Einsatz von GovWare – zulässig oder nicht?

Zum Einsatz von Computerprogrammen bei der Überwachung von Internet-Telefonie

Dr. Thomas Hansjakob

Über den Einsatz von GovWare wurde in den letzten Wochen in den Medien breit berichtet; der Bundesrat hat am 23. November 2011 angekündigt, eine gesetzliche Grundlage für die Verwendung von «Staatstrojanern» zu schaffen. Der Autor beschreibt den praktischen Anwendungsbereich solcher Software, die geltenden gesetzlichen Grundlagen und kommentiert das geplante Gesetzgebungsvorhaben.

Inhaltsübersicht

I. Einleitung ^

[Rz 1] Der Einsatz von «Trojanern» durch Strafverfolgungsbehörden wurde in den Schweizer Medien in den letzten Wochen breit thematisiert, nachdem es dem Chaos Computer Club in Deutschland offenbar gelungen war, ein von deutschen Strafverfolgern eingesetztes Programm zu identifizieren und genauer zu analysieren, was dieses Programm auf dem betroffenen Computer bewirkt. Seither wird auch in der Schweiz die Frage gestellt, ob der Einsatz solcher Programme zulässig sei. Am 23. November 2011 hat der Bundesrat nun die Revision der Verordnung über die Überwachung des Post- und Fernmeldeverkehrs (VÜPF)[1] vorgelegt (welche dieses Problem noch nicht regelt) und gleichzeitig angekündigt, das Gesetz[2] revidieren zu wollen. Er sieht vor, dort den Einsatz solcher Computerprogramme zur Überwachung von Internet-Telefonie und E-Mails zu erlauben.[3]

[Rz 2] Vorerst eine Präzisierung zum Begrifflichen: Unter einem Trojaner versteht man üblicherweise ein Programm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt.[4] In der Regel geht es (relativ harmlos) bloss darum, den infizierten Computer für den Massenversand von Werbemails zu benutzen. Gefährliche Trojaner spionieren auch Daten, insbesondere Passwörter, aus oder löschen bzw. manipulieren Daten des Benutzers oder Systemdaten so, dass der Computer im schlimmsten Fall nicht mehr benutzt werden kann.

[Rz 3] Wenn Strafverfolger verdeckt Computerprogramme auf Computern von Verdächtigen installieren, dann wollen sie keinen Schaden verursachen, sondern im Rahmen des strafprozessual Zulässigen «bloss» ohne Wissen des Beschuldigten Daten ausleiten, die in einem Strafprozess als

Beweismittel von Bedeutung sind. Die fraglichen Programme sollten denn auch nichts zerstören[5] und dienen auch nicht unlauteren Zwecken, sondern sie erfüllen genau definierte Aufgaben bei der Erhebung von Beweisen, die auf andere Art nicht (oder nicht geheim) beschafft werden könnten. Strafverfolger reden deshalb in diesem Zusammenhang nicht von Trojanern, sondern von Government Software bzw. GovWare.

II. Warum braucht es GovWare und was kann sie? ^

1. Das Grundproblem ^

[Rz 4] Primär ging es bei der Entwicklung von GovWare darum, verschlüsselte Internet-Telefonie überwachen zu können. Das hängt mit der technischen Besonderheit zusammen:

[Rz 5] «Normale» Internet-Telefonie benutzt zur Datenübertragung nicht das Telefonnetz, sondern eben das Internet, das zur weltweiten Übertragung von grossen Datenmengen besser geeignet ist und in der Regel gratis zur Verfügung steht. Der Kunde hat einen Vertrag mit seinem Internet-Provider, der auch die Internet-Telefonie umfasst, und erhält vom Provider die nötige Soft- und allenfalls auch die Hardware, um telefonieren zu können. Solche Internet-Telefonie ist nicht verschlüsselt, der Provider des Kunden verfügt wie ein normaler Telefonanbieter über den elektronischen Verkehr, den er auch abgreifen und (bei entsprechender Verfügung der Strafverfolgungsbehörden) zum Zweck der Strafverfolgung zur Verfügung stellen kann.

[Rz 6] Allerdings hat sich nicht diese «normale» Internet-Telefonie, sondern ein anderes System in den letzten Jahren stark verbreitet. Das gilt in erster Linie für «Skype», neuerdings aber auch für Apps auf Smartphones wie zum Beispiel «Viber», das auf iPhones und mit Android funktioniert. Die Anbieter von Programmen nach diesem System liefern nur eine Software, welche es dem Benutzer ermöglicht, Internet-Telefonie mit allen Leuten zu betreiben, welche die gleiche Software auf ihrem Computer oder Smartphone installiert haben. Der Programmanbieter verfügt aber natürlich nicht über den Gesprächsverkehr seiner Kunden, weil er ja nur das Programm, nicht aber die Infrastruktur zur Übertragung von Gesprächen zur Verfügung stellt.

[Rz 7] Aus Gründen der Datensicherheit benutzen solche Programme erstens eine End-zu-End-Verschlüsselung: Der Gesprächsverkehr wird auf dem Gerät des Absenders bereits verschlüsselt und erst auf dem Gerät des Empfängers wieder entschlüsselt, sodass die Informationen auf dem Übertragungsweg nicht lesbar sind. Zweitens bauen solche Programme in der Regel auf der Peer-to-Peer-Architektur auf (P2P); das heisst, dass die Informationen in einzelne kleine Datenpakete aufgeteilt, dann über verschiedene Wege vom Absender zum Empfänger geschickt und erst dort wieder zusammengesetzt und entschlüsselt werden. Es werden also nicht die ganzen Informationen auf dem gleichen Weg verschickt; selbst der Provider des Absenders oder des Empfängers kann deshalb die einzelnen Datenpakete nicht identifizieren und zusammensetzen.

2. Die Form der Überwachung ^

[Rz 8] Die Überwachung solcher Internet-Telefonie ist also auf konventionellem Weg nicht möglich: Der Programmanbieter verfügt gar nicht über den Gesprächsverkehr des Kunden; der Provider des Kunden leitet zwar die Daten paketweise weiter, kann sie aber weder zu einem Ganzen

zusammenfügen noch entschlüsseln.

[Rz 9] Für die Überwachung bedeutet dies, dass die konventionelle Technik nicht funktioniert, weil sie darauf basiert, dass der Provider den Gesprächsverkehr des Kunden an die überwachende Behörde (bzw. in der Schweiz an den Dienst Überwachung des Post- und Fernmeldeverkehrs ÜPF) ausliefern kann. Die Strafverfolgungsbehörden sind damit zu einer andern Strategie gezwungen: Sie müssen den Gesprächsverkehr direkt auf dem Computer bzw. Smartphone des Überwachten abgreifen, und zwar, bevor er verschlüsselt wird; sie müssen verdeckt eine unverschlüsselte Kopie dieses Gesprächsverkehrs ausleiten. Dazu dient die GovWare.

3. Weitere Möglichkeiten ^

[Rz 10] Wenn GovWare so programmiert wird, dass sie verdeckt den Gesprächsverkehr der Internet-Telefonie ausleiten kann, dann ist es ein Leichtes, auch weitere Funktionen zu programmieren: Zunächst können die auf dem Computer gespeicherten Daten durchsucht und nach Bedarf wie der Gesprächsverkehr ausgeleitet werden. Es ist aber auch möglich, die Tastatureingaben zu protokollieren, um etwa die Eingabe von Passwörtern aufzeichnen zu können. Es können auch Screenshots, also Bilder der aktuellen Bildschirmanzeige, in frei wählbaren Zeitabständen ausgeleitet werden. Schlussendlich können auch das in jedem Laptop oder Smartphone eingebaute Mikrophon oder die Webcam ferngesteuert eingeschaltet werden, um deren Aufzeichnungen auszuleiten. Das alles benötigt zwar Rechen- und Übertragungskapazität und nicht zuletzt auch Energie, trotzdem werden solche Manipulationen nur von sehr geübten Benutzern von Computern erkannt.

4. Wie kommt GovWare auf den Computer der Zielperson? ^

[Rz 11] Es stellt sich natürlich die Frage, wie man Computerprogramme auf den PC oder das Smartphone eines Beschuldigten bringt, ohne dass dieser es bemerkt. Am einfachsten ist dies, wenn man das entsprechende Gerät physisch in der Hand hat. Es gibt aber durchaus Strategien, welche die Installation solcher Programme auch aus der Ferne ermöglicht, denn wer Internet-Telefonie betreibt, benutzt ja eben das Internet und tauscht damit ohnehin Daten mit dem Provider aus. Im Grunde genommen kann GovWare auf gleichem Weg auf einen Computer kommen wie ein Trojaner oder ein Virus. Es muss allerdings einerseits gelingen, die allfällige Virensoftware zu täuschen. Anderseits kommt bei GovWare eine zusätzliche Schwierigkeit dazu: Man muss sicherstellen, dass sie nur auf genau identifizierte Geräte installiert wird. Das ist dann schwierig, wenn die Zielperson über die gleiche Datenleitung Internetverkehr mit mehreren Geräten, etwa mit einem PC, einem Laptop und einem Smartphone betreibt, oder wenn sich mehrere Personen einen Internet-Anschluss teilen.

[Rz 12] Wesentlich einfacher als die Installation ist die Entfernung. Gängige GovWare ist heute so programmiert, dass sie sich ferngesteuert auch wieder löschen oder von vornherein mit einem «Verfalldatum» versehen lässt, an dem sie sich selbständig löscht.

III. Der Einsatz von GovWare vor Inkrafttreten der StPO ^

[Rz 13] Soweit mir bekannt wurde GovWare in der Schweiz bisher nur ganz vereinzelt eingesetzt (in den Medien war von vier Fällen die Rede). Der pragmatische Ansatz zur Begründung lautete, dass

das BÜPF die Überwachung des Fernmeldeverkehrs erlaube, ohne zu definieren, ob er über das normale Telefonnetz oder über Internet erfolge. Diese Zulässigkeit der Überwachung umfasse auch das Recht, die dafür notwendige Technologie einzusetzen. Möglich war auch die Argumentation, dass sich das Recht zur Überwachung des Telefonverkehrs aus dem BÜPF ergebe, während es sich beim Einsatz von Trojanern um eine technische Überwachung handle, die in den meisten Kantonen unter den gleichen Voraussetzungen zulässig war wie die Telefonüberwachung. Dieser Ansicht kam entgegen, dass die meisten kantonalen Prozessgesetze darauf verzichteten, näher zu umschreiben, was unter einer technischen Überwachung zu verstehen ist.

IV. Der Einsatz von GovWare nach StPO ^

1. Die gesetzliche Grundlage für die Überwachung des Telefonverkehrs ^

[Rz 14] Dass es sich bei Internet-Telefonie um Fernmeldeverkehr im Sinn von Art. 269 Abs. 1 StPO handelt, ist offensichtlich.[6] Es kann bei der Frage, ob deren Überwachung zulässig ist, nicht darauf ankommen, welche Übertragungswege und welche Technologien eingesetzt werden. Internet-Telefonie fällt wie konventionelle Telefonie unter das Fernmeldegeheimnis nach Art. 43 des Fernmeldegesetzes (FMG),[7] und Art. 269 StPO enthält die Rechtsgrundlage für die Aufhebung dieses Fernmeldegeheimnisses zum Zweck der Beweiserhebung im Strafprozess.

2. Die gesetzliche Grundlage für das Aufspielen von GovWare ^

[Rz 15] Höchstrichterlich bisher nicht geklärt ist die Frage, ob das Aufspielen von GovWare auf einen Computer zum Zweck der Überwachung von Internettelefonie eine zusätzliche gesetzliche Grundlage erfordert und ob es in der StPO eine solche Grundlage gibt. Diese Frage ist gegenwärtig brisant, weil die Revision des BÜPF stockt und frühestens 2013, eher erst 2014 in Kraft treten wird. Der Vorentwurf zu diesem Gesetz[8] sah eine Ergänzung der StPO vor, um eine ausdrückliche Grundlage für solche Manipulationen zu schaffen[9].

[Rz 16] Man könnte sich natürlich weiterhin auf den Standpunkt stellen, wenn Art. 269 StPO die gesetzliche Grundlage zur Überwachung von Telefonie biete und die verwendete Technologie keine Rolle spiele, dann brauche es keine zusätzliche Grundlage, um die dafür nötigen technischen Einrichtungen einzusetzen. Diese Argumentation greift allerdings meines Erachtens zu kurz: «Normale» Telefonüberwachungen verändern auf den vom Überwachten benutzten Geräten nichts, sondern leiten den Gesprächsverkehr beim Provider aus, ohne dass die vom Kunden benutzte (und ihm gehörende) Infrastruktur irgendwie manipuliert werden muss. Art. 269 StPO (wie der frühere Art. 3 des BÜPF und vor dessen Inkrafttreten die entsprechenden Bestimmungen der kantonalen Strafprozessordnungen) rechtfertigt nur die Aufhebung des Fernmeldegeheimnisses zu strafprozessualen Zwecken und liefert damit einen gesetzlichen Rechtfertigungsgrund für ein Verhalten, das sonst unter Art. 179bis StGB fallen würde. Dagegen braucht es für das Eindringen in fremde Datenverarbeitungssysteme nach Art. 143bis StGB meines Erachtens eine gesonderte gesetzliche Grundlage.

[Rz 17] Da es um geheime Beweiserhebungen geht, kommt in dieser Hinsicht nur Art. 280 StPO in Frage. Die Schwierigkeit dieser Bestimmung im vorliegenden Zusammenhang liegt darin, dass Art. 280 StPO (anders als die meisten bisherigen kantonalen Strafprozessgesetze) relativ genau

umschreibt, welche Arten von technischer Überwachung möglich sind. Art. 280 lit. a StPO meint den Einsatz von akustischen Abhörgeräten und liefert die Rechtfertigung für den Einsatz von Techniken, die sonst unter Art. 179bis StGB fallen würden. Art. 280 lit. b StPO beschreibt den Einsatz von optischen Überwachungsgeräten an nicht öffentlichen Orten und rechtfertigt Verhaltensweisen nach Art. 179quater StGB. Art. 280 lit. c StPO schliesslich betrifft den Einsatz von GPS-Ortungen.

[Rz 18] Man könnte am ehesten versucht sein, den Einsatz von GovWare unter Art. 280 lit. a StPO zu subsumieren. Eingesetzt werden aber eben keine technischen Geräte, sondern es wird in ein Datenverarbeitungssystem des Beschuldigten eingegriffen. Dessen Software wird so manipuliert, dass das dem Beschuldigten gehörende technische Gerät dazu verwendet werden kann, seine Gespräche zu überwachen. Das ist offensichtlich von der Eingriffstiefe her etwas anderes als der Einsatz von Geräten der Strafverfolgungsbehörden, und es betrifft eben einen Eingriff nach Art. 143bis StGB, für welchen Art. 280 lit. a StPO meines Erachtens keine gesetzliche Grundlage liefern kann.

[Rz 19] Dies führt zum (zugegebenermassen für den Praktiker unbefriedigenden) Ergebnis, dass die Überwachung der Internet-Telefonie mittels GovWare zurzeit mangels klarer gesetzlicher Grundlage nicht zulässig ist. Ich halte denn auch den vorgesehenen Weg des Bundesrates, die gesetzliche Grundlage mit der Revision des BÜPF zu schaffen, für richtig – in der VÜPF wäre eine solche Regelung unzulässig gewesen, weil von der Eingriffsschwere her eine Grundlage in einem formellen Gesetz erforderlich ist.

3. Die gesetzliche Grundlage für weitere Anwendungen ^

[Rz 20] Zu prüfen bleibt, ob die anderen Funktionen, mit denen GovWare ausgestattet werden kann, eine ausreichende gesetzliche Grundlage haben.

[Rz 21] Es geht zunächst um die in Deutschland heftig umstrittene Online-Durchsuchung, also die Durchsuchung von Daten auf einem Computer vom Internet aus ohne Wissen des Betroffenen. In der Schweiz erlaubt zwar Art. 246 StPO die Durchsuchung von Datenträgern, aber nach Art. 247 StPO nur mit Wissen des Betroffenen, denn dieser muss die Siegelung nach Art. 248 StPO verlangen können. Selbst wenn Art. 280 StPO also durch eine Bestimmung ergänzt würde, welche das geheime Aufspielen von Computerprogrammen auf einen Computer erlaubt, wäre damit noch keine ausreichende gesetzliche Grundlage für die Online-Durchsuchung geschaffen.[10]

[Rz 22] Das ferngesteuerte Einschalten des Mikrofons oder der Webcam eines Laptops oder eines Smartphones könnte zwar unter Art. 280 lit. a bzw. b StPO subsumiert werden, aber auch in diesem Zusammenhang gilt das bisher Gesagte: Solange die gesetzliche Grundlage fehlt, um verdeckt in Computersysteme einzudringen, ist es nicht zulässig, mittels GovWare das Mikrofon oder die Kamera eines Laptops unbemerkt einzuschalten.

V. Ausblick ^

1. Die Revision des BÜPF ^

[Rz 23] Wie bereits erwähnt, enthielt der Vorentwurf des BÜPF eine Bestimmung, welche den Einsatz

von GovWare erlauben würde. Der Bundesrat will nun offenbar diese Bestimmung insofern präzisieren, als mit solchen Programmen nur die Entschlüsselung von E-Mail-Verkehr und Internet-Telefonie möglich ist und der Deliktskatalog von Art. 286 StPO gelten soll.[11]

[Rz 24] Systematisch passt eine solche Regelung meines Erachtens eher unter Art. 280 StPO als in den Abschnitt über die Überwachung des Post- und Fernmeldeverkehrs. Damit würde einerseits klargestellt, dass zwei verschiedene Anordnungen und Genehmigungen notwendig sind (wobei in beiden Fällen eine Anordnung durch die Staatsanwaltschaft und eine Genehmigung durch das Zwangsmassnahmengericht erforderlich ist, sodass keine administrativen Schwierigkeiten entstehen). Anderseits könnte durchaus geprüft werden, ob eine technische Überwachung nach Art. 280 lit. a StPO nicht auch durch das verdeckte Einschalten des PC-Mikrofons und eine Überwachung nach Art. 280 lit. b StPO durch das Einschalten der Webcam möglich sein könnte – die Installation eigener Geräte durch die Polizei führt nicht nur zu ähnlichen Ergebnissen, sondern ist mit einem schwereren Grundrechtseingriff verbunden, weil verdeckt in die vom Beschuldigten benutzten Räume eingedrungen werden muss.

[Rz 25] Nicht einzusehen vermag ich, wieso für die Überwachung von Internet-Telefonie oder E-Mails dann (und nur dann) der Deliktskatalog von Art. 286 StPO und nicht derjenige von Art. 269 StPO gelten soll, wenn der Einsatz von GovWare erforderlich ist. Zum einen wird man bei der Prüfung der Verhältnismässigkeit der Massnahme durchaus berücksichtigen können, dass die Eingriffsschwere tiefer ist, wenn GovWare eingesetzt wird, als wenn der Gesprächsverkehr beim Provider ediert werden kann; das ist aber schon nach Art. 269 Abs. 1 lit. b StPO möglich. Zum andern ist aber der Deliktskatalog von Art. 269 StPO auf Delikte abgestimmt, die durch Überwachung des Post- und Fernmeldeverkehrs aufgeklärt werden können, der Deliktskatalog von Art. 286 StPO dagegen auf Delikte, die ein verdecktes Eindringen in das Milieu der kriminellen Gruppe erforderlich machen. Das Zweite hat mit Kommunikationsüberwachung wenig zu tun. Richtig an der Überlegung ist nur, dass der Katalog von Art. 286 StPO enger ist als derjenige von Art. 269 StPO[12], systematisch wird aber ein sachfremder Katalog angewendet. Konkret: Wieso soll es zulässig sein, eine Gefährdung des Lebens nach Art. 127 StGB durch Überwachung des Telefonverkehrs über Swisscom aufzuklären, nicht aber durch Überwachung des Gesprächsverkehrs über Skype?

2. Die Revision der VÜPF ^

[Rz 26] Die Verordnung zur BÜPF soll bereits auf 1. Januar 2012 revidiert werden.[13] Das Vorhaben eilt, weil auf Grund eines Entscheides des Bundesverwaltungsgerichtes die Provider zurzeit mangels klarer gesetzlicher Grundlage nicht verpflichtet werden können, an einer Internetüberwachung mitzuwirken.

[Rz 27] Die Verordnungsrevision wird keine Bestimmung zur Überwachung von verschlüsselter Internettelefonie und insbesondere keine Rechtsgrundlage für den Einsatz von GovWare liefern, und zwar zu Recht: Ein solcher Grundrechtseingriff muss auf Gesetzesstufe geregelt werden. Ausdrücklich geregelt sind künftig Antennensuchläufe[14] (Art. 16 lit. e VÜPF) und Kopfschaltungen[15] (Art. 16b VÜPF). Art. 24 VÜPF enthält nicht nur wie bisher die Bestimmungen über die E-Mail-Überwachung, sondern auch über die Überwachung des Internetverkehrs als solchem. All dies ist nicht mit einer Erweiterung der gesetzlichen Möglichkeiten der Überwachung verbunden, sondern aktualisiert den Verordnungstext nur auf Grund der heute zur Verfügung stehenden technischen

Möglichkeiten; die Anbieterinnen haben also eine gewisse Rechtssicherheit darüber, welche Pflichten sie zu erfüllen haben.

3. Die Revision des BWIS ^

[Rz 28] Ursprünglich war geplant, in der Revision zum Bundesgesetz über die Wahrung der inneren Sicherheit BWIS[16] eine ausdrückliche Rechtsgrundlage für die Online-Durchsuchung im Rahmen von vorbeugenden Massnahmen zur Bekämpfung von Kriminalität, welche die innere Sicherheit gefährdet, zu schaffen. Die mittlerweile in Bearbeitung stehende dritte Vorlage[17] verzichtet zu Recht auf dieses Instrument. Es wäre denn auch nicht sinnvoll, im BWIS Möglichkeiten für Eingriffe zu schaffen, deren Ergebnisse im Strafverfahren mangels gesetzlicher Grundlage nicht verwendet werden können.

4. Das PolAG ^

[Rz 29] Auch der Vorentwurf des Bundesgesetzes über die polizeilichen Aufgaben des Bundes[18], das eine neue und einheitliche Rechtsgrundlage für die Aufgaben der Polizeibehörden des Bundes schaffen soll, enthält keine Bestimmungen über den Einsatz von GovWare.

VI. Schlussbetrachtung ^

[Rz 30] Der Einsatz von GovWare zur verdeckten Beweiserhebung ist nach der geltenden Rechtslage in der Schweiz zurzeit noch nicht möglich. Die Revision des BÜPF und die damit verbundene Ergänzung der StPO sollen diese Lücke schliessen, wobei (wohl vorwiegend aus politisch-taktischen Gründen) die GovWare auch in Zukunft in der Schweiz nur dazu verwendet werden soll, Internet-Telefonie und verschlüsselten Mailverkehr überwachen zu können.

[Rz 31] Das Misstrauen gegen solche Massnahmen scheint (wenn man die Medienberichte für repräsentativ hält) gegenwärtig noch gross zu sein. Einmal mehr entsprechen sich Medienecho und tatsächliche praktische Bedeutung der geplanten Massnahmen nicht: Natürlich wird es auch in Zukunft nicht darum gehen, den Internet-Verkehr von Leuten zu überwachen, die pornografische Seiten besuchen. Es sollen auch nicht in grossem Stil Computer «gehackt» werden, um harmlose Leute auszuspionieren. Es geht ausschliesslich darum, das bereits vorhandene Instrumentarium zur verdeckten Beweiserhebung im Bereich der Kommunikationsüberwachung und allenfalls der technischen Überwachung der aktuellen technischen Entwicklung anzupassen. Weiterhin werden verdeckte Beweiserhebungen nur im Rahmen eines Strafverfahrens bei Bestehen eines konkreten Tatverdachtes auf schwere Straftaten von der Staatsanwaltschaft angeordnet werden können, eine Bewilligung des Zwangsmassnahmengerichtes wird in jedem Einzelfall erforderlich sein.

[Rz 32] Die Erfahrungen in Deutschland zeigen, dass der Einsatz von GovWare auch dann, wenn eine saubere gesetzliche Grundlage vorliegen wird, nicht zu einem Massengeschäft werden dürfte: In Deutschland wurden bisher offenbar nur einige Dutzend Einsätze durchgeführt, wobei es nur in einem Drittel der Fälle überhaupt gelungen ist, tatsächlich Daten an die Strafverfolgungsbehörden auszuleiten. Der Einsatz der Software ist zudem ausgesprochen teuer: Offenbar sollen in Deutschland Kosten von 10'000 bis 15'000 Euro pro Einsatz nur für die Software anfallen – zu beachten ist dabei, dass die Auswertung der Daten unter Umständen noch teurer sein dürfte[19]. Die

Strafverfolger in der Schweiz werden sich also auch in Zukunft auf konventionelle Überwachungen konzentrieren und GovWare nur in ausserordentlich schweren Fällen einsetzen, nämlich dann, wenn alle andern Mittel der Beweiserhebung versagen.

Dr. Thomas Hansjakob ist Erster Staatsanwalt im Kanton St. Gallen, Verfasser eines Kommentars zu BÜPF und VÜPF und war Mitglied verschiedener Arbeitsgruppen des Bundes, die sich mit geheimen Beweiserhebungen befassten.

---

[1] SR 780.11.

[2] Bundesgesetz über die Überwachung des Post- und Fernmeldeverkehrs (BÜPF), SR 780.1.

[3] Unterlagen auf http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2011/2011-11-23.html.

[4] So die Definition bei Wikipedia (besucht am 16. November 2011).

[5] Vom Chaos Computer Club wurde allerdings darauf hingewiesen, dass die in Deutschland eingesetzten Programme offenbar Sicherheitslücken auf den betroffenen Computern öffnen, die auch von Schadprogrammen ausgenützt werden können.

[6] SCHMID, StPO, Praxiskommentar, N. 1 vor Art. 269; HANSJAKOB in DONATSCH/HANSJAKOB/LIEBER, Kommentar zur StPO, N. 3 zu Art. 270; sinngemäss JEAN-RICHARD-DIT-BRESSEL in BSK-StPO, N. 15 zu Art. 269.

[7] SR 784.10.

[8] Abrufbar unter http://www.admin.ch/ch/d/gg/pc/documents/1719/Vorlage.pdf.

[9] VE Art. 270bis StPO: «[1] Sind bei einer Überwachung des Fernmeldeverkehrs die bisherigen Massnahmen erfolglos geblieben oder wären andere Überwachungsmassnahmen aussichtslos oder würden die Überwachung unverhältnismässig erschweren, so kann die Staatsanwaltschaft auch ohne Wissen der überwachten Person das Einführen von Informatikprogrammen in ein Datensystem anordnen, um die Daten abzufangen und zu lesen. Die Staatsanwaltschaft gibt in der Anordnung der Überwachung an, auf welche Art von Daten sie zugreifen will. [2] Die Anordnung bedarf der Genehmigung durch das Zwangsmassnahmengericht.»

[10] Zwar kann man sich fragen, ob geheime Durchsuchungen unter gewissen Rahmenbedingungen möglich sind (vgl. dazu HANSJAKOB: Geheime Erhebung von Beweisen nach StPO, Forum poenale 2011 S. 303); solange aber eine rechtliche Grundlage für das geheime Aufspielen von GovWare fehlt, ist eine Online-Durchsuchung schon aus diesem Grund nicht zulässig.

[11] Vgl. die Medienmitteilung in http://www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2011/2011-11-23.html.

[12] Insbesondere gibt es seit Einführung der StPO keine Straftaten mehr, die mittels verdeckter Ermittlung aufgeklärt werden dürfen, nicht aber mittels Telefonüberwachung.

[13] Vorlage zurzeit unter http://www.ejpd.admin.ch/content/dam/data/sicherheit/uepf/vorentw-vuepf-d.pdf.

[14] Vgl. dazu BGE 130 II 249 und die Hinweise bei HANSJAKOB in DONATSCH/LIEBER/HANSJAKOB (Fn.6), N. 13 zu Art. 269.

[15] Vgl. dazu BVGE vom 10. März 2009, A-2335/2008.

[16] SR 120.

[17] «BWIS II reduziert», vgl. BBl 2010 7841.

[18] Bericht und Vorentwurf unter http://www.bfm.admin.ch/content/dam/data/pressemitteilung/2009/2009-11-271/erlaeuterungen_27-11-09d.pdf.

[19] Vgl. dazu http://www.spiegel.de/netzwelt/netzpolitik/0,1518,799407,00.html.

Rechtsgebiet(e):	Fernmeldewesen. Fernmeldenetze; Informatik und Recht; Strafprozessrecht
Kategorie:	Beiträge
Erschienen in:	Jusletter 5. Dezember 2011
Zitiervorschlag:	Thomas Hansjakob, Einsatz von GovWare – zulässig oder nicht?, in: Jusletter 5. Dezember 2011 [Rz]