überwachte Person verhält sich im Internet unvorsichtiger als am Telefon und gibt üblicherweise mehr Preis. Man trifft auf verschiedene Typen von Internet-Nutzern (Chatter, Mailer, Phoner, Downloader, Tauscher) und nicht alle nutzen alle Möglichkeiten des Internets. Man lernt viel über die überwachte Person (Verhalten, Vorlieben, Kontakte, Gelüste, Gewohnheiten, Geschäftsgebaren). Die Personen sind schamloser (unbeobachtet, keine soziale Kontrolle vorhanden) und Internetkriminalität lässt sich nicht mehr in klassische Delikte – Kategorien einteilen:

Urteil Bezirksgericht 4.5.2011 Zitat Artikel in der NZZ:

Teure Fernsehgeräte, Spielkonsolen, Mobiltelefone, Schmuck, Möbel, iPods, Notebooks oder auch Rasierklingen: Die Produktepalette, die der 33-jährige EDV-Supporter, der am Mittwoch vor dem Zürcher Bezirksgericht gestanden hat, von Oktober 2004 bis Juli 2008 auf Auktionsplattformen im Internet unter falschen Namen anbot, war sehr breit gefächert. Ausserdem verkaufte der mehrfach einschlägig Vorbestrafte im Internet gefälschte Goldbarren, und er bestellte selber unter falschem Namen bei Web-Anbietern in grossen Mengen Waren, ohne diese zu bezahlen. Er verkaufte einen Luxuswagen, den er nie bezahlt hatte, und fälschte Betreibungsregister-Auszüge, um einen Vermieter zu täuschen. Und er hatte auf zwei Computern Kinderpornografie gespeichert, um sie später an eine

Abnehmerschaft zu verkaufen, die gut zahlen und bestimmt niemandem etwas von dem schmutzigen Geschäft erzählen würde. Der gesamte Deliktsbetrag liegt bei rund einer Viertelmillion Franken. Die Staatsanwältin wollte den seit einem Dreivierteljahr im Gefängnis sitzenden Mann 36 Monate hinter Gittern sehen. Doch auch das war dem Gericht zu mild. Es sprach eine Freiheitsstrafe von 5 Jahren aus. Der Verurteilte sei mit grosser krimineller Energie und raffiniert vorgegangen, so der Gerichtsvorsitzende: Er sei ein hartgesottener Rechtsbrecher.

7. Wie weiter?

Verschlüsselt die Anwendung die Kommunikation, so sind die Untersuchungsbehörden – wie gezeigt – machtlos. Da die meisten Anbieter von neuen Kommunikationsdiensten im Ausland beheimatet sind, unterstehen sie auch nicht der Schweizerischen Gesetzgebung (BÜPF) und können demzufolge auch nicht dazu verpflichtet werden, die Kommunikation (unverschlüsselt) an die Untersuchungsbehörden des jeweiligen Landes auszuleiten. Sie dürfen wohl ihre Dienstleistungen in jedem Land dieser Erde über das Internet anbieten (und Geld verdienen), müssen jedoch den Anforderungen der Strafverfolgungsbehörden im jeweiligen Land keine Folge leisten. Dies wird – realistisch betrachtet – wohl in der nahen Zukunft auch so bleiben.

7.1 Reale – Virtuelle Raumüberwachung

Für reale, private, physische Räume existieren bereits heute in der eidgenössischen Strafprozessordnung unbestrittene gesetzliche Grundlagen, wie vorzugehen ist. Dort ist auch geregelt, bei welchen Straftaten eine Überwachung (Mikrophon, Kamera) zum Einsatz kommen darf (Straftatenkatalog, ultimo Ratio) und wie der schwere Eingriff in die Privatsphäre zu bewilligen ist. Die Hürden sind hoch und garantieren dem Rechtstaat, dass die Bürger vor ungewollter flächendeckender Überwachung effizient geschützt werden können.

Für den privaten, virtuellen Raum existieren heute in der Schweiz und anderswo noch keine solchen unbestrittenen Rechtsgrundlagen. Diese müssen erst geschaffen werden. Ob sie im BÜPF oder in der StPO zu schaffen sind, ist für die effiziente Verfolgung von Straftätern nicht entscheidend, Hauptsache es wird geregelt.

Zu Bedenken ist, dass das BÜPF unter anderem dazu da ist, die Fernmeldedienstanbieter vom Fernmeldegeheimnis zu entbinden, wenn in ihrem Netz überwacht werden soll. Werden die Fernmeldedienstanbieter nicht tangiert (d.h. die Überwachung findet nicht in ihrem Netz statt), so kann Sinnvollerweise auch eine Regelung in der StPO erfolgen (Technische Überwachungsmassnahme). Entscheiden muss der Gesetzgeber.

7.2 Government Software

Folgerichtig bleibt in Zukunft als einziges erfolgsversprechendes, technisches Überwachungsmittel der Strafverfolger die Government Software (= GovWare) oder die Government Hardware (= „Wanze") übrig. Sie muss auf dem persönlichen Endgerät (= virtueller Raum) des Nutzers installiert werden können. Dies ist der einzige Ort im globalen Internet, an dem die Kommunikation des mutmasslichen Straftäter noch unverschlüsselt vorhanden ist. Zudem ist sie das einzige Überwachungsinstrument, das die globale Nomadisierung und das Problem der Verpflichtung der Internetzugangsanbieter von einer (notabene nicht erfolgsversprechenden) Überwachung löst.

