

Zeitschrift: Reihe Kriminologie / Schweizerische Arbeitsgruppe für Kriminologie =
Collection criminologie / Groupe suisse de travail de criminologie

Herausgeber: Schweizerische Arbeitsgruppe für Kriminologie

Band: 24 (2006)

Artikel: Kontrolle und Überwachung von Inhalten bei elektronischen oder
telefonischen Verbindungen aus der Strafvollzugsanstalt

Autor: Ruf, Marcel

DOI: <https://doi.org/10.5169/seals-1051083>

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

Download PDF: 13.01.2026

ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>

MARCEL RUF

KONTROLLE UND ÜBERWACHUNG VON INHALTEN BEI ELEKTRONISCHEN ODER TELEFONISCHEN VERBINDUNGEN AUS DER STRAFVOLLZUGSANSTALT

Zusammenfassung

Ein Bereich von zunehmender gesellschaftlicher, wirtschaftlicher aber auch kriminalistischer Bedeutung betrifft die modernen Kommunikations- und Informationstechnologien. Mit jedem Fortschritt steigt auch automatisch das Missbrauchspotenzial. Dies zeigte sich an Hand der Beiträge während der Kriminologie-Fachtagung «Mehr Sicherheit – weniger Freiheit?» in Interlaken im Jahre 2003.

Hier steht der Staat im Spannungsfeld von Sicherheit und Freiheit. Der Autor versucht, dieses Spannungsfeld auf den geschlossenen Strafvollzug zu übertragen. Nebst einem historischen Rückblick sollen speziell die elektronischen Kommunikations- und Informationsmöglichkeiten für Gefangene in Strafanstalten erläutert und auf deren Risiken hingewiesen werden. Im Detail wird dabei der Missbrauch von illegal eingeschmuggelten Mobiltelefonen beleuchtet. Trotz der diversen Missbrauchsmöglichkeiten sollten die elektronischen Mittel aber auch nur dort eingeschränkt werden, wo eine angemessene Kontrolle bzw. Überprüfung nicht möglich ist.

Oberste Priorität haben auch hier:

- Schutz der Bevölkerung und insbesondere der Opfer
- die Sicherheit der Strafanstalt sowie deren Mitarbeiter und Gefangene
- die Gewährleistung des geordneten gesetzeskonformen Freiheitsentzuges

Contrôle et surveillance du contenu des connexions électroniques et téléphoniques vers l'extérieur des établissements pénitentiaires

Le domaine des nouvelles technologies de la communication et de l'information prend de plus en plus d'importance, que ce soit socialement, économiquement, mais aussi criminologiquement. Tout progrès a pour corollaire une augmentation automatique des risques d'abus. Cet état de fait a été démontré au cours de la conférence du groupe suisse de travail de criminologie, intitulée «Plus de sécurité – moins de liberté?», qui s'est tenue à Interlaken en 2003.

Dans cette situation, l'Etat doit mettre en balance la sécurité et la liberté. L'auteur a essayé d'appliquer cette pesée d'intérêts au domaine de l'exécution des peines en milieu fermé. Outre un aperçu historique, les possibilités de communication et d'information électroniques offertes aux détenus, de même que les risques qui en découlent, doivent être mentionnés. A cet effet, on s'intéressera plus particulièrement aux utilisations abusives de téléphones mobiles introduits illégalement en milieu fermé. Malgré les diverses possibilités d'utilisation abusive qui en découlent, les

moyens de communication électroniques ne devraient toutefois être limités que dans les cas où un contrôle ou une surveillance appropriés ne sont pas possibles. La priorité absolue doit également être donnée aux domaines suivants:

- La protection de la population et plus particulièrement de la victime
- La sécurité de l'établissement pénitentiaire, de même que celle de ses employés et des détenus
- La garantie d'une privation de liberté conforme à la loi

Sollen wir alles dürfen, was man machen könnte?

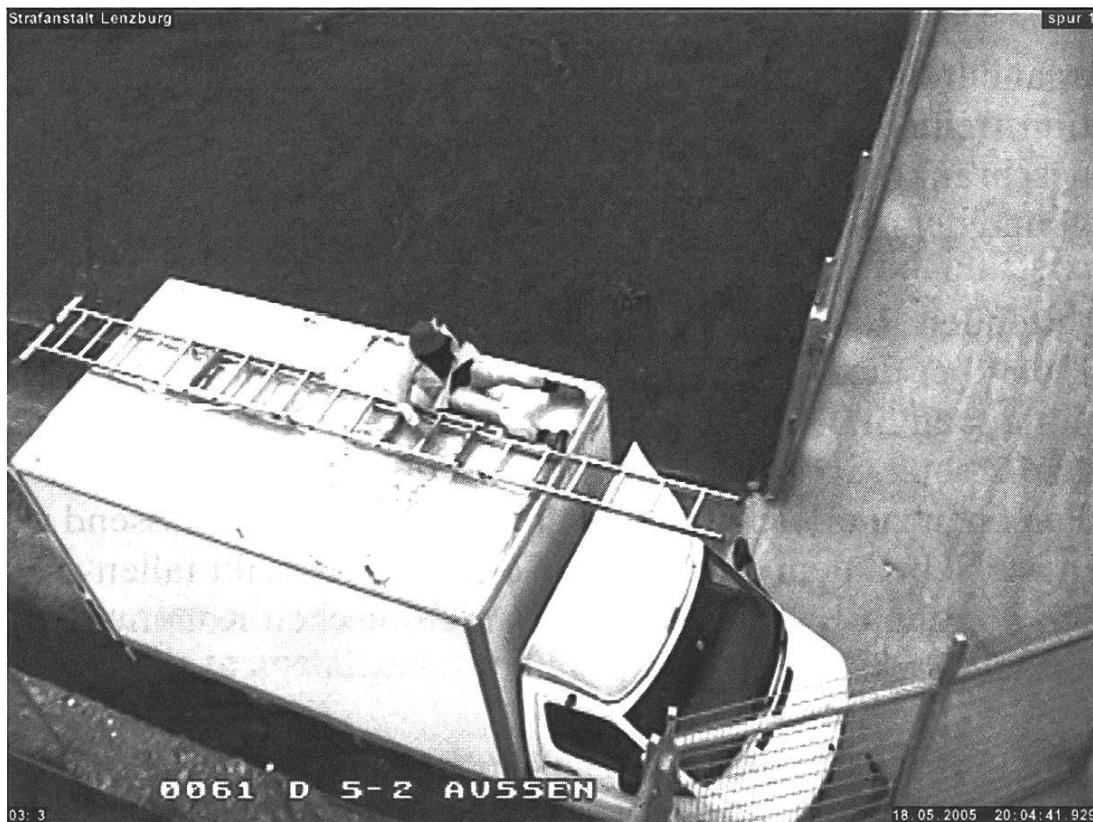
Diese Frage stellt sich einem Anstaltsleiter einer Strafanstalt täglich in vielen Bereichen des Vollzugsalltages, speziell im geschlossenen Vollzug. Die technischen Möglichkeiten zur Maximierung der Sicherheit innerhalb und ausserhalb der Institution sind noch längst nicht ausgeschöpft. Andererseits eröffnen Lockerungen des Vollzugsrahmens den Gefangenen neue Gelegenheiten und Chancen, diese zu missbrauchen. Um dieser Missbrauchsgefahr zu begegnen, ist es wiederum unerlässlich, Gegenmassnahmen, meist technischer Art, zu ergreifen. Dies bedingt eine intensive Schulung des Vollzugspersonals, und zwar aus zwei Gründen: erstens führt nur die Vertrautheit mit der neuen Technik zur deren Akzeptanz und somit zu deren korrekten Anwendung, und zweitens ist der Mitarbeitende zu sensibilisieren, um Missbräuche aller Art zu unterbinden.

Die Bedeutung der Aufrechterhaltung der Kontakte Gefangener mit der Aussenwelt ist in der Schweiz seit langem anerkannt. Besonders gefördert werden die Beziehungen der Gefangenen zu ihrer Familie und zum Freundes- und Bekanntenkreis. Der Vollzugszweck, die Anstaltsordnung und Sicherheitserwägungen setzen diesen Kontakten allerdings Grenzen. Der Kontakt zur Aussenwelt wird zudem über den Bezug von Presseerzeugnissen und den Empfang von Radio und Fernsehen aufrechterhalten, ferner auch durch persönliche Kontakte (Briefe, Pakete, Telefonverbindungen, Besuche). Die wichtigste Form des Kontaktes mit der Aussenwelt ist die Gewährung von Urlauben.

In der heutigen Zeit ist es – vor allem für die junge Generation – nicht mehr vorstellbar, ohne moderne Kommunikationsmittel wie Telefon, Fax, Internet, Handy etc. zu leben, und es ist leicht nachvollziehbar, dass sich auch die Gefangenen die neue Technik zu Nutze machen wollen. Entsprechend sind die Handys mit den SMS- und MMS-Diensten nicht nur der Klingeltöne wegen äusserst begehrt.

Im vorliegenden Bericht wird nur Bezug auf die elektronischen Kommunikationsmittel genommen, die je nach Anwendungsart oder -ort legal oder illegal sein können.

Im Speziellen wird dabei auf die Mobiltelefontechnik eingegangen, da diese in den letzten fünf Jahren zu einem nicht zu unterschätzenden Risikofaktor geworden ist. Fluchtvorbereitungen und Fluchthilfen sind damit wesentlich effizienter, kurzfristiger zu planen und mit den herkömmlichen Mitteln nicht mehr zu kontrollieren.



Befreiungsversuch vom 18. Mai 2005

Wie effizient Mobiltelefone sein können, zeigte sich bei den Jugendunruhen im Sommer 2005 in Frankreich. Trotz grossem Aufgebot der Sicherheitskräfte konnten die Jugendlichen per SMS-Gruppenruf kurzfristig auf Veränderungen reagieren und die Massnahmen der Polizei unterlaufen.

Gesetzliche Rahmenbedingungen

Meinungen und Informationen, die durch keines der spezifischen Kommunikationsgrundrechte wie Medienfreiheit (Art. 17 BV), Versammlungs- und Vereinigungsfreiheit (Art. 22 und 23 BV) etc. erfasst sind, fallen unter den allgemeinen Schutzbereich der Meinungsfreiheit als subsidiäres oder Auffanggrundrecht der freien Kommunikation. Im Bereich des Freiheitsentzuges sind zudem die Bestimmungen der EMRK, der Europäischen Strafvollzugsgrundsätze und die Kantonalen Bestimmungen zu berücksichtigen.

Wie jedes andere Grundrecht kann auch die Kommunikations- und Informationsfreiheit gestützt auf eine genügende gesetzliche Grundlage eingeschränkt werden, wenn der Eingriff im öffentlichen Interesse liegt und dem Gebot der Verhältnismässigkeit entspricht.

Die im geltenden Recht unübersichtlich und lückenhaft geregelten Vorschriften über die Beziehungen der Gefangenen zur Aussenwelt werden im neuen StGB in Art. 84 durch mehr oder weniger klare Grundsätze ersetzt. So ist beispielsweise der Kontakt mit nahe stehenden Personen zu erleichtern, wobei der «Kontakt» umfassend zu verstehen ist. Neben dem direkten persönlichen Kontakt fallen darunter auch Formen der brieflichen und telefonischen Kommunikation (Botschaft vom 21.9.1998, Seite 140).

Art. 84 Abs. 2 n StGB regelt die Einschränkungen: Die Kontakte können zum

- Schutz der Ordnung in der Strafanstalt und zur

- Sicherheit der Strafanstalt

beschränkt oder gar untersagt werden. Für strafprozessuale Massnahmen enthält dieser Absatz einen Vorbehalt.

Auf kantonaler Ebene finden sich entsprechende Bestimmungen in Strafvollzugsgesetzen und Strafvollzugsverordnungen (vgl. z.B. die Verordnung über den Vollzug von Strafen und Massnahmen des Kantons Aargau vom 9. Juli 2003, § 68 ff.).

- § 68:

7. Kontakt zur Aussenwelt:

- a. Post- und Fernmeldeverkehr:

1. Der Post- und Fernmeldeverkehr der Gefangenen wird kontrolliert. Der Verkehr mit Behörden sowie bevollmächtigten oder amtlich als Rechtsbeistand ernannten Anwälten und Anwältinnen wird inhaltlich nicht überwacht.
2. Die Vollzugsanstalt kann aus Sicherheitsgründen den Umfang der täglichen Post und den Adressatenkreis beschränken. Sie regelt den Fernmeldeverkehr.

- § 69:

- b. Besuche:

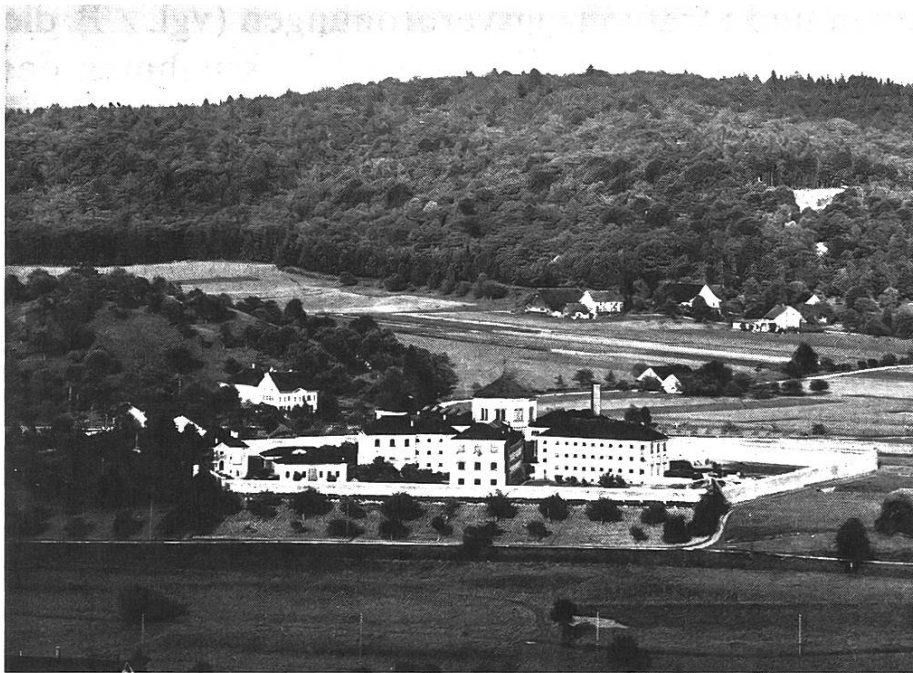
1. Die Gefangenen dürfen mit Bewilligung der Anstaltsleitung Besuche von Verwandten und nahen Bezugspersonen empfangen.
2. Die Hausordnung bestimmt die Besuchsmodalitäten und kann insbesondere Einschränkungen bezüglich der Häufigkeit, der Dauer der Besuche und der Anzahl der Besuchenden vorsehen.

Die verschiedenen Kontakte sind in den Einzelheiten in Hausordnungen sowie in anstaltsinternen Richtlinien und Merkblättern geregelt.

Halten wir jedoch, bevor wir in die Praxis gehen, eine kurze Rückschau in die Vergangenheit des Strafvollzuges sowie der Informa-

tionstechnik, die beide im Laufe der Zeit sehr starke Entwicklungen durchlaufen haben.

Geschichtlicher Rückblick: Strafvollzug



Strafanstalt Lenzburg – gebaut 1864 / Aufnahme aus dem Jahre 1882

Bis in die späten Sechziger und Siebziger Jahre des 20. Jahrhundert waren sämtliche Kontakte zur Aussenwelt für Strafgefangene stark eingeschränkt bzw. waren gänzlich verboten (Radio, Fernsehen). Der Freiheitsentzug sollte für den Missetäter nebst dem Entzug der Freiheit auch eine Trennung bzw. Isolierung vom gesellschaftlichen Leben ausserhalb der Mauern beinhalten.

Um diesen Anstieg von Aussenkontakten in den letzten Jahrzehnten zu belegen, ziehen wir die Daten der Strafanstalt Lenzburg heran. An Hand der Brief- und Besucherkontrollen kann der markante Anstieg sehr gut dargestellt werden:

Jahr	Besuchspersonen	Briefe von Gefangenen	
		Ausgehend	Eingehend
1872	630	370	343
1891	735	421	–
1915	769	1199	–
1927	846	1708	–
1937	1317	1803	2056
1943	1343	2200	2815
1964	3085	3450	–
1982	5900	5115	–
1992	6600	6320	5850
2003	7300	8150	6230

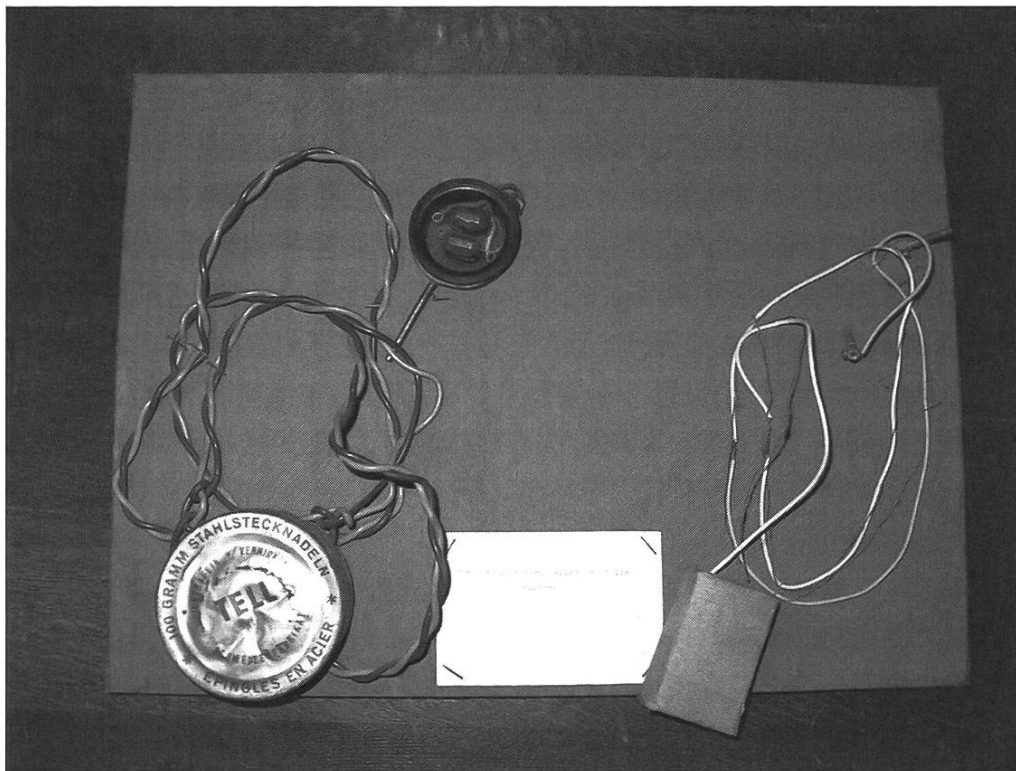
(Die Zahlen beziehen sich auf eine durchschnittliche Gefangenenzahl von 180–210.)

Was die Menge der Briefe betrifft, sind die Zahlen im 19. Jahrhundert zu relativieren, da damals nicht mehr als 2 Briefe pro Monat (Besuche 1x pro Monat) erlaubt waren. Auch war der Anteil der Analphabeten im Vergleich zu heute wesentlich höher.

Bei den Besucherzahlen (7300) ist der obere Grenzwert, was das Platzangebot im Besucherraum betrifft, erreicht. Da jedem Gefangenen ein Besucherstamm von maximal 14 erwachsenen Personen zur Verfügung steht, hat sich die Zahl der Besucherpersonen auf hohem Niveau stabilisiert.

Die enorme Zunahme des Briefverkehrs zeigt auf, dass eine Kontrolle der ein- bzw. ausgehenden Post (ca. 50 Briefe pro Tag) sehr aufwendig ist und entsprechendes Know-how (Sprachen/Fachkenntnisse etc.) vorhanden sein muss. Hier sind Sprachkenntnisse beim Personal gewünscht bzw. sollten gefördert werden.

Auch die Informationsbeschaffung war bis in die späten 60er-Jahre äusserst schwierig. Radios waren bis 1952 verboten (davon zeugen noch viele alte Basteleien, Detektor-Radioempfänger etc.).



Detektor-Radioempfänger um 1940

Zeitungen und Zeitschriften waren streng reglementiert und Telefongespräche waren nur in Ausnahmefällen möglich. Die Einführung des Fernsehens in den frühen Achtziger Jahren war ein Meilenstein in der Kommunikation und Informationsbeschaffung, wobei die Sendezeiten noch lange eingeschränkt wurden (max. bis 24.00 Uhr). In den Neunziger Jahren des 20. Jahrhunderts kamen mit PC und Spielkonsole neue technische Geräte zum Zuge.

Geschichtlicher Rückblick: Kommunikation und Informationstechnik

Um 1890 erzeugte ein gewisser Herr HERTZ mittels eines Oszillators einen Funken, der in einem Empfänger in der Nähe eine Spannung erzeugte. Aus diesem Namen heraus entstand auch der heutige Name der Funktechnik, obwohl inzwischen von keinem Mobiltelefon Funken erzeugt werden. In den letzten 30 Jahren machte die Technolo-

gie riesige nie für möglich gehaltene Fortschritte. Die Geräte wurden immer schneller und leistungsfähiger und vor allem vielseitiger.

Die Entwicklung der Mobiltelefonie in der Schweiz verdeutlicht dies:
1978: Mit der Inbetriebnahme des ersten Natel A-Teilnetzes beginnt die Erfolgsstory der Mobilfunkkommunikation in der Schweiz.

1980: Der Telefax wird versuchsweise eingeführt.

1983: Inbetriebnahme des Natel B-Netzes. Vorläufer der heutigen Handys ist ein 12kg schweres, tragbares Funktelefon in einem Koffer (max. 10 000 Teilnehmer, nie mehr als 20 Teilnehmer gleichzeitig, max. Gesprächsdauer 3 Min.).

1987: Die Lancierung des Natel C-Netzes ebnet den Weg für die moderne Mobiltelefonie.

1992: Inbetriebnahme von Natel D (GSM-Netze, digitales, zellular aufgebautes Mobiltelefonnetz).

1996: Natel Easy: erste Prepaid-Karte für Natel D.

2004: UMTS-Netz in Betrieb, Handys der dritten Generation.

Die Spirale der digitalen Welt und Ihrer neuen Technologien dreht sich immer schneller: Internet, E-Mail, GSM, GPSR, UMTS, W-LAN, WIMAX, HSDPA, SDSDH, etc., wobei der Vorrat an einfach auszusprechenden und einigermassen einprägsamen Abkürzungen nun erschöpft zu sein scheint.

Von der Theorie zur Praxis:

Folgende Informations- und Kommunikationsmittel werden praxisbezogen erläutert:

- Festnetztelefone
- TV / Radio
- PC / Laptop / PDA
- Spielekonsolen
- Mobiltelefone

Wobei sich die Angaben auf den geschlossenen Strafvollzug und nicht auf den halboffenen und offenen Vollzug oder die Ausschaffungshaft beziehen.

Festnetztelefonie

In der Strafanstalt Lenzburg verfügt der Strafgefangene über keinen freien Zugang zu Telefonkabinen. Zu Kontrollzwecken aber auch für gerichtlich angeordnete Überwachungen (2005:4) können Gespräche mitgehört werden; selbstverständlich ausgenommen davon sind Anwalts- und Sachtelefone, bei welchen nur die korrekte Verbindung kontrolliert wird. Dem Gefangenen stehen pro Woche zwei Beziehungstelefone zur Verfügung. Davon ausgenommen sind wiederum Anwalts- und Sachtelefone. Diese Praxis entspricht auch derjenigen der grössten Strafanstalt der Schweiz, der Strafanstalt Pöschwies in Regensdorf / Kanton Zürich.

Die Gesprächsgesuche müssen jeweils 3 Tage vor dem gewünschten Termin eingereicht werden, unter Angabe der vollständigen Adresse und Personalien des gewünschten Gesprächsteilnehmers. Auch bei angeordneten Kontrollen der Telefongespräche ist es von Vorteil, wenn im Personal entsprechende Fremdsprachenkenntnisse vorhanden sind. (Die Strafanstalt Lenzburg deckt momentan 14 verschiedene Sprachen ab.) Eine Vermittlung der Telefongespräche ist jedoch nur mit entsprechenden personellen und finanziellen Aufwendungen möglich.

Aber warum lässt man die Gefangenen nicht frei telefonieren? Zirka 45% der Gefangenen im geschlossenen Vollzug befinden sich im so genannten vorzeitigen Strafantritt, d.h. sie warten auf ihre Gerichtsverhandlung und sind somit noch nicht verurteilt. Sehr oft werden dabei Gefangene, welche in demselben Strafverfahren involviert sind, auf drei bis vier Anstalten verteilt (Kollusionsgefahr), und die zuständige Behörde verfügt zudem eine Telefon- bzw. Kontaktsperre.

Die Telefonsperre kann jedoch mit frei zugänglichen Telefonzellen nicht aufrechterhalten werden, wenn alle übrigen Gefangenen über Telefonkarten verfügen.

Selbst wenn die Telefonzellen für Aussenanrufe gesperrt sind, können mittels Drittpersonen und einer Konferenzschaltung sämtliche Beteiligten zur gleichen Zeit Kontakt miteinander aufnehmen. Dies wird mittels fremd vermittelten Gesprächen zu fremd bestimmten Zeiten wesentlich erschwert, wenn nicht sogar verunmöglicht. Im Weiteren ist die Gefahr sexueller Belästigungen, Drohungen und Beeinflussungen von Zeugen und Opfern über frei zugängliche Telefonzellen um ein Wesentliches höher, da selbst die Sperrung von gewissen Nummern über Drittapparate umgangen werden können.

Da die Kontaktdaten zur Telefonvermittlung bis zur Entlassung abgespeichert bleiben (Datum, Adresse und Telefonnummern, nicht die Gespräche selber), konnten auch sehr oft schon verfahrensdienliche Hinweise an diverse Polizeicorps (Drogenhandel etc.) gegeben werden. Auch bei der Flucht des Sexualstraftäters Markus W. vom 12. 1. 2006 konnte dieser dank der Adresse eines Telefonkontaktes sowie eines Besuches, welcher 12 Monate zurücklag, sechs Stunden nach der Flucht in einer Wohnung in St. Gallen verhaftet werden.

Eine Liberalisierung der Telefonpraxis hätte zur Folge, dass Absprachen zwischen den Gefangenen untereinander und zwischen Gefangenen und Zeugen nicht mehr zu verhindern wären. Eine Kontrolle von Gesprächen würde ad absurdum geführt (stundenlange Kassetten), wobei nochmals festgehalten werden muss, dass wir hier nur vom geschlossenen Strafvollzug reden. Anrufe von aussen werden aus Datenschutzgründen nicht vermittelt. Die Anrufer werden darauf aufmerksam gemacht, dass sie sich schriftlich an die Anstalt wenden können.

TV und Radio

Der Fernseher oder das Radio dürfen in der SL selbstverständlich benutzt werden. Bei den Fernsehgeräten werden jedoch nur Mietgeräte verwendet. Auf individuelle Geräte wird aus Kontroll- und Platzgründen verzichtet. Eine freie Gerätewahl würde auch zu einer Klassengesellschaft unter den Gefangenen führen. Die Fernseh- und Stereogeräte werden plombiert, damit bei einer Zellenkontrolle eine Demontage entfällt.

Dem Gefangenen stehen 55 Fernsehkanäle zur Verfügung, wobei nebst dem normalen Kabelangebot auch zwei zusätzliche Sender (albanisch/serbisch) eingemietet wurden. Mit diesem Senderangebot ist ein Grossteil der Sprachgruppen abgedeckt. Die Möglichkeit, den Gefangenen Fernseher abzugeben, hat zu einer starken, spürbaren Entspannung und Beruhigung im Anstaltsalltag geführt. Lediglich beim Videotext müssen gewisse Abstriche gemacht werden, da mit dem Videotext Nachrichten übermittelt werden können, jedoch ist keine direkte Kommunikation möglich. Dies lässt sich mit der Sperre des Videotextes leicht lösen.

PC / Laptop / PDA

Seit 1992 dürfen in der SL PCs an Gefangene abgegeben werden. Ursprünglich war die Einführung zur beruflichen Weiterbildung vorgesehen, im Laufe der letzten Jahre wurden die PC-Kenntnisse beinahe ein Allgemeingut, speziell bei den jungen Gefangenen, und diese machen bei uns 70% aus. Word, Excel, Access sind keine Fremdwörter mehr und werden in der SL auch als Anfänger- und Fortgeschrittenen-Kurse angeboten. Heutzutage sind mehr die Multimedia-Anwendungen wie Spiele, Musik, Video oder DVDs gefragt. Ein PC kann über die SL gemietet oder von draussen bezogen werden. Die Hardware wird wie folgt begrenzt:

Nicht erlaubt sind Modems (externe/interne), alle Geräte und Linkverbindungen, die der Datenfernübertragung dienen, Scanner, CD-, DVD-Brenner, mobile Speichermedien und entsprechende Kartenleser. Als Software wird nur Originalware abgegeben. Gebrannte CDs oder DVDs werden eingezogen. Vermehrt mussten bereits bei Neueintritten grosse Mengen an schwarz gebrannter Software konfisziert werden. Dies ist mit auch ein Grund, warum Brenner nicht zugelassen sind. Eine Urheberrechtsverletzung darf nicht als Kavaliersdelikt betrachtet werden, da ansonsten ganz schnell ein Handel mit gebrannter Software und Filmen aus und in der Anstalt entsteht. Insbesondere die Verbreitung von Kinderpornographie gehört dabei zu den abscheulichsten Begleiterscheinungen.

Jede von aussen angelieferte Hard- und Software wird durch den PC-Verantwortlichen der SL kontrolliert. Der PC wird ausgebaut, überprüft, anschliessend versiegelt und alle freien Modem- und Netzwerkanschlüsse verplombt. Wird auf der Festplatte eine Verschlüsselungssoftware festgestellt oder weist die Festplatte versteckte Partizipationen auf, wird der PC nicht bewilligt bzw. auf unbestimmte Zeit entzogen.

Auch bei der PC-Kontrolle gilt: ohne entsprechend geschultes und ausgebildetes Fachpersonal (IT; PC-, Programmierkenntnisse), welches ständig weitergebildet werden muss, machen Kontrollen und Tests keinen Sinn. Nur so sind gewissenhafte und glaubwürdige Kontrollen möglich. Pro Jahr werden in der SL noch ein bis zwei PCs beanstandet bzw. eingezogen.

Laptops

Laptops werden nicht bewilligt, da diese nicht geöffnet werden können, ohne die Garantiegewährleistung des Herstellers zu verletzen und den Gefangene somit zu benachteiligen. Im Weiteren besitzen die neuen Laptops seit 2003 den neuen Centrino-Chip, welcher be-

reits als Kommunikations- und Funkchip konzipiert wurde und somit für den drahtlosen Funkverkehr prädestiniert ist. Auf dem Markt gibt es auch kaum Geräte, welche keine Netzwerkkarten, Modems oder W-LAN-Vorrichtungen geschweige denn Brenner besitzen. Es sind auch keine wichtigen Belange erkennbar, die angesichts des möglichen Schadens eine Nichtgenehmigung unverhältnismässig erscheinen lässt.

Die neueste technologische Entwicklung, die HSDPA-Karte (High Speed Downlink Packet Access-Karte), zeigt auf, dass wir mit dem Verbot von Laptops auf dem richtigen Weg sind.

Das Gleiche gilt für alle Arten von PDAs (Personal Digital Assistant), welche kaum zu kontrollieren sind (Grösse, Speicherkarte, W-LAN). Der Besitz eines Terminplaners macht im geschlossenen Strafvollzug auch keinen direkten Sinn, da der Nutzen gleich Null ist.

Spielekonsolen

Seit vier Jahren werden in der SL auch Spielekonsolen zugelassen. Mit der Genehmigung ist man einem grossen Wunsch von vor allem jüngeren Inhaftierten nachgekommen, wobei auch die einfachere Kontrollmöglichkeit sowie die kleineren Dimensionen gegenüber eines PCs für die Zulassung sprachen. Lediglich der Netzwerkanschluss muss bei den Geräten verplombt werden. Softwaremässig gelten dieselben Bestimmungen wie bei den PCs.

Nicht mehr genehmigt werden jedoch die neueste Spielekonsole von Microsoft, die X-Box 360 sowie die im 2006 von Sony erhältlichen PS3. Diese Geräte besitzen nun auch bereits eine Modemfunktion, eine portable Festplatte (X-Box), sind WiFi-ready, und die PS3 hat drei Ethernet-, einen W-Lan- und Bluetooth-Anschluss.

Bei den Video-Spielen für PC und Spielekonsole gilt es, die Gewaltspiele (Ego-Shooter) aus psychiatrisch/psychologischer Sicht, speziell bei entsprechend verordneten Therapien, besonders im Auge zu behalten. Diese Spiele, zugelassen ab 18 Jahren, funktionieren nach dem Prinzip der operanten Konditionierung. Man versucht, dem Spieler das Töten beizubringen. So können gewalttätige Spiele die Neigung zu aggressivem Verhalten verstärken und emotional abstumpfend wirken.

Mobiltelefonie

Grundsätzlich sind Mobiltelefone in Strafanstalten verboten. In den letzten fünf Jahren ist der Missbrauch von eingeschmuggelten Mobiltelefonen in Strafanstalten/JVAs jedoch sehr stark angestiegen. In Deutschland versuchen mehrere Deutsche Bundesländer seit Monaten, federführend sind dabei Baden-Württemberg und Mecklenburg-Vorpommern, eine entsprechende Verordnung für den Einsatz von Störsendern in den Bundestag einzubringen.

In der Schweiz sind wir in Zusammenarbeit mit dem Bakom und den Mobilfunkanbietern schon deutlich weiter. Der Erhalt einer Konzessionsbewilligung ist nun bereits *vor* einer Gesetzesrevision des Fernmeldegesetzes möglich (die Verordnung über Fernmeldeanlagen wurde bereits angepasst). Nach den Pilotbetrieben im Sommer 2005 in Genf, Lenzburg und Zürich konnten erste erfolgversprechende Erfahrungen gesammelt werden, wobei in jeder Anstalt ein anderer Lieferant und dementsprechend unterschiedliche Resultate entstanden.

Doch wie gelangen die Mobiltelefone überhaupt in die Anstalten?

Das Einschleusen von Mobiltelefonen in Strafanstalten ist trotz sorgfältiger Kontrollen und Sicherheitsmassnahmen nicht gänzlich zu

vermeiden. Über betriebliche Transporte von draussen, Postpakete etc. sind Möglichkeiten gegeben, um entsprechende Waren einzuschleusen. Auch werden über die Besucher Einzelteile sowie ganze Handys unbemerkt eingeschmuggelt, da immer weniger Metallbestandteile verwendet werden. Allein die Grösse und die Gewichte der Handys haben in den letzten Jahren stark abgenommen. Das C2 von Siemens mit Jahrgang 1988 wog satte 7 Kilos. Um die Jahrtausendwende lag das Durchschnittsgewicht bereits unter 100 Gramm.

Nach meiner Einschätzung wird sich das Mobiltelefon in naher Zukunft (5–10 Jahre) entmaterialisieren. Möglich macht das die Polymer-Technik – dann sind Funkchips aus Plastik, die auf beliebige Gegenstände aufgedruckt werden, Standard. Aber auch die Nanotechnologie wird die Bestandteile weiter verkleinern, bis die Mobiltelefone nahezu unsichtbar werden. Experten sprechen von «Pervasive Computing», einer alle Lebensbereiche durchdringenden Digitalisierung. Somit wird das unbemerkte Einschmuggeln zu einem Kinderspiel.

Missbrauch durch die Mobiltelefonie

Obwohl vermutlich $\frac{3}{4}$ aller Gespräche nur für private, familiäre Telefongespräche benutzt werden, ist der Missbrauch durch Mobiltelefone beinahe so umfangreich wie deren Ausrüstung. Diese Missbräuche entsprechen der Praxis und sind keine theoretische Auflistung:

- Fluchtvorbereitung, Fluchthilfe, alle Meldungen
- Bedrohung und sexuelle Belästigung von Drittpersonen
- Absprache mit Komplizen (Kollusionsgefahr)
- Umgehung von Telefonsperren
- Opferbeeinflussung vor der Gerichtsverhandlung
- Drogenhandel aus der Anstalt
- Missbrauch durch das Internet (ADSL-Kapazität) wie:
 - Kinderpornographie, Zahlungsanweisungen, Betrug
- Unerwünschte Aussenkontakte

- Foto- und Kameraaufnahmen aus der Anstalt
- Abhören von Raumgesprächen mittels Handys (manipuliert oder direkt)
- GPS-Positionsbestimmungen
- Push-to-Talk (mehrere Geräte gleichzeitig als Walkie-Talkie)
- Bei einer Geiselnahme würden für die Polizeiorgane unhaltbare Zustände entstehen

Der Schmuggel von Mobiltelefonen hat aber auch grossen Einfluss auf die Ruhe und Ordnung innerhalb der Anstalt. Da pro Gerät CHF 1000.– geboten werden, führt es immer wieder zu Auseinandersetzungen und Streitigkeiten, da viele Lieferungen den Besteller trotz Bezahlung nicht erreichen, was sehr oft in Drohungen, Schlägereien und Körperverletzungen ausartet.



Handy-/SIM-Kartenfunde im Jahr 2005

Welche technischen Möglichkeiten gibt es, um den Handymissbrauch zu unterbinden?

Einsatz mobiler/stationärer Detektoren



Die Detektoren sind bei uns seit vier Jahren in Verwendung, doch der Einsatz eines mobilen Detektors zum Aufspüren von aktiven Mobiltelefonen ist nur bedingt geeignet. Die Erfassung kurzer Telefonate oder SMS ergeben keine genaue Ortsangabe. Bei der genauen Detektion der Mobiltelefone spielt der Faktor Glück eine grosse Rolle. Auch gibt es Örtlichkeiten, welche nicht jederzeit kontrolliert werden können, ohne entsprechendes Aufsehen zu erzeugen. Man benötigt seit 2005 nun bereits zwei verschiedene Geräte (UMTS/ GSM). Eine ähnliche Lösung basiert auf stationären Detektoren pro Zelle/Raum. Auf einer zentralen Erfassung wird jeder Handykontakt raumbezogen angezeigt.

Abschirmung der Gebäulichkeiten

Diese Lösung würde ein Gebäude durch entsprechende Abschirmung (Faradayscher Käfig) vor externen Strahlungsfeldern schützen. Diese Variante ist für Altbauten völlig ungeeignet. Zusätzlich würde der Funkverkehr des Sicherheitsdienstes auch in Mitleidenenschaft gezogen.

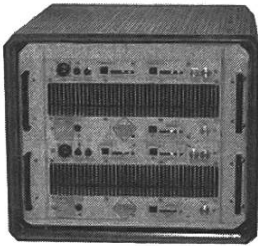
Einsatz mehrerer Mobiltelefon-Störsender

Das Gerät sendet Störsignale aus, mit denen die Signale eingehender und ausgehender Gespräche überlagert werden. Das Gerät ist für den Gebrauch in einzelnen Räumen oder Sälen konzipiert und kann keine ganzen Hausbereiche stören.

Einsatz einer Mobiltelefon-Störanenne

Hier handelt es sich um eine Antenne und den entsprechenden Sender. Die Antenne stört während deren Betriebszeit ständig alle Mobiltelefon-Frequenzen. Eine Antenne auf dem Anstaltsgelände würde den ganzen Anstaltsbereich abdecken (stört Umfeld zu stark).

Stationäre Detektion und Störung(Jammer)



Durch entsprechende Detektion eines Verbindungsaufbaues wird die anschliessende Störung durch kurzzeitige Emission eines Störsignales durchgeführt.

Mobiltelefonantenne mit Provider zusammen betreiben

Zusammen mit allen Providern (Swisscom, Sunrise, Orange usw.) würden mehrere Mobiltelefonantennen auf dem Areal betrieben. Die Antennen müssen von den Providern geliefert werden. Somit hätten wir die Möglichkeit, alle Anrufe in einem definierbaren Bereich zu lokalisieren und die Telefonrufnummern festzustellen. Eine Unterbindung der Anrufe erfolgt nur, wenn der Besitzer innerhalb der Anstalt lokalisiert wird. Dies benötigt eine enge Zusammenarbeit mit den Providern. Die Provider verfügen jedoch nicht alle über die entsprechenden technischen Mittel und Fachleute.

Ortung mittels Funkwellenerfassung ab Gebäudefront



Dieses System wird in der JVA Gelsenkirchen (D) betrieben. Eine Antenne auf dem Gefängnisgelände, welche auf die Zellenfenster gerichtet ist, erkennt die Funkwellen und leitet die Information an den Computer der Sicherheitszentrale weiter (nur Detektion). Die Anlage ist

für die räumlichen Bedingungen der SL denkbar ungeeignet, da sehr viele Antennen benötigt würden (teuer). Nach einer längeren Evaluationsphase in 2003/2004 entschlossen wir uns für den Einsatz eines Jamming-Systems für den Pilotbetrieb im Jahre 2005. Umso mehr, da dieses System auch den UMTS-Telefonverkehr erfolgreich stören kann.

Jamming

Grundsätzlich ist das Stören oder Unterdrücken von mobiler funkbasierter Kommunikation wie gesehen auf mehrere Arten möglich. Bei der Jamming-Technik wird das zu übertragende Funksignal durch einen Jammer (Störsender) gestört. Dabei gibt es verschiedene Methoden, doch nicht jede ist für den Einsatz in Strafanstalten gleich gut geeignet. Speziell innerhalb von Städten gibt es durch das anfallende Störsignal Probleme. Auch die Bauweise der Anstalten (Baumaterial etc.) spielt eine grosse Rolle.

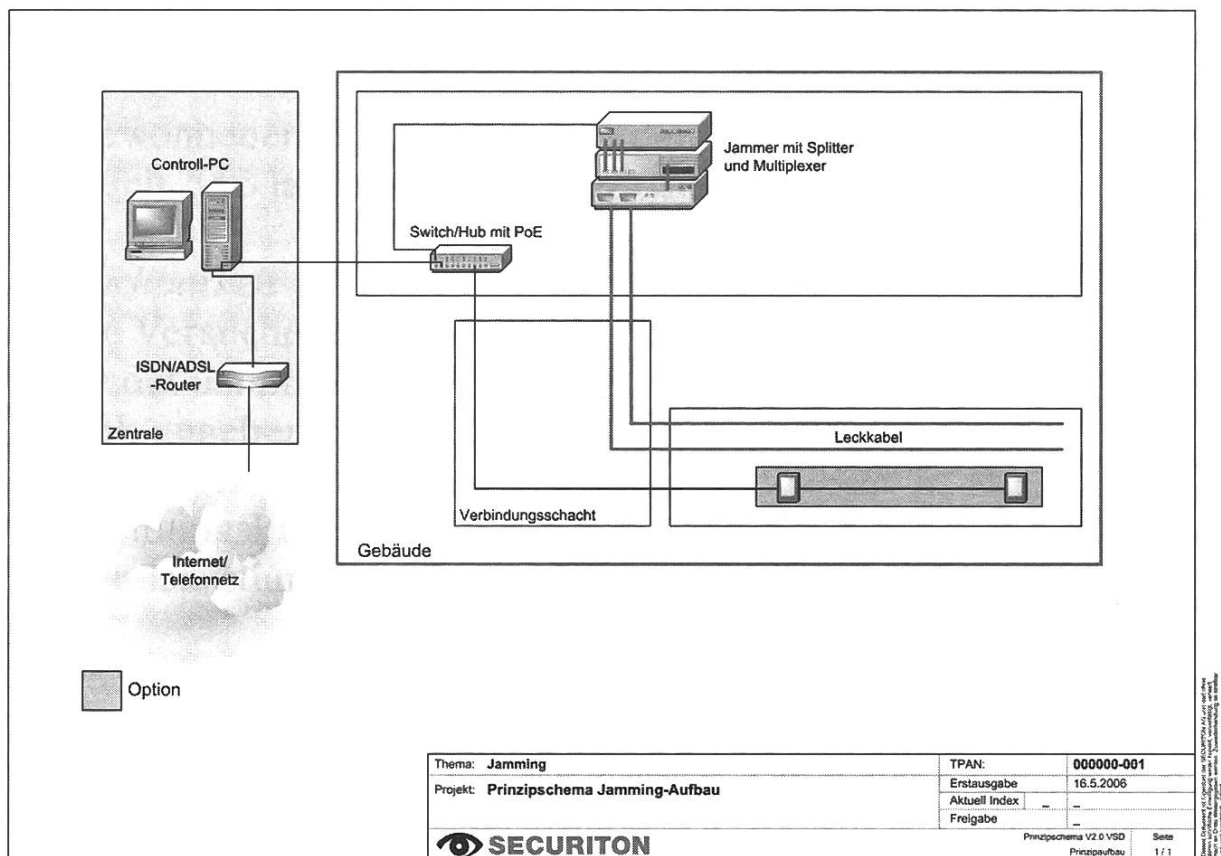
Herausforderung

Es sind mehrere Herausforderungen als Hürde bei der Realisierung zu nehmen. Nachfolgend sind die wichtigsten aufgelistet:

- Stören der heute verfügbaren Kommunikationssysteme, aber auch der Zukunft (GSM, UMTS, W-LAN, WiMax)
- Keine Störung angrenzender Benutzer von mobiler Kommunikation ausserhalb der Strafanstalten
- Es werden nur so genannte Down-Link-Systeme bewilligt
- Höchst mögliche Abdeckung innerhalb der Strafanstalt (indoor) mit Störsignal
- Berücksichtigung der baulichen Gegebenheiten, welche in Strafanstalten für die Ausbreitung von Funkwellen alles andere als ideal sind
- Die anderen Frequenzbänder dürfen nicht gestört werden
- Keine Dauerstörsignale
- Aufzeichnung der Störungen müssen vorhanden sein
- Abschaltung muss jederzeit möglich sein
- Die NIS-Grenzwerte müssen eingehalten werden

Grundlagen

In der Schweiz sind die Technologien GSM (900 MHz resp. 1800 MHz) sowie neu auch UMTS (2200 MHz) im Einsatz, wobei auch die W-LAN-Technologie (Hotspots) beachtet werden sollte. Der Aufbau des Jamming Systems erfolgt nach folgendem Schema:

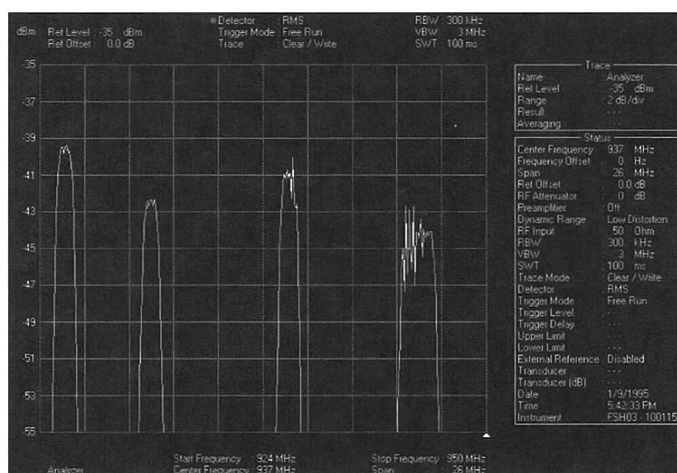
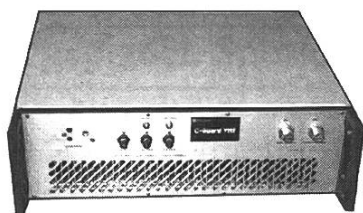


Systemaufbau

Die Jammer, Sensoren und der Kontroll-PC werden über ein separates Ethernet Netzwerk verbunden. Über dieses Netzwerk wird das System konfiguriert, werden durch die Sensoren erkannte Kommunikationsversuche gemeldet und Daten zur Koordination unter den Jammern ausgetauscht.

Ein Kernelement der verwendeten Jammer ist das kanalselektive Jammen. Dabei werden nur jene Kanäle gestört, welche von den

Providern im GSM oder UMTS-Netz zur Kommunikation am jeweiligen Standort verwendet werden. Die Störleistung wird ganz gezielt abgegeben im Gegensatz zum breitbandigen Jammer. Zudem wird nur dann gestört, wenn ein Kommunikationsversuch eines Mobiltelefons erfolgt und auch nur für 30 Sekunden und die Strahlenbelastung wird auf einem absoluten Minimum gehalten.



Spektrum beim kanalspezifischen Stören

NIS-Messung

Betreffend Strahlenbelastung muss bei einer Handystöranlage auf die NISV-Verordnung speziell geachtet werden. Am 1. Februar 2000 hat der Bundesrat die Verordnung über den Schutz vor nicht ionisierender Strahlung (NISV) in Kraft gesetzt. Der Vollzug der NIS-Verordnung obliegt im Falle von Jamming dem jeweiligen Kanton. Der Anlagengrenzwert (AGW) liegt bei 5V/m.

Der Grenzwert innerhalb der Wohnzellen bei der vorgeschlagenen Lösung wurde beim Pilotbetrieb bei Weitem unterschritten, da durch

den Einsatz von kanalselektiven Jammern die Leistung pro Kanal eingestellt und schmalbandig abgegeben wurde. Die abgegebene Störleistung pro Kanal wird so eingestellt, dass das Störsignal nur geringfügig stärker ist als am jeweiligen Standort die empfangene Leistung des Providersignals von Swisscom, Orange oder Sunrise.

Pilotbetrieb Sommer 2005

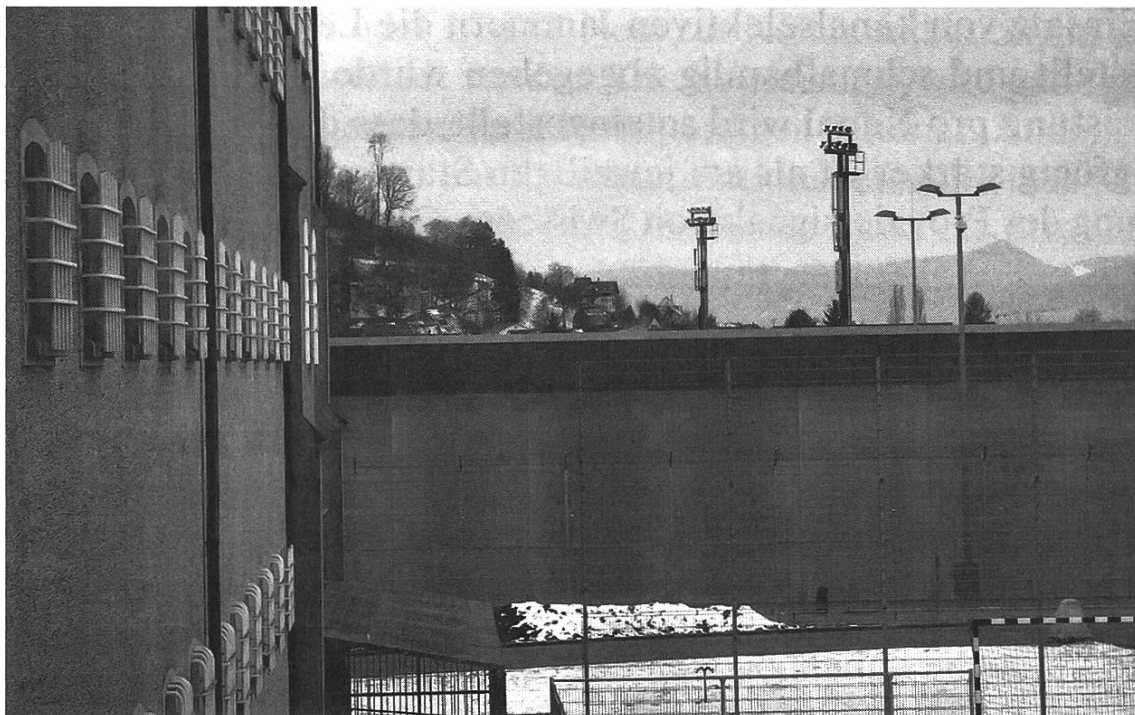
Die gewonnenen Erkenntnisse aus dem Pilotbetrieb in den Monaten Mai – Juli 2005 lassen sich wie folgt zusammenfassen:

1. Machbarkeit

Die Versuche haben gezeigt, dass eine technische Machbarkeit für das Jamming von GSM900-, GSM1800- und UMTS-Mobilfunk gegeben ist. Die Störwirkungen ausserhalb einer Anstalt oder Anlage können durch gezielten Einsatz der Antennen/Strahlungskabel und optimierte Einstellung der Parameter (Sendeleistung, Empfindlichkeit) minimiert werden.

2. Design der Anlage

Für eine optimale Wirkung ist ein professionelles und umfassendes Design von zentraler Wichtigkeit. Die genaue Verlegung des Strahlungskabels oder der Antenne(n) ist sehr stark von den baulichen Gegebenheiten abhängig und je nach Situation unterschiedlich. Die Signale in den Zellen sind diffus durch Reflexionen. Wegen den höheren Dämpfungswerten bei Strahlungskabeln bei höheren Frequenzen ist dort mehr Signalleistung erforderlich. Speziell problematisch waren die nahen Antennenstandorte (200m) von Swisscom und Sunrise. Speziell der UMTS-Sender verursachte einige Schwierigkeiten.



Antennenstandorte vor der Anstalt

3. *Einsatz von kanalspezifischen Störsendern (engl. «channel-specific jamming»)*

Für eine Realisierung mittels Jammern sollte der Einsatz von schmalbandigen, kanalspezifischen Sendern gewählt werden. Die jeweils zu störenden Frequenzen der nahe liegenden Basisstationen lassen sich somit spezifisch konfigurieren und sind auch problemlos für neue Frequenzen bzw. Mobilfunknetze einsetzbar (WIMAX, W-LAN etc.). Das Gerät wird dazu einfach mit einer neuen Karte ausgerüstet.

4. *Praxisbezogene Ergebnisse innerhalb der Anstalt*

Der HSI, der Handyschmuggelindex, fiel innert Tagen von CHF 1000.– auf unter CHF 400.–. Inzwischen hat sich der Markt erholt und ein Mobiltelefon wird wieder für CHF 800.– angeboten. Die Zellenplätze im betroffenen Flügel waren vorübergehend äusserst unbeliebt, da der Empfang effektiv unterbunden wurde.

5. *Ein Gegenangriff auf eine Störanlage*

mittels Peilantennen ausserhalb der Anstalt ist aus folgenden Gründen sehr unrealistisch:

- Die Antennen müssten von Drittpersonen sehr nahe an der Anstalt montiert werden können.
- Der Verbindungsaufbau würde trotzdem detektiert und die Signale der Antenne erfasst.
- Bei keinem erfolgreichen Stören des Funkverkehrs würden die entsprechenden Räumlichkeiten überprüft (innerhalb/ausserhalb).

Nachdem wir nun per Ende Februar ein Gesuch für eine Funkkonzession eingereicht haben, hoffen wir – vorausgesetzt ist grünes Licht vom Bakom – im Sommer 2006 die Handystöranlage in Betrieb zu nehmen.

Fazit

Gesamthaft lässt sich die Problematik der Informations- und Kommunikationstechnologie in Strafanstalten wie folgt zusammenfassen:

- Man muss sich von Seiten der Anstalt mit der Materie intensiv befassen und nur diejenigen Mittel freigeben, welche man auch entsprechend kontrollieren kann, ein Rückschritt wäre wesentlich schwieriger.
- Den Missbrauch, welcher in den Anstalten auf verschiedenste Art und Weise vorhanden ist, erkennt und gewillt ist, im Sinne der Vorsorge zu bekämpfen (Prävention).
- Man muss Mut beweisen, erste Schritte einzuleiten, bevor man von den Ereignissen dazu gezwungen wird. Dies klappt jedoch nur, wenn von der politischen Seite her auch die entsprechenden finanziellen und rechtlichen Mittel zur Verfügung gestellt werden.

Nachstehend einige Abkürzungen zum besseren Verständnis:

GSM (Global System for Mobile Communications) wurde 1982 vom CEPT, einer Arbeitsgruppe mit dem Namen Groupe Spéciale Mobile ins Leben gerufen mit der Aufgabe, eine Spezifikation für ein Europäisches Mobilfunksystem zu erarbeiten. GSM sollte alle analogen Mobilfunknetze ersetzen. Im Jahr 1987 fiel dann auch die Entscheidung zu Gunsten der digitalen Technik. Im Sommer 1992 gingen dann die ersten Mobilfunknetze an den Start. Die ersten GSM-Netze arbeiteten im Frequenzbereich um 900 MHz. Etwas später kam dann die Technik für ein GSM-1800 im Frequenzbereich um 1800 MHz hinzu, das unter der Bezeichnung DCS-1800 bekannt ist.

HSCSD (High Speed Circuit Switched Data), eine Erweiterung des GSM-Standards, ist ein kanalvermittelnder Datendienst. Zur Datenübertragung werden gleichzeitig mehrere GSM-Funkkanäle genutzt.

GPRS (General Packet Radio Service) ist ein paketorientierter Datendienst zur Datenübertragung im GSM-Netz. Im Gegensatz zu HSCSD basiert GPRS auf der Vermittlung einzelner Datenpakete und nicht auf der Schaltung fester Übertragungswege. Dieser Datendienst ist daher besonders für dialogorientierte Anwendungen, WAP- i-modeTM und E-Mail geeignet.

SMS: Mit SMS (Short Message Service) können Textnachrichten an Mobilfunkteilnehmer in aller Welt versendet wurden. Bis zu 160 Zeichen dürfen die Kurzmitteilungen umfassen.

EMS: Eine EMS-Nachricht (Enhanced Messaging Service) besteht aus mehreren aneinander gereihten SMS-Nachrichten. Daraus resultiert, dass auch Mitteilungen mit weit mehr als 160 Zeichen versendet werden können.

MMS (Multimedia Message Service) ist eine Weiterentwicklung von SMS und EMS. MMS ermöglicht mit Hilfe gesteigerter Mobilfunk-

Bandbreiten die Übertragung von farbigen Bildern (Digital-Fotos) und kurzen Filmsequenzen auf entsprechend ausgestattete Mobiltelefone.

WAP: Das WAP (Wireless Application Protocol) und i-mode™ sind Standards zur Datenübertragung von Internet-Inhalten und Servicesdiensten (z.B. Banking, Brokerage, Information, Shopping) auf mit jeweils speziellem Browser ausgestattete Mobiltelefone, Handhelds oder PDAs. WAP beschreibt den Übertragungsstandard, der Informationen aus dem Internet an mobile Endgeräte (Handys, Organizers, Smartphones) transportieren und darstellen kann.

i-mode™ ist ein aus Japan kommender Datendienst und ermöglicht wie WAP den mobilen Internet-Zugang.

UMTS (Universal Mobile Telecommunications System) ist Teil der IMT-2000-Familie, dem Dachbegriff für die dritte Generation der Mobilfunksysteme. UMTS wurde von der Europäischen (ETSI) und der Japanischen (ARIB) Standardisierungsorganisation initiiert. Besonders die Japaner hatten es eilig, da Engpässe im japanischen Mobilfunknetz zu befürchten waren. Deshalb ging im Oktober 2001 das erste öffentliche UMTS-Netz an den Start. UMTS ist die zukünftige drahtlose Breitband-Technik, die Multimedia-Dienste zur Verfügung stellen und GSM ablösen soll. Die Technik basiert auf einer paketorientierten Vermittlung und dem Internet-Protokoll. Damit soll eine effektive Bandbreitennutzung ermöglicht werden, um die Voraussetzung für neue mobile Kommunikationsdienste zu schaffen:

- Videokonferenz
- Interaktives Entertainment
- Bild-Telefonie
- Internet-Zugang
- Finanzdienstleistungen
- E-Mail / Voice-Mail
- E-Commerce
- Punkt-zu-Mehrpunktkommunikation (Broadcast)

Bluetooth ist ein offener Industriestandard (vgl. IEE 802.15.1-2002 [1]) für ein lizenzfreies Nahbereichsfunkverfahren zur kabellosen Sprach- und Datenkommunikation zwischen IT-Geräten (Kabelersatz und Ad-hoc-Networking).

WiMax (der viel versprechende grosse Bruder von WLAN): Öffentlich zugängliche Wireless-Local-Area-Netzwerke (W-Lan) findet man mittlerweile in Universitäten, Hotels, Bahnhöfen, Flughäfen und neuerdings auch in Zügen. In der Schweiz gibt es gegen 1500 Hotspots, dazu kommen noch unzählige private Funknetze – Tendenz stark steigend. Solche Netze ermöglichen den drahtlosen Zugriff vom Notebook über eine mobile Funk-Verbindung aufs Internet und Intranet. Voraussetzung dafür sind eine W-Lan-Karte mit Mini-Antenne und eine W-Lan-Antenne in der Umgebung. Die lokalen Funknetze haben eine Reichweite von etwa 100 Metern und Übertragungsraten von max. 2 Mbits. WiMax arbeitet mit Mikrowellen und das ist ein Nachteil. Für genügend Bandbreite sorgt jedenfalls der zweite Datenturbo. WiMax ist bis zu 40 Megabytes schnell und steht für «Worldwide Interoperability for Microwave Access». Bei dieser Mikrowellenfunktechnik handelt es sich um eine Weiterentwicklung des bekannten W-Lan-Standards, der hier zu Lande bereits Hunderte von Hotspots zum Funken bringt. Salopp könnte man WiMax als einen gigantischen Hotspot bezeichnen, der das drahtlose Surfen nicht nur in der Hotellobby, sondern auch in Quartieren, ja in ganzen Städten oder Landstrichen ermöglichen wird (bis 50 km Reichweite).