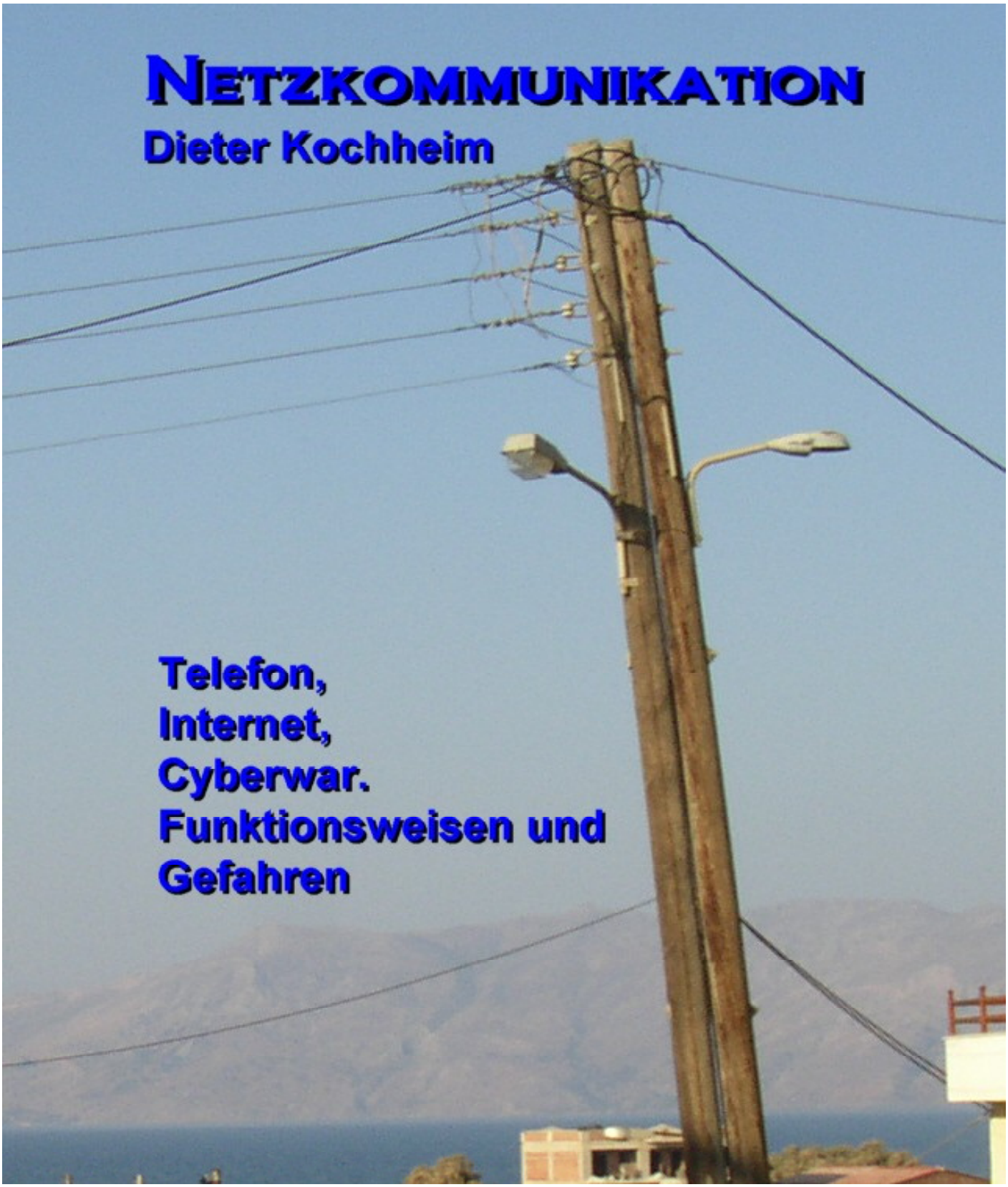

Netzkommunikation
Dieter Kochheim
Telefon,
Internet,
Cyberwar.
Funktionsweisen und
Gefahren

Die Zitate in den Fußnoten, das Inhaltsverzeichnis und einzelne Textpassagen sind im PDF-Dokument mit Links unterlegt, die einen einfachen Zugriff auf die Quellen oder eine Bewegung im Dokument zulassen. Sie erscheinen in blauer Farbe. In ausgedruckter Form sind die Quellen leider nicht sichtbar.

Thema:	**Netzkommunikation**
Autor:	Dieter Kochheim
Version:	1.01
Stand:	10.07.2010
Cover:	„Netzlast“ (Kissamos, Kreta, 2003), D. Kochheim

Impressum: **CF**, cyberfahnder.de

Sprach- und Datenkommunikation. Cyberwar

Was passiert, wenn man telefoniert oder Dateien aus dem Internet lädt? Die Techniken und Protokolle mögen sich unterscheiden. Durch konvergente Entwicklungen ist die Sprach- und Datenkommunikation miteinander verwachsen und beide nutzen dieselben physikalischen Verbindungswege.

Das Arbeitspapier gibt einen Überblick über die verschiedenen Formen der Telekommunikation unter den Schwerpunkten der Adressierung und der technischen Infrastruktur im Hintergrund. Es beginnt mit der analogen und digitalen Telefonie, beschreibt die technischen Grundlagen der Mobilnetze und endet zunächst mit den Grundlagen der Internettechnik (Kapitel 1. bis 4.).

Die beiden anschließenden Kapitel befassen sich mit den weltweiten Kabelnetzen und dem Routing, das die Grundlage für eine effiziente Netzverwaltung bildet (Kapitel 5. und 6.).

Kapitel 7. beschäftigt sich mit der Verschlüsselung und den wichtigsten Aspekten des Zusammenwirkens von Netztechnik und Verschlüsselung.

Darauf baut das Kapitel 8. auf, das sich mit der Zensur im Internet und den Maßnahmen von Schurkenprovidern beschäftigt.

Den Schluss bildet eine Auseinandersetzung mit den Gefahren eines Netzkrieges, dem Cyberwar. Die heutigen Erkenntnisse lassen es erwarten, dass sich die Methoden im Cyberwar nicht groß von denen der Cybercrime unterscheiden werden, so dass in seiner ersten unterschwelligen, noch „Kalten Phase“ bevorzugt Hacking, DoS-Angriffe, Malware, Botnetze und das Social Engineering zum Einsatz kommen. Sie dürften mit zunehmender Eskalation um geheimdienstliche, terroristische und militärische Methoden erweitert werden.

Wird der Cyberwar definiert als eine gezielte, zerstörerische Auseinandersetzung mit den Mitteln und gegen die gegnerischen Infrastrukturen der Netzkommunikation, so umfasst der Begriff nicht nur militärische Akteure, sondern auch politische Aktivisten, Unternehmen und die organisierte Cybercrime. Er ist gekennzeichnet vom der strategischen Einsatz der Informations- und Kommunikationstechnik mit dem Ziel, Gegner und Opfer existenziell zu schädigen, also nicht nur ihre Datenverarbeitung und Netzkommunikation zu stören oder auszuschalten, sondern ihre Funktionstüchtigkeit insgesamt.

Dabei dürften sich anfangs die Akteure kaum unterscheiden. Ob die Hinterleute kriminelle, terroristische oder militärische Ziele verfolgen, dürfte unerheblich sein, weil sie zunächst auf die kriminellen Fachleute zurückgreifen werden, der sich die Organisierte Cybercrime bereits jetzt bedient.

Deshalb komme ich auch zu dem Schluss, dass der erste Schritt in der Bekämpfung des Cyberwar in der grenzüberschreitenden Bekämpfung der Cybercrime besteht.

Die erste Textfassung habe ich handschriftlich unter kretischer Sonne geschrieben. Dabei habe ich mir einige Abschweifungen erlaubt, weil ich den Eindruck hatte, dass sie zum Thema gehören, ohne zwingend nötig zu sein. Wieder zuhause habe ich den Text überarbeitet, die eine oder andere Unstimmig- und Unrichtigkeit verbessert und die Anmerkungen hinzugefügt. Verbleibende Fehler bitte ich den besonderen Umständen des Entstehens nachzusehen.

Mit der Netzkommunikation lege ich jetzt den dritten zusammenfassenden Bericht über die Hauptthemen des Cyberfahnders vor. Das **Arbeitspapier Skimming** hat bereits einige Resonanz verursacht. Dasselbe erwarte ich von dem **Arbeitspapier Cybercrime**, in dem Elemente aus vier Jahren Berichterstattung zusammen gekommen sind. Das vorliegende Arbeitspapier hat eine mehr strategische Ausrichtung, weil es die Notwendigkeit des Begreifens der technischen Prozesse und der Gefahrenabwehr in den Vordergrund stellt.

Kolymbari, Hannover
Juni 2010

Es gibt bestimmte Aufgabenstellungen, vor denen wir als Forscher tatsächlich zurückschrecken. Weil wir sagen, wenn wir auf diesen Gebieten forschen, und das, was wir herausfinden tatsächlich veröffentlichen, dann laufen wir Gefahr, dass wir Angreifer schlau machen. Und dann müssen wir vielleicht sogar teilweise die Verantwortung dafür übernehmen, dass ein Angriff auf eine bestimmte Art und Weise passiert. Wenn sich ein paar Experten zusammensetzen und Szenarien überlegen, kommen da oft verblüffend einfache Lösungen für Angriffe heraus, die dann von Terroristen mit Sicherheit begierig aufgegriffen werden könnten. Deshalb meinen wir, solche Themen kann man wirklich nur dann in voller Breite bearbeiten, wenn man wesentliche Ergebnisse – also solche, die potenziellen Angreifern nützlich sein könnten – unter Verschluss hält.

Jürgen Beyerer [1]

[1] Bei: Wolfgang **Stieler,** "... verblüffend einfache Lösungen für Angriffe", Technology Review 26.03.2007;
siehe auch: FBI sieht ernsthafte Bedrohungen aus dem Cyberspace, Heise online 07.01.2009

1. Analoge Welt

Bei der Kommunikation per Netz geht es darum, mindestens zwei räumlich voneinander getrennte Partner durch eine technische Infrastruktur so miteinander zu verbinden, dass sie Sprach- oder andere Nachrichten miteinander austauschen können. Das trifft bereits auf die indianischen Rauchzeichen oder die nautischen Signale per Flaggen oder mit Leuchtsignalen per Morsecode zu. Mit ihnen lassen sich Nachrichten über Entfernungen übermitteln, soweit sich die Partner darauf verständigt haben, welche Bedeutungen sie dem einzelnen Zeichen und ihren Abfolgen beimessen wollen. Das ist noch heute so. In der digitalen Welt sind die Zeichen Signale und die Codierungen sind Protokolle.

Für die analoge Telekommunikation wurden exklusive Kabelverbindungen von einem zum anderen Ende geschaffen [2], zunächst von Hand gestöpselt vom „Fräulein vom Amt“ und dann elektromagnetisch geschaltet von Relais in Verbindungsstellen [3]. Den Schlüssel dafür lieferte die Telefonnummer [4].

Den Zahlen auf der Wählscheibe sind verschieden lange elektrische Impulse zugewiesen gewesen, mit denen elektromagnetische Schalter in definierte Stellungen gebracht wurden. Mit der Ziffernfolge wurde schließlich das Zielgerät angesteuert [5].

Die Null ist eine besondere Ziffer, wenn sie den anderen Ziffern voran gestellt ist. Sie signalisiert, dass das lokale Anschlussnetz [6] verlassen und ein übergeordnetes Verbindungsnetz angesteuert werden soll [7]. Sie stellt zunächst die Verbindung zu einem Netzknoten her – heute würde man sagen: zu einem Gateway, der das Anschlussnetz des Anrufers mit dem Verbindungsnetz verknüpft, über das der Angerufene erreichbar ist.

Die Ziffernfolge nach der Null bestimmt das Zielnetz. Aus der klassischen Telefonie sind diese Ziffernfolgen als Ortsvorwahlen überliefert [8]. Jedes örtliche Netz wird als autonomes System begriffen [9], dessen Kopfstelle und Zentrale mit den Kopfstellen anderer Ortsnetze verbunden ist [10].

Die führende Null ist noch heute ein Steuerzeichen, das die Verbindung zu einem übergeordneten Netz herstellt. Zwei führende Nullen signalisieren, dass eine internationale Verbindung hergestellt werden soll. So erklären sich die Ländervorwahlen [11]. Mit der ersten Null stellt der Anrufer eine überregionale, aber nationale Verbindung her, mit der zweiten verlässt er das nationale Netz und wählt die Verbindungsstelle zu den internationalen Verbindungsnetzen an. Die folgenden zwei oder drei Ziffern bestimmen das nationale Zielnetz, die weiteren Ziffern das Subnetz (Ortsnetz, Mobilnetz) und schließlich die Anschlussnummer.

Das System der Länder- und Ortsvorwahlen sowie der Anschlussnummern zeigen deutlich die hierarchische und technische Struktur, auf dem es beruht. Jede Ziffer mit ihren unterschiedlich langen Impulsen setzt einen elektromagnetischen Schalter in Bewegung, der zu einer anderen Kabelverbindung führt. Das setzt sich auf der lokalen Ebene fort: Vom örtlichen Netzknoten zum Schaltkasten im Stadtteil und womöglich über weitere Zwischenstationen bis zum Endgerät des Angerufenen.

Die Nummerierung in Deutschland kannte in der analogen Welt nur zwei reservierte Sondernummern für die Rettungsdienste, also für die Polizei (110) und die Feuerwehr (112 [12]). Mit allen anderen Nummern steuerte der Anschlussnetzbetreiber seine Schaltstationen bis hin zum Endgerät mit elektromagnetischen Schaltern. Anhand seiner Telefonnummer konnte man ziemlich genau erkennen, in welchem Ortsteil und womöglich in

---

2 **WP**, Telefonnetz

3 **WP**, Plain old telephone service

4 **WP**, Rufnummer

5 **WP**, Nummerierung (Telekommunikation)

6 Auch: **WP**, Zugangsnetz

7 **WP**, Verkehrsausscheidungsziffer

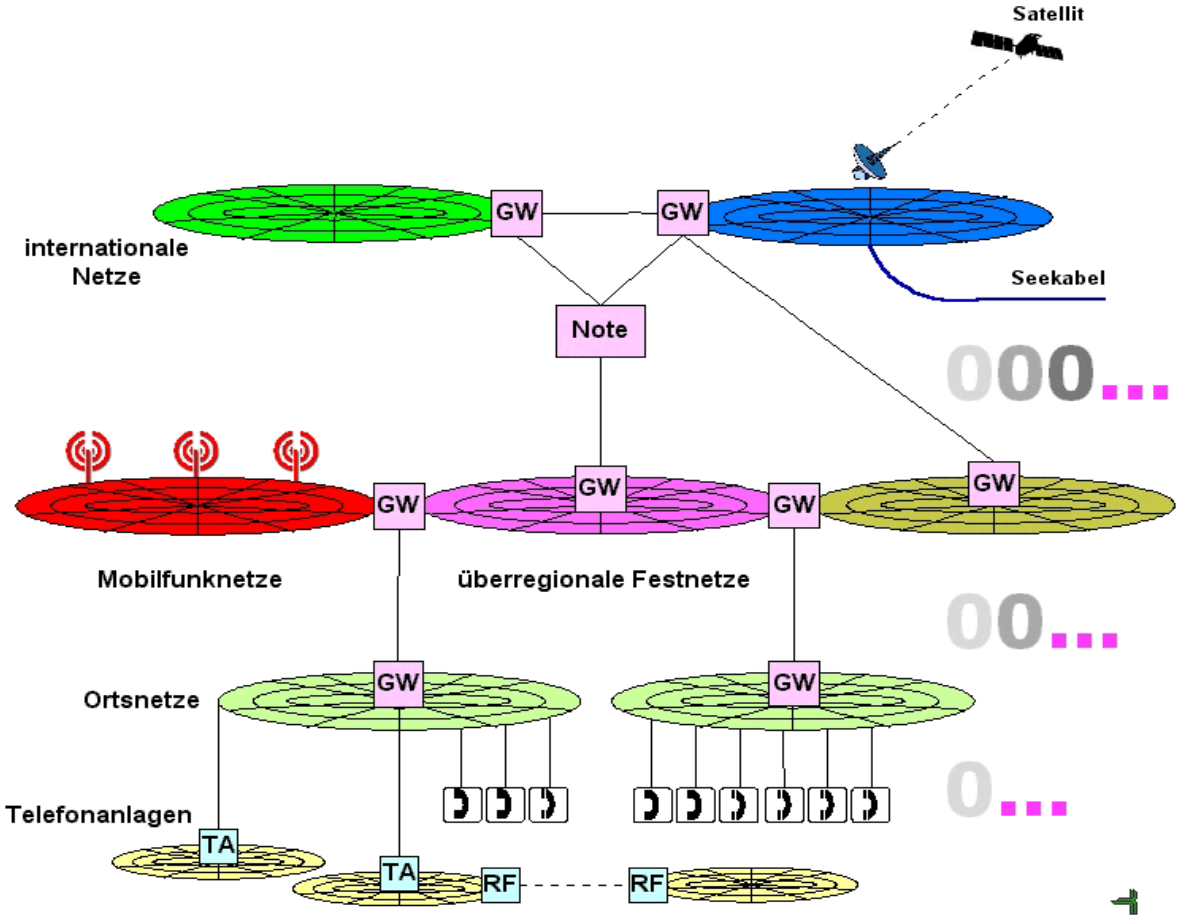
8 **WP**, Telefonvorwahl

9 Der Begriff gilt im engeren Sinne nur für Datennetze, die durch das Interetprotokoll verbunden werden: **WP**, Autonomes System.

10 **WP**, Vermittlungsstelle

11 **WP**, Ländervorwahlliste sortiert nach Nummern

12 Jetzt: **WP**, Euronotruf.



welchem Straßenzug der betreffende Anschlussinhaber wohnt, weil sie ein genaues Abbild der technischen Schaltfolge für die Relais in den Verbindungsstellen waren.

Die Nummerierung dient dem Verbindungsaufbau. Für die Kommunikation selber bedarf es eines Trägers, der die Signale überträgt. Das kennt man schon vom Dosentelefon [13]. Der Schall des Sprechers bringt den Dosenboden zum Schwingen und diese Schwingungen werden von einem straff gespannten Bindfaden zum Boden der zweiten Dose übertragen, wo sie wiederum Schall erzeugen, so dass man die Worte des Sprechers hören kann.

Der Träger der analogen Telefonie ist fließender Strom [14]. Seine Frequenz wird entweder in Bezug auf die Wellenlänge (Frequenzmodulation [15]) oder die Schwingungsgröße (Amplitudenmodulation [16]) verändert, so dass mit diesen Schwankungen der Lautsprecher beim Empfänger angesprochen wird. Aus dieser Technik leitet sich noch der Begriff des Modems ab [17]. Mit ihm werden die digitalen Daten des Computers zu akustischen Signalen „moduliert“ und so durch das analoge Telefonnetz transportiert. Das Modem beim Empfänger „demoduliert“ sie wieder zu digitalen Daten. Anders als direkt an das Telefonnetz angeschlossene Modems stellen Akustikkoppler eine Hardware-Schnittstelle zum Telefonhörer her [18] .

[13] **WP**, Schnurtelefon
[14] **WP**, Telefon, Übertragungsmedium
[15] **WP**, Frequenzmodulation
[16] **WP**, Amplitudenmodulation
[17] **WP**, Modem
[18] **WP**, Akustikkoppler

2. Digitale Welt

In den siebziger Jahren wurden die Standards für die digitale Telefonie entwickelt und die analogen Telefonnetzen zu digitalen Netzen umgewandelt. Zunächst betraf das nur die Infrastruktur im Hintergrund und seit den neunziger Jahren mit der Einführung von ISDN auch die Endgeräte [19].

Datenkommunikation und klassische Telekommunikation nutzen als physikalische Basis grundsätzlich dieselben (Glasfaser-) Kabel. Nur an den Knotenpunkten bedarf es unterschiedlicher Komponenten, die den Datenstrom spalten und die für die jeweilige Anwendung bestimmten Daten (kontinuierlicher Datenstrom: Telefonie) und Datenpakete (Internetprotokoll) aufnehmen und weiter verarbeiten. Das betrifft auch die „letzte Meile“ [20], wenn man die Breitbandtechnik beim DSL betrachtet [21]. Der Anschluss wird über Kupferkabel bis ins Haus geführt. Ein Splitter [22] trennt die Frequenzen von Telefon und DSL und führt sie zum Haustelefon einerseits [23] und für die Datenkommunikation zu einem DSL-Modem andererseits [24]. Durch neue Techniken wie Voice over IP - VoIP [25] - werden die Grenzen zwischen beiden Anwendungsbereichen weiter verwischt.

Während analoge Netze über dieselbe Verbindung sowohl die Adressierung wie auch die Kommunikation abwickeln, werden diese Funktionen im digitalen Netz getrennt. Zunächst wird das Signalisierungsnetz [26] angesprochen (D-Kanal beim ISDN [27]), um die Verbindung herzustellen. Die Sprachkommunikation verläuft dann über andere Stationen im Kommunikationsnetz (B-Kanal [28]). Die Signalisierung dient nur zu Schaltung, Aufrechterhaltung und Abrechnung der Kommunikationsverbindung.

Aus den analogen Netzen haben die digitalen die Netzvorwahlen übernommen. Sie adressieren aber nicht nur aneinander gekoppelte Anschluss- und Verbindungsnetze, sondern vor allem auch verschiedene Betreiber [29] und besondere Dienste [30].

Das Rückgrat der Verbindungssteuerung in digitalen Telefonnetzen bilden - statt Schaltkästen mit verdrahteter Logik - Router [31], die mit der Signalverwaltung [32] und Datenbanken verbunden sind. Die Datenbanken verwalten die Nummern und geben Auskunft darüber, in welchem Netz und auf welchem Weg der angewählte Zielpunkt zu erreichen ist [33]. Nur in solcher Art unterstützten „Intelligenten Netzen“ [34] sind Rufnummernmitnahmen [35], Mehrwertdienste [36] und besondere Dienste wie Shared Cost [37], MABEZ [38] (vor allem Televoting [39]) oder Auskunftsdienste [40] (Kurzwahlen [41]) überhaupt erst möglich geworden.

Router sind intelligente Netzwerkkomponenten [42], die gezielte Verbindungen in Kabelnetzen (und Funknetzen) herstellen. Darin unterscheiden sie sich von den veralteten Hubs [43], die eingehende Daten ungeprüft an alle angeschlossenen Gegenstellen weiterleiten, die ihrerseits prüfen müssen, ob sie den Endanschluss verwalten oder erreichen können.

---

19 **WP**, Integrated Services Digital Network - ISDN

20 **WP**, Letzte Meile

21 **WP**, Digital Subscriber Line - DSL

22 **WP**, DSL-Weiche

23 **WP**, Network Termination for ISDN Basic rate Access – NTBA;
WP, Telekommunikations-Anschluss-Einheit – TAE

24 **WP**, DSL-Modem

25 **WP**, IP-Telefonie

26 **WP**, Signalling System 7

27 **WP**, D-Kanal

28 **WP**, B-Kanal

29 Carrier; **WP**, Telefongesellschaft.

30 **BNA**, Nummernverwaltung

31 **WP**, Router

32 **WP**, Signalling Transfer Point - STP

33 **WP**, Service Control Point - SCP

34 **WP**, Intelligentes Netz

35 **WP**, Rufnummernmitnahme

36 **WP**, Mehrwertdienst;
CF, Nummertricks. 1900-Nummern. Abrechnung. Missbrauch

37 Jetzt: **WP**, Service-Dienste.

38 **WP**, MABEZ

39 **WP**, Televoting

40 **BNA**, Liste der Anbieter von Auskunftsdiensten

41 **WP**, Kurzwahl

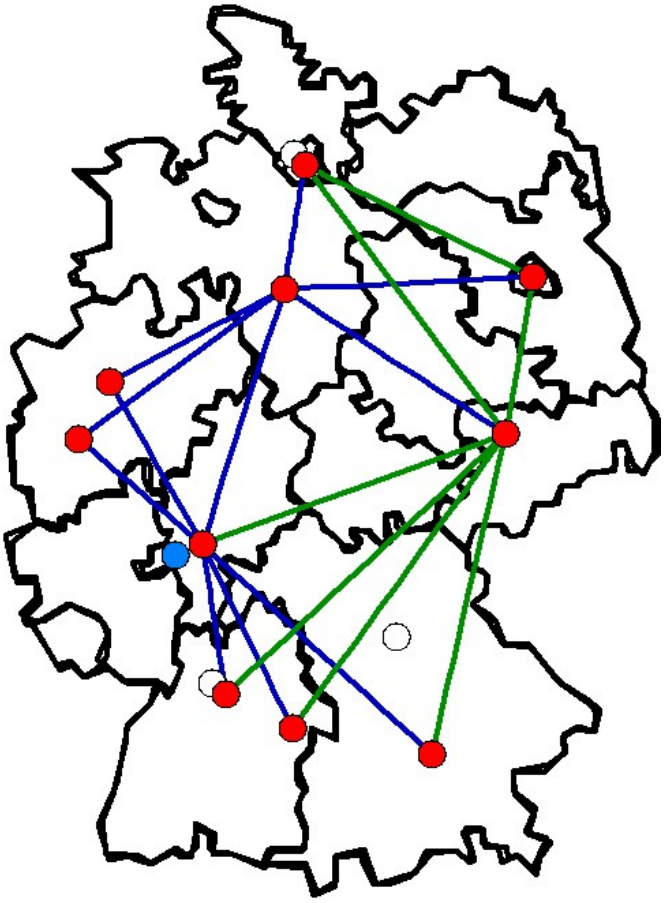
42 **Kochheim**, Cybercrime, 2010; IT-Sicherheit, Schwachstellen, Angriffe (S. 6 unten)

43 **WP**, Hub (Netzwerk)

Die Rufnummern werden in Deutschland von der Bundesnetzagentur [44] zugeteilt und verwaltet. Sie vergibt, mit Ausnahme der MABEZ-Nummern, die nur für eine zeitlich begrenzte Besonderheit freigeschaltet werden (Televoting), und Kurzwahlen für Auskunftsdienste, die Rufnummern blockweise an die großen Provider ab [45]. Mehrwertdienst-, Rückruf- [46] und andere Dienstnummern werden dann zumeist über Reseller [47], also „Wiederverkäufer“ in der Fläche vertrieben.

Die großen Anschlussnetzbetreiber sind zur Rechnungsstellung für Dritte wegen derer besonderen Dienste gegenüber ihren Endkunden verpflichtet (§ 45h TKG). Dazu werden ihnen die Verbindungskosten noch während der laufenden Verbindung von dem Inhaber des betroffenen Rufnummernblocks im Onlineverfahren übermittelt. Das ist besonders wichtig wegen der Mehrwertdienste, deren Gebühren nicht nur für die technische Verbindung selber entstehen, sondern einen maßgeblichen Anteil für die Dienstleistung (Auskünfte, Beratung, Download) enthalten, die unter der Nummer angeboten werden. Solche „Premiumdienste“ sind zunächst auch unter Fax-Anschlüssen angeboten worden und seit einigen Jahren auch als SMS [48].

Im Hinblick auf die technische Infrastruktur, die sie zur Verfügung stellen, wird zwischen den Betreibern von Anschluss- und Verbindungsnetzen unterschieden. Anschlussnetze sind solche, die sich auf die Erreichbarkeit von Endkunden konzentrieren [49]. Das sind vor allem die Betreiber von Ortsnetzen und die Mobilnetzbetreiber. Verbindungsnetze stellen vor allem überregionale, internationale und weltweite Verbindungen her. Als früherer Monopolist beherrscht die DTAG [50] noch immer den deutschen Anschlussnetzmarkt („Letzte Meile“), betreibt daneben auch das stärkste nationale Verbindungsnetz (siehe Schaubild).



Als größter Anschlussnetzbetreiber in Deutschland verfügt die DTAG über drei redundante Datenbanken für die intelligente Netzsteuerung in verschiedenen Orten, in denen die Standort- und Gebührendaten ihrer Kunden gespeichert sind. Redundanz bedeutet hier, dass sie über den gleichen Datenbestand verfügen und sich jedenfalls kurzfristig wegen der laufenden Änderungen abgleichen.

Die doppelte oder dreifache Datenhaltung ist dann unsinnig, wenn dieselben Daten mehrfach erhoben und verwaltet werden müssen. Diese Art von Redundanz gilt es im Wege der Datenbankpflege zusammen zu führen. Redundanz im Sin-

---

44 **BNA**, Aufgaben der Bundesnetzagentur; füher: Regulierungsbehörde für Telekommunikation und Post – RegTP.

45 Wenn hier vereinfacht von „Providern“ gesprochen wird, dann sind alle drei Grundtypen gemeint: Zugangsprovider (§ 8 TMG) stellen nur die Netzinfrastruktur zur Verfügung, Inhaltsprovider (§ 7 TMG) veröffentlichen Inhalte im eigenen Namen und sind dafür voll verantwortlich und Hostprovider (§ 10 TMG) stellen den Speicherplatz für Dritte zur Verfügung. Für rechtswidrige Inhalte sind sie nur verantwortlich, wenn sie sie kennen und dann nicht unverzüglich gesperrt haben.

46 **WP**, Callback (Telekommunikation); siehe auch: **Kochheim**, ebenda, kostenpflichtige Rückrufe (S. 29).

47 **WP**, Wiederverkäufer

48 **WP**, Short Message Service. Premium-Dienste

49 Siehe auch: **CF**, TK-Netze, 2007

50 **WP**, Deutsche Telekom

ne davon, Ausfallsysteme und Lastverteilungen zu schaffen, sind hingegen bei systemkritischen Anwendungen im Interesse der Daten- und Betriebssicherheit zwingend notwendig. Von der „chaotischen“ Redundanz unterscheidet sich diese Form der doppelten Datenhaltung auch dadurch, dass sie keine zusätzlichen Aufwände bei der Dateneingabe und Datenpflege auslösen, sondern in eine Backup-Strategie eingebunden sind.

Direkter Draht,
Rethimnon, Kreta, 2003

3. Mobile Welt [51]

Eine Besonderheit stellen die mobilen Telefonnetze dar, die alles andere als mobil sind. Mobil sind nur die Endgeräte. Das Mobilfunknetz besteht aus stationären Sendestationen. Ihre Masten verfügen rundum meistens über drei vertikale Stabantennen, die jede eine Funkzelle bedienen [52]. Die Ausdehnung und Form einer Funkzelle wird von den geographischen Gegebenheiten (Berge, Bewuchs, Gebäude) und dem Bedarf bestimmt. Auf dem flachen Land kann eine Funkzelle mehr als 30 Kilometer überstreichen, wenn klare Sicht besteht [53], in Metropolen kann sich eine Funkzelle auf einen Bahnsteig einer stark frequentierten S-Bahn beschränken.

Untereinander sind die Funkmasten mit Kabeln oder Richtfunkstrecken verbunden. Die Betreiber der Mobilfunktechnik verwenden zwar ihre eigenen Funkanlagen (Antennen und Systemtechnik), nutzen in aller Regel aber gemeinsam Funkmasten und Technikräume, die von einer gemeinsamen Betreibergesellschaft zur Verfügung gestellt werden (Site-Sharing [54]).

Die zentralen Komponenten der mobilen Netze (Mobile Switching Centre [55]) leisten noch komplexere Verwaltungsaufgaben als die im Festnetz, weil sie nicht nur die Erreichbarkeit des angerufenen Endgerätes (einschließlich Verbindungsgebühren) verwalten müssen, sondern auch die aktuelle Funkzelle, in der sich das jeweilige Endgerät befindet.

Hinzu kommt das Roaming [56]. Vereinzelt schließen sich Mobilnetzbetreiber zusammen, um ihren Kunden einen flächendeckenden Empfang zu ermöglichen, in grenznahen Gebieten können sich in- und ausländische Funkzellen abwechseln und das Handy kann sich ganz im Ausland befinden

---

51 Weitere Einzelheiten: **CF**, Mobilfunk, 23.08.2008

52 Ebenda, Funkzellen, 23.08.2008

53 Zur Nachtzeit werden gelegentlich einzelne Masten abgeschaltet, so dass die Erreichbarkeit über benachbarte Funkzellen erfolgt. Siehe auch: **CF**, Positionsbestimmung in Funknetzen, 17.09.2008.

54 **WP**, Site-Sharing

55 **WP**, Mobile-services Switching Centre

56 **CF**, Mobilfunk. Roaming, 23.08.2008

und dennoch empfangsbereit sein.

Die inländischen und grenznahen Roamingprozesse bekommt der Anschlussinhaber in aller Regel nicht mit, weil sie zwischen den Netzbetreibern abgewickelt und verrechnet werden.

Das Roaming im Ausland ist komplizierter, weil es ihm auch um die Abrechnung gegenüber dem einzelnen Kunden geht. Die wichtigste Rolle spielen dabei Clearing Houses [57]. Der ausländische Netzbetreiber erkennt anhand der IMSI [58], also der Anschlussnummer einschließlich der nationalen und der Providerkennung (maximal 15 Zeichen), die Zugehörigkeit des Anschlussinhabers. Diese Daten sendet er an das Clearing House, das seinerseits beim heimatlichen Netzbetreiber die Autorisierung abfragt. Damit wird geklärt, ob der Anschlussinhaber existiert, ob er Auslandsgespräche führen darf und ob die Kosten gedeckt sind. Nach dem Abschluss der Verbindung be- und verrechnet das Clearing House die Verbindungskosten zwischen den beteiligten Providern, damit sie der heimatliche Zugangsprovider seinem Kunden in Rechnung stellen kann.

Ansonsten weisen die mobilen Telefonnetze dieselbe Intelligenz auf wie die Festnetze. Sobald ein Handy in Betrieb genommen wird, autorisiert es sich nicht nur gegenüber der Funkzelle, in der es sich befindet, sondern gegenüber der zentralen Netzverwalung insgesamt. Beim Verbindungsaufbau wird ebenso zwischen dem Signalisierungs- und dem Kommunikationsnetz (Sprachnetz) unterschieden.

Ein erträgliches Abfallprodukt der Signalisierung ist der Short Message Service – SMS [59]. Neben den reinen Signalisierungsdaten stehen im Signalisierungssystem [60] 160 Zeichen für freie Texte zur Verfügung [61]. Das ist etwa so, wie wenn man das Feld „Verwendungszweck“ bei einer Überweisung für private Nachrichten nutzt.

Die mobile Telefonie verbindet Dank neuer breitbandiger Techniken die Sprach- mit der Datenkommunikation. UMTS [62] reicht mit einer maximalen Bandbreite von 14,4 Mbit/s fast an die Leistung von ADSL2 im Festnetz heran [63]. Die jetzt versteigerten Lizenzen [64] eignen sich für die Long Term Evolution [65] und können damit den Glasfaserkabeln in der Flächenversorgung Konkurrenz bieten.

Die Zusammenführung von Sprach- und Datendiensten wird unter dem Begriff „Konvergenz“ diskutiert [66]. Die mobilen Dienste haben damit eine Entwicklung nachgeholt, die seit der Digitalisierung des Festnetzes und seiner breitbandigen Ausrichtung [67] dort längst vollzogen worden war.

57 **CF**, Mobilfunk. Clearinghouses, 23.08.2008

58 **WP**, International Mobile Subscriber Identity - IMSI

59 **WP**, Short Message Service - SMS

60 **WP**, Signalling System 7

61 **WP**, Short Message Service. Übertragung;
WP, Signalling System 7. MAP – Mobile Application Part.

62 **WP**, Universal Mobile Telecommunications System - UMTS

63 **CF**, Netzneutralität und Breitbandtechnik. Infokasten, 08.12.2007

64 Bitkom rechnet mit raschem Ausbau des breitbandigen Mobilfunks, Heise mobil 11.06.2010

65 **WP**, Long Term Evolution

66 **WP**, Konvergenz (Telekommunikation);
CF, Netzkonvergenz, 12.02.2008

67 **CF**, Netzneutralität und Breitbandtechnik, 08.12.2007

4. Globale Welt

Es gibt keine prinzipielle Trennung mehr zwischen Sprach- und Datendiensten [68]. So nutzt die Internettelefonie – Voice over IP [69] – die im Internet übliche Adressierung und bietet damit eine kostengünstige und gleichzeitig verschlüsselte Alternative zu Telefon- und vor allem Ferngesprächen.

Eine Besonderheit der Internetkommunikation ist es, dass die Inhalte nicht in einem „Strom“, also über eine feste und exklusive Verbindung, sondern Paketweise übermittelt werden. Alle Pakete verfügen über einen Header mit dem Absender- und Empfängerdaten sowie darüber, wie ihre Vorgänger- und Nachfolgerpakete benannt sind, die am Ziel wieder zusammengefügt werden müssen. Auf der Strecke dazwischen können die Pakete unterschiedliche Strecken und Knotenpunkte durchlaufen.

Verantwortlich dafür ist das Internetprotokoll, das aus zwei wesentlichen Teilen besteht: Das Internet Protocol – IP – als solches [70], das vor allem für die Adressierung zuständig ist, und das Transmission Control Protocol – TCP [71], das für die Aufteilung und korrekte Zusammensetzung der Datenpakete sorgt. Das TCP ist es auch, das vom versendenden Gerät (oder den Zwischenstationen im Internet) nicht oder verstümmelt angekommene Datenpakete nachfordert.

TCP/IP ist bidirektional ausgelegt, auch wenn Datenpakete nur in eine Richtung gesendet werden sollen (Download, FTP [72]). Sende- und Empfangsstation müssen sich zunächst über das Protokoll verständigen, das der Kommunikation zugrunde gelegt werden soll, und beide Überwachen auch die laufende Übermittlung auf Vollständigkeit und Integrität der Datenpakete.

Der Adressierung im Internet liegt ein nummerisches System zugrunde, das eine gewisse Ähnlichkeit mit den Telefonnummern hat. Die aus Ziffern bestehende Intenetadresse [73] verfügt über vier durch Punkte voneinander getrennte Zifferngruppen, mit denen jedoch nur die Zahlen 0 bis 255 abgebildet werden können (8 Bit = 1 Byte).

Zuständig dafür ist die US-Organisation IANA [74], die die Adressen an die fünf regionalen Registrierungsstellen [75], an Zugangs- und andere Provider vergibt [76]. Dabei hat der Grundgedanke bestanden, dass das Nummernsystem auch die geographische Position widerspiegeln soll [77]. Davon hat sich die Praxis weit entfernt.

Das Réseaux IP Européens Network Coordination Centre – RIPE NCC [78] – verwaltet die Nummernblöcke, die für Europa, den Nahen Osten und Zentralasien vorgesehen sind. Es verfügt – wie die anderen RIR – über eine Datenbank, in der die Nutzer der hier verwalteten Nummernblöcke eingetragen sind [79]. Der Adresseninhaber kann sie beliebig und irgendwo einsetzen, nur muss er dafür sorgen, dass sie in seinem Netz oder bei einem Partner erreichbar ist, wenn vom

---

68 Die in den folgenden Kapiteln angesprochenen Kommunikationstechniken beziehen sich in erster Linie auf die Datenkommunikation. Auf die Besonderheiten der Sprachkommunikation (Telefonie) wird im Einzelfall hingewiesen.

69 **WP**, IP-Telefonie

70 **WP**, Internet Protocol - IP

71 **WP**, Transmission Control Protocol – TCP

72 **WP**, File Transfer Protocol - FTP

73 **WP**, IP-Adresse

74 **WP**, Internet Assigned Numbers Authority - IANA

75 **WP**, Regional Internet Registry - RIR

76 Verzeichnis der vergebenen IP-Adressen (Hauptgruppe, erste Ziffterngruppe): IANA IPv4 Address Space Registry.

77 Siehe auch: Von der IP-Adresse zur Ortsinformation, ix 08/2002

78 **WP**, RIPE Network Coordination Centre

79 Der Nummernblock 91.0.0.0 bis 91.255.255.255 ist zum Beispiel der DTAG zugeordnet: RIPE NCC, Who is (91.15.).

Internet aus mit ihr Verbindung aufgenommen werden soll.

Auf das nummerische System der IP-Adressen ist das Domain Name System – DNS [80] – aufgesetzt. Es bietet unter einer Top Level Domain – TLD [81] - eine freie, beschreibende Adressierung, die eine einfache Navigation im Internet zulässt [82].

Im wesentlichen wird zwischen generischen TLD [83] und Ländercodes unterschieden [84]. ***.com*** ist eine generische und die am meisten verbreitete TLD, die kommerziellen (comercial) Zwecken zugewiesen ist und weltweit genutzt wird [85]. ***.mil*** und ***.gov*** sind für das US-amerikanische Militär und den dortigen Verwaltungsbehörden reserviert, ***.edu*** steht für Ausbildung, Schulen und Hochschulen, ***.net*** für Netzdienste und ***.org*** für nichtkommerzielle Organisationen [86]. Die Namensräume werden ebenfalls von der IANA verwaltet, die einzelnen Adressen auf der zweiten Ebene (Second Level Domain – SLD [87]) von kommerziellen und nichtkommerziellen Zonenverwaltern [88].

.de ist die am meisten verbreitete Länderdomain [89]. Sie ist der europäischen Internetzone zugeordnet, die von dem RIPE NCC verwaltet wird. Den .de-Namensraum selber verwaltet das DeNIC [90] in Frankfurt am Main. Seiner liberalen Vergabepolitik ist die weite Verbreitung von .de-Domains zu verdanken, wobei hinzu kommt, dass die Provider, die die einzelnen .de-Adressen vertreiben und verwalten, in aller Regel äußerst günstige Preise verlangen.

DNS-Adressen müssen zunächst in die nummerischen Adressen des Internetprotokolls aufgelöst werden. Die bekanntesten Adressen – zum Beispiel von Google – sind bereits in der lokalen Hostdatei [91] verzeichnet, die sich auf jedem PC befindet und bei der Installation eines Browsers eingerichtet wird.

„Unbekannte“ DNS-Adressen werden beim Zugangsprovider abgefragt und wenn er sie nicht kennt, an die Zonen- und darüber hinaus an die zentrale Internetverwaltung weitergeleitet [92]. Sie kennt zwar nicht die genaue IP-Adresse des DNS-Namens, wohl aber die Zonenverwaltung, die für die TLD verantwortlich ist. Diese weiß wiederum, wenn sie die Verwaltung des Namensraumes übertragen hat und richtet an ihn die Anfrage weiter.

TCP/IP sorgen dafür, dass die Datenpakete über beliebige Zwischenstationen zum Zielgerät übertragen werden. Die Zwischenstationen und Strecken können dabei wechseln. Die Protokolle lassen auch Umwege zu, um die Last zu verteilen oder Störungen auszuweichen [93]. Im großen Maßstab sind die Streckenverläufe aber in aller Regel zielgerichtet, weil sie der kaufmännischen und technischen Logik der Netzbetreiber folgen.

---

80 **WP**, Domain Name System - DNS

81 **WP**, Top Level Domain - TLD

82 Zum Beispiel cyberfahnder.de.

83 **WP**, Generische Top-Level-Domains

84 **WP**, Länderspezifische Top-Level-Domains

85 Siehe auch: **CF**, Am Jahrestag wird's weniger, 13.05.2010.

86 Siehe ebenfalls: **WP**, Generische Top-Level-Domains.

87 Die Wikipedia spricht jetzt nur noch von **WP**, Domain.

88 Verzeichnis der TLD: **IANA**, Root Zone Database; Landkarte mit den Ländercodes (bei united-domains).

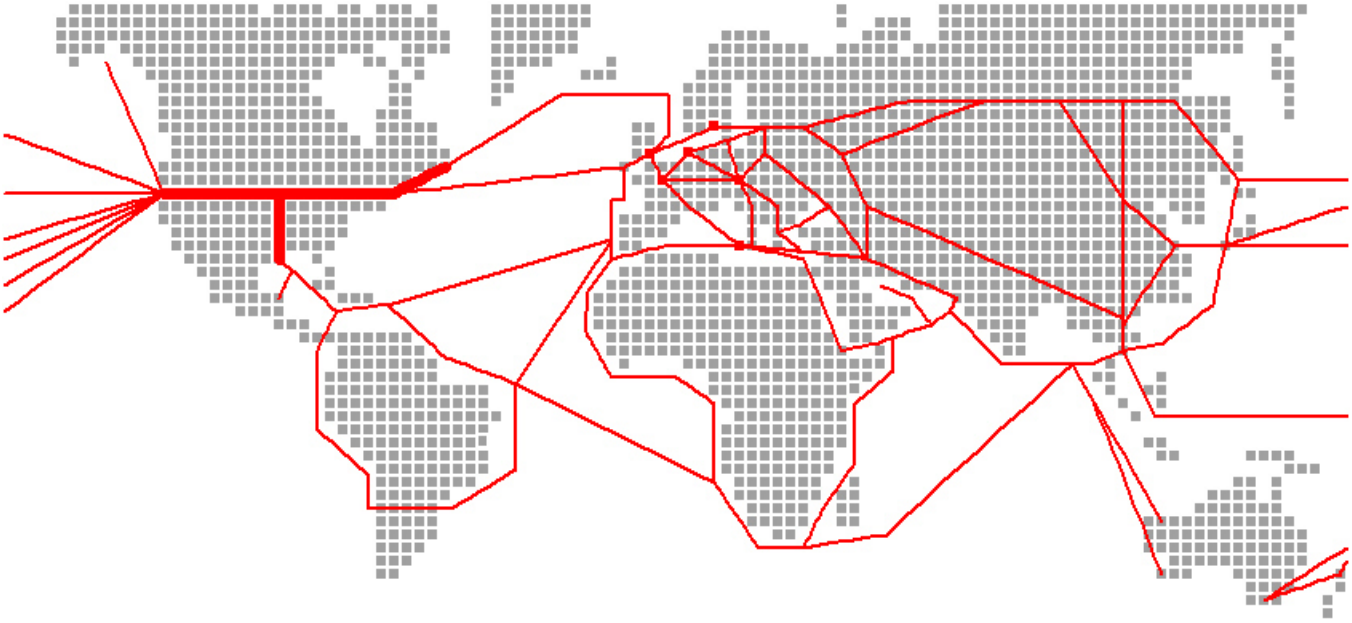
89 Siehe ebenfalls: **CF**, Am Jahrestag wird's weniger, 13.05.2010.

90 **WP**, Deutsches Network Information Center – DENIC eG

91 **CF**, Nummertricks. DNS-Poisoning, 21.11.2008

92 **WP**, Nameserver; **WP**, Root-Nameserver; **CF**, Auflösung von DNS-Adressen, 2007.

93 Das ist der militärische Grundgedanke, der dem Internet zugrunde liegt: Wenn im Krieg einzelne Netzstrecken ausfallen, kann die Kommunikation über andere Verbindungswege fortgesetzt werden.



5. Verkabelte Welt

Internet und Telekommunikation nutzen dieselben Langstreckenverbindungen [94]. Sie bestehen ganz überwiegend aus Glasfaserkabeln. Nur wegen der regionalen Anbindung mobiler Endgeräte oder abgelegener Festnetzanschlüsse kommen auch unterschiedliche Funktechniken zum Einsatz, vor allem Richtfunk [95], aber auch Funknetztechniken (WLAN [96], Wi-Fi [97]) und künftig auch der breitbandige Mobilfunkstandard Long Term Evolution [98]. Die Satellitenkommunikation [99] ist eingebunden, wird aber nur wenig und im wesentlichen in den infrastrukturell unerschlossenen Gebieten im Inneren von Afrika [100], Südamerika und Australien genutzt [101].

Die internationalen Verbindungskabel sind ganz überwiegend Seekabel und folgen den klassischen Seefahrtswegen [102]. Die ältesten, immer wieder erneuerten und ergänzten Trassen führen von den britischen Inseln nach Noramerika (siehe Schaubild oben [103]), eine Haupttrasse direkt durch den Atlantik und eine weitere nördlich Großbritanniens unterhalb Island und Grönland vorbei nach Neufundland. Der europäische Kontinent ist im wesentlichen via Ärmelkanal, über Norwegen und Dänemark sowie entlang der Westküste bis Spanien angebunden.

Die etwa 60 europäischen Knotenpunkte befinden sich vor allem in London, Paris, Amsterdam und inzwischen auch in Frankfurt am Main, wo der deutsche Internetknoten – DE-CIX – betrieben wird [104]. DE-CIX ist weltweit der Knoten mit dem größten Datendurchsatz geworden [105] und hat eine besondere Bedeutung für die Verbindungen nach Osteuropa und den Nahen Osten [106]. Weitere deutsche Internetknoten befinden sich zum Beispiel in Berlin, Hamburg und München [107], womit das Baltikum, Österreich und beson-

94 Siehe auch: **CF**, Physik des Internets, 06.12.2009.

95 **WP**, Richtfunk

96 **WP**, Wireless Local Area Network - WLAN

97 **WP**, Wi-Fi

98 **WP**, Long Term Evolution

99 **WP**, Satellitenkommunikation;
siehe auch: **CF**, Puffer im Weltraum, 11.07.2009.

100 **CF**, Internet für Afrika, 27.12.2009

101 Siehe Schema: **CF**, Internationale Kabel und Netze, 2007.

102 **CF**, internationale Kabel und Netze, 2007

103 Es handelt sich um eine vereinfachte Darstellung, die nicht alle Kabelstrecken berücksichtigt. Ausgenommen wurden zum Beispiel die exklusiven Trassen von IBM (**CF**, Besonderheit: IBM, 2007; Grafik) und die Mehrzahl der kontinentalen Verbindungen in Europa und Nordamerika.

104 **WP**, German Commercial Internet Exchange

105 **WP**, Tabelle internationaler Internet-Knoten;
Monika **Ermert**, Frankfurter Internet-Knoten DE-CIX weltweit auf Platz eins, Heise online 27.04.2010.

106 Frankfurt soll zum größten Internetknoten der Welt werden, tecchannel 18.04.2008

107 **WP**, Tabelle regionaler Internet-Knoten in

ders auch Italien verbunden werden.

Besonders stark ausgebaut sind die Seekabel in Ost-West-Richtung durch das Mittelmeer mit ihrer Hauptverbindung durch den Suezkanal und dem Roten Meer, die weiter um die Arabische Halbinsel bis zum Irak und per Indien in den Fernen Osten führen. Über Hongkong und dann Japan führen wieder diverse Seekabel zur nordamerikanischen Westküste. Markante Knotenpunkte im Mittelmeer befinden sich in Palermo und auf Zypern.

Die Seekabel werden von leistungsstarken Landkabeln ergänzt, die vor allem die USA in alle Richtungen vernetzen, die Metropolen in Westeuropa, über Norwegen und Schweden sowie über Dänemark auch das Baltikum und Russland.

Andere mächtige Kabelstränge verlaufen entlang Italien, wo sie sich in Palermo mit den Mittelmeer-Kabeln verbinden. Weitere innereuropäische Strecken führen über Bukarest und Athen nach Zypern, wo auch sie sich mit den Mittelmeer-Kabeln verbinden, und von dort nach Istanbul und in das Schwarze Meer hinein. Eine weitere wichtige Landstrecke führt vom Baltikum nach Moskau und von dort durch den Norden Russlands bis nach Japan einerseits und nach China andererseits [108].

Australien wird im Norden von Indonesien aus und durch (teure) Direktverbindungen nach Nordamerika erschlossen. Diese führen vor allem zu den Metropolen im Süden des Kontinents [109].

Wenig erschlossen sind Südamerika und Afrika. Diverse Kabel führen durch die Karibik, Südamerika wird aber im wesentlichen durch Seekabel entlang den kontinentalen Küsten erschlossen, wobei der feuerländische Süden durch ein Inlandskabel quer durch den Kontinent abgeschnitten wird.

Dasselbe gilt für Afrika. Auch dieser Kontinent wird durch Seekabel entlang den kontinentalen Küsten erschlossen, wobei die Osttrasse vom Roten Meer kommend bis Südafrika erst 2010 aus Anlass der Fußballweltmeisterschaft realisiert wurde [110].

Diese Beschreibung der Hauptverbindungen zeigt, dass das weltweite Kommunikationsnetz kein diffuses und undurchdringliches Konstrukt ist, sondern dass es abgrenzbare Hauptlinien hat, deren Ausfall durchaus merkbar wird. Als Anfang 2008 zwei Kabel vor Ägypten und später zwei weitere in der Nähe von Dubai ausfielen, waren davon besonders die aus Europa ausgelagerten Callcenter in Ägypten und Indien betroffen [111]. Die indischen Betreiber mussten zusätzliche Netzkapazitäten via Japan und den USA anmieten [112].

Die Einrichtung und der Betrieb von leistungsstarken Kommunikationskabeln ist ein teures Geschäft, das vor allem von rund einem Dutzend international tätiger Unternehmen betrieben wird. Sie werden als Tier 1-Provider bezeichnet [113] und zeichnen sich besonders dadurch aus, dass sie für ihre Dienstleistung – Durchleitung von Daten – von anderen nationalen oder regionalen Providern Gebühren erhalten [114], ohne solche selber an andere bezahlen zu müssen [115]. Dazu wird an den Verbindungsstellen die Datenmenge des ein- und ausgehenden Traffics gemessen [116].

Eine Besonderheit stellt in diesem Zusammenhang wieder die DTAG dar. Sie ist zwar kein internationaler Carrier, betreibt aber ein starkes nationales Verbindungsnetz und dominiert mit ihren Anschlussnetzen. Ohne Zugang zur „Letzten Meile“ kommt kein Verbindungsnetzbetreiber aus. Das macht auch die DTAG zu einem Tier 1 [117].

Deutschland

108 **CF**, eurasische Verbindungen, 06.12.2009

109 Siehe auch: **CF**, schematische Grafik, 05.12.2009; die blauen Linien stellen die „Wurfleinen“ von IBM dar.

110 **CF**, neue Kabel für Ostafrika, 29.03.2008; **CF**, Internet für Afrika, 27.12.2009.

111 **CF**, 4 Seekabel im Nahen Osten gestört, 05.02.2008

112 John **Borland**, Warum das Netz zusammenbrach, Technology Review 08.02.2008

113 **CF**, Tier-1 ... 2 ... 3, 2007; **WP**, Tier-1.

114 **WP**, Peering

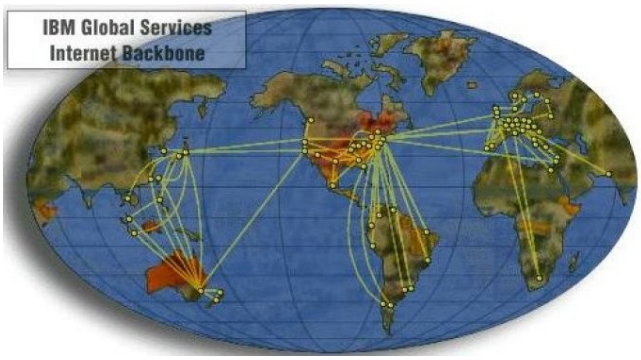
115 Siehe auch: **CF**, Tier-1 ... 2 ... 3, 2007.

116 Einzelheiten bei robtex.com.

117 Holger **Bleich**, Bosse der Fasern. Die Infrastruktur des Internet, c't 7/2005, S. 88;

Sie nutzt deshalb auch nicht den deutschen Internetknoten in Frankfurt, sondern hat mehrere Verbindungen zu den großen Tier 1-Verbindungsnetz-betreibern [118].

Aus Kostengründen streben jedenfalls die großen Tiers danach, die Daten ihrer Kunden möglichst lange in dem eigenen Netz zu transportieren und erst am Zielort einem regionalen Anschlussnetz-betreiber zu übergeben. Diese kaufmännische und technische Strategie wird als „cold potato“ bezeichnet. Carrier mit schwachen oder ohne Verbindungsnetzen sind hingegen daran interessiert, die Daten ihrer Kunden möglichst schnell an einen anderen Verbindungsnetzbetreiber abzugeben (hot potato).



Die cold potato-Strategie wird besonders extrem von IBM betrieben [119]. Dieses Unternehmen hat eigene Direktverbindungen nach Europa und auf dem Landweg zu den Metropolen in Australien, Südafrika und Südamerika verlegt („Wurfleinen“) und übergibt erst dort die Daten an nationale oder regionale Anschlussnetzbetreiber. Damit setzt es sich von den übrigen Tier 1-Cariiern ab, deren Seekabel den oben beschriebenen Haupt- und Seefahrtslinien folgen.

Die Daten bewegen sich keineswegs wahllos und chaotisch durch ein Netz, sondern durchaus gesteuert. Zuständig dafür sind die Netzknoten, an denen sich eine aktive Netzkomponente und in aller Regel ein Router befindet. Dieser kann auswählen, in welche von mehreren Kabelstrecken er die ankommenden Datenpakete schleust [120]. Ausschlaggebend dafür sind kaufmännische Gründe (cold potato), der Ausgleich von Netzlasten und Sicherheitsaspekte.

siehe auch: **CF**, Tier-1 ... 2 ... 3, 2007 (Zitat). Anderer Meinung ist die Wikipedia (**WP**, Klassifikation von Internetprovidern/Autonomen Systemen), die die DTAG nur als besonders aggressiv ansieht.

[118] **CF**, horizontale und vertikale Verbindungen, 2007; **CF**, Schaubild, 2007.

[119] Großansicht

[120] Einzelheiten: **WP**, Routing. Verfahren im Einzelnen.

6. Geroutete Welt

Die Router an den Verbindungsstellen zwischen größeren Netzen führen Routingtabellen, anhand der die Zwischenstation die Weiterleitung von Daten steuert. Darin sind alle oder wenigstens die wichtigsten Autonomen Systeme – AS – eingetragen, die über den Netzverbund erreichbar sind.

Ein autonomes System ist ein beliebig großes Netz [121], das über mindestens zwei Schnittstellen zu anderen Netzen verfügt und deshalb als Verbindungsnetz taugt. Jedes AS hat eine eindeutige, höchstens fünfstellige AS-Nummer. Diese Nummern werden einzeln und blockweise von der IANA [122] an die fünf regionalen Registrierungsstellen [123] vergeben [124], die ihrerseits die einzelnen Nummern an Carrier und andere Unternehmen vergeben und verwalten [125]. In ihren Tabellen sind die Betreiberdaten, die zugehörigen IP-Adressen und AS-Nummern erfasst. Außerdem wird von den Registrierungsstellen vermerkt, mit welchen anderen AS das Autonome System verbunden ist. Beim Transport können die Daten dann von einem AS zum nächsten weitergegeben werden, bis sie zum Zielgerät gelangen.

Das zielgerichtete Steuern der Datenströme beim Routing [126] der Netzbetreiber verhindert chaotische oder von großen Umwegen gekennzeichnete Verbindungswege [127].

Die Dauer, die die Daten vom Sender bis zum Empfänger benötigen, ist von mehreren Faktoren abhängig. Durch Standardisierung fällt kaum noch der „Handshake“ [128] ins Gewicht, also die anfängliche Verständigung der Endgeräte über das Protokoll des Datenaustausches. Hinzu kommen drei Faktoren: Die Transportgeschwindigkeit in den Kabeln, die Belastung und die Verarbeitungsgeschwindigkeit an den Netzknoten.

Funksignale breiten sich mit Lichtgeschwindigkeit aus [129]. Diese Geschwindigkeitsbegrenzung macht sich bei der Satellitenkommunikation [130] durchaus bemerkbar: Die Satelliten befinden sich auf einer geostationären Erdumlaufbahn [131] in rund 36.000 Kilometer Höhe über der Erdoberfläche über dem Äquator. Das von einem Satelliten vermittelte Signal muss immer rund 72.000 km zurücklegen, was einer Laufzeit von knapp 0,3 Sekunden entspricht [132]. Müssen mehrere Satelliten nacheinander angesprochen werden, dann läuft das Signal in aller Regel zu einer Bodenstation und von dort zum entfernteren Satelliten. Das erhöht die Signallaufstrecke auf rund 145.000 km (~ 0,5 sec).

Die Signalgeschwindigkeit in Glasfasern beträgt rund 200.000 km in der Sekunde. Das sind nur zwei Drittel der Lichtgeschwindigkeit. Ein Signal, das die andere Seite der Erdkugel über Kabel erreichen soll, muss aber nur rund 20.000 km Strecke bewältigen, was einer technischen Laufzeit von 0,1 Sekunden entspricht.

An den Knotenpunkten werden die Daten zunächst gepuffert [133] (zwischengespeichert), wegen ihres Zieles analysiert, auf Vollständigkeit geprüft, ihre weitere Route ausgewählt und dann weiter geschickt. Das benötigt, auch wenn es sehr schnell geht, messbare Rechenzeit.

Schließlich kommt die Datenlast hinzu. Ungeachtet der physikalischen Höchstgeschwindigkeit kann jede Verbindungsstrecke nur eine bestimmte Datenmenge je Zeiteinheit übermitteln (Durch-

---

121 **WP**, Autonomes System - AS

122 **WP**, Internet Assigned Numbers Authority - IANA

123 **WP**, Regional Internet Registry - RIR

124 **IANA**, Autonomous System (AS) Numbers (Tabelle mit den registrieren AS-Nummern)

125 Siehe RIPE NCC:
Countries ordered by country code (Verzeichnis der Ländercodes);
Local Internet Registries offering service in Germany (Verzeichnis der AS in Deutschland);
RIPE Database Free Text Search (Freitextsuche)

126 **WP**, Routing-Protokolle

127 Siehe auch: **CF**, horizontale und vertikale Verbindungen, 2007.

128 **WP**, Datenflusskontrolle

129 **WP**, Ausbreitung von Funkwellen

130 **WP**, Satellitenkommunikation

131 **WP**, Geostationäre Umlaufbahn

132 Siehe auch: **CF**, Geostationäre Umlaufbahn, 11.07.2009

133 **WP**, Puffer (Informatik)

satz [134]). Das macht sich vor allem bei großen Dateien bemerkbar, zum Beispiel bei Videosequenzen von YouTube [135] oder großen Programmdateien, die von Peer-to-Peer-Anwendungen verteilt werden [136].

Der Ressourcenhunger [137] populärer Internetdienste hat bei den Carriern verschiedene Reaktionen ausgelöst, einerseits in die Richtung, die Bandbreiten der Kabel und Knoten immer mehr zu vergrößern, und andererseits dahin, über Beschränkungen nachzudenken. Diese können darin bestehen, bestimmte Daten zu privilegieren und andere zu benachteiligen [138]. Eine Alternative dazu besteht in dem Caching [139], bei dem häufig nachgefragte Daten (Videos, Programme, Nachrichtenseiten) zwischengespeichert und mehreren Nachfragern auf kurzem Weg aus dem Zwischenspeicher und nicht um den halben Erdball herum übermittelt werden [140]. Das funktioniert aber nicht beim Filesharing, weil es den Download nur nach Verfügbarkeit und nicht nach Netzlastgesichtspunkten steuert [141].

Das Konzept der Zwischenspeicherung wird bereits beim Internet-Radio [142] und beim Streaming [143] von Fernsehsendungen umgesetzt. Die Datenpakete werden dazu von einem zentralen Sender an einen Webserver in der Nähe der Bedarfsorte verteilt, die ihrerseits zu den Empfängern streamen. Auch bei dieser Technik müssen die Datenpakete zusammengefügt werden, aber nur kontinuierlich und nicht wie beim klassischen Download, wo zunächst alle Datenpakete zusammengefügt werden müssen, bis die ganze Datei für die weitere Verarbeitung zur Verfügung steht.

Ähnliche Techniken werden beim Download großer Dateien angewendet, indem der Browser nach einem Abbruch den weiteren Download an der Stelle wieder aufnimmt, an der der Abbruch erfolgte [144], oder wenn PDF-Dokumente bereits angezeigt werden, währen der weitere Download noch andauert (Linearisierung [145]).

Lastverteilung liegt auch den Peer-to-Peer-Konzepten (P2P [146], Filesharing [147]) zugrunde. Alle angeschlossenen Teilnehmer können gleichzeitig Dateien downloaden und dienen die Teile, die sie der Gemeinschaft anbieten, gleichzeitig zum Upload an. Sie kommen ohne einen zentralen Datenspeicher aus, bedürfen aber im Netz erreichbare Zwischenstellen, die die Teilnehmer darüber unterrichten, von wo sie die gesuchten Dateien laden können und das auch von mehreren Stellen gleichzeitig.

P2P-Netze werden meistens mit illegalen Film-, Musik- und Programmangeboten in Verbindung gebracht und praktisch ist das auch zutreffend. Das ändert aber nichts daran, dass ihr Konzept grundsätzlich für alle Dateien und Inhalte verwendet werden kann. Weltweit operierende Unternehmen nutzen es zur Datenverteilung an ihre Mitarbeiter und vermindern damit die Netzlast und die Belastung ihrer zentralen Hostserver.

Das P2P-Konzept wird auch in den wenig infrastrukturell erschlossenen Gebieten in Zentralafrika erprobt, um damit Bandbreite zu sparen und populäre Inhalte zu verteilen [148]. Das ist zwar kein Ersatz für den Ausbau der Infrastruktur, wohl aber ein guter Behelf für die Übergangszeit.

---

134 **CF**, Netzneutralität und Breitbandtechnik. Infokasten, 08.12.2007

135 **CF**, Das Lifestyle-Internet fordert die Bandbreite, 08.12.2007

136 **CF**, kollabiert das Internet? Die P2P-Netze beanspruchen mehr als zwei Drittel der Internet-Kapazität, 13.09.2008

137 Über die Netzlast durch DoS-Angriffe: **CF**, heftige Angriffe, 20.09.2007.

138 **CF**, Forderung nach Übertragungsgebühren, 18.12.2007;
Torsten **Kleinz**, Netzneutralität - ein amerikanisches Problem? c't 05.12.2007.

139 **CF**, verteilter Zwischenspeicher, 04.09.2008

140 Siehe: Mason **