Die GovWare ist entstanden, weil es keine andere Überwachungsmöglichkeit (mehr) gibt. Der Einsatz von GovWare ist risikoreich: Der Einsatz kann fehlschlagen und/oder nicht zum gewünschten Erfolg führen. Der Einsatz der GovWare ist so unzuverlässig wie der PC oder das Internet selber – und – die GovWare kann entdeckt werden, so wie eine konventionelle „Wanze" auch entdeckt werden kann

7.3 Funktion

Die Government Software muss analog zu einem physischen Raumüberwachungsmikrofon (Wanze) im virtuellen Raum der zu überwachenden Person (PC, Smartphone, Pad, Laptop etc) installiert werden. Sie schneidet die Mikrophon- und die Lautsprechersignale am PC mit und übermittelt die Aufzeichnung verschlüsselt (bestenfalls in nahezu Echtzeit) über das vom mutmasslichen Straftäter genutzten Internet an die Strafverfolgungsbehörden. Selbstverständlich darf sie die Bandbreite der Internetverbindung des Benutzers nicht vollständig ausnutzen, sondern nur einen kleinen Teil, damit der Überwachte nicht Verdacht schöpft.

7.4 Online Durchsuchung

Die GovWare eignet gut für die Überwachung von verschlüsselter Sprachkommunikation (z.B. Skype). Sie kann NICHT für eine Online Durchsuchung eingesetzt werden. Warum? Eine kleine Festplatte von 150 GByte Datenvolumen liesse sich bei den heute gängigen Breitband Internet Anschlüssen in 416 Stunden herunterladen (Annahme 5 MBit/s Download mit 500 kBit/s Upload und Nutzung der maximalen Bandbreite von 10% des Uploads = 50 kBit/s). Dies entspricht einer Dauer von rund 17 Tagen (unter der Annahme, dass das Endgerät des Nutzers 24 Stunden ununterbrochen mit dem Internet verbunden ist). In dieser Zeit hat der Benutzer die Festplatte bereits wieder stark verändert. Es kann also keine forensisch gesicherte und gerichtsverwertbare Spiegelung der Festplatte des mutmasslichen Straftäters vorgenommen werden.

7.5 Mythos Trojaner

Im Gegensatz zur landläufig und von den Medien verbreiteten Meinung ist die GovWare kein Trojaner. Sie darf sich nämlich unter keinen Umständen wie ein Trojaner unkontrolliert über das Internet verbreiten, sonst könnten viele unbeteiligte Personen betroffen werden. Dies ist für die Strafverfolgung ungeeignet und würde die makellose, gerichtsverwertbare Beweisführung verunmöglichen. Sie kann demzufolge auch nicht per Mail oder ähnlich verschickt werden, weil sonst die die Gefahr besteht, dass sie weitergeschickt werden könnte und schliesslich die falsche Person überwacht würde. Die einzige sichere Methode ist, sie vor Ort auf dem Zielrechner oder Smartphon zu installieren, um sicherzustellen, dass sie funktioniert und die richtige Person überwacht wird.

Der Quellcode des Programms muss dem Gericht zur Begutachtung zur Verfügung stehen. Damit kann sichergestellt werden, dass die GovWare nur das leistet, was das Zwangsmassnahmengericht bewilligt hat. Die GovWare ist zudem, im Gegensatz zu einem Trojaner, kein sogenanntes Rootkit, das sich über eine Schwachstelle des Betriebssystems einnistet. Die GovWare wird wie ein normales Programm auf dem Zielrechner installiert, damit sie nach Beendigung der bewilligten Überwachungsdauer vollständig deinstalliert werden kann, ohne die Funktion des Zielrechners zu beeinträchtigen. Die GovWare enthält ein gerichtlich genehmigtes Ablaufdatum, nachdem sie sich selbständig deinstalliert und vollständig löscht.

8. Zukunft ohne Government Software

Heute werden bereits viele spezielle Anwendungen verwendet um zu kommunizieren. Einige heute populäre Anwendungen wurden bereits erwähnt. Es existieren aber noch zahlreiche andere. Viele neue werden in Zukunft auf den Markt kommen. Die Verbreitung sog. Flatrate Abonnemente (unlimitierter Datenverkehr für einen fixen Betrag pro Monat) für das Festnetz-Internet und auch das Mobilfunk-Internet bewirken, dass die Benutzer vermehrt auf Applikationen umsteigen, die Telefonie, Meldungsdienste und Videokonferenzen über das Internet anbieten, weil deren Benutzung kostenfrei ist. Die meisten Applikation sind sowohl für feste PC's aber auch für moderne Smartphone erhältlich. Besitzen beide Gesprächspartner dieselbe Software, kann darüber kommuniziert werden.

Verschlüsselt die Anwendung die Kommunikation, so sind die Untersuchungsbehörden machtlos.

Da die Anbieter im Ausland beheimatet sind, unterstehen sie nicht der Schweizerischen Gesetzgebung (BÜPF) und können demzufolge auch nicht dazu verpflichtet werden, die Kommunikation unverschlüsselt an die Untersuchungsbehörden auszuleiten. Steht den Untersuchungsbehörden das Mittel GovWare nicht zur Verfügung, kann die Kommunikation mutmasslicher Straftäter in naher Zukunft nicht mehr überwacht werden.

Quellenangaben:

1) Bakom Fernmeldestatistik 2010.
2) Überwachungsstatistik 2010, ISC-EJPD ÜPF.
3) SF TV, Nachrichtensendung 10vor10, vom 25.2.2010, „Schlupfloch für Pädophile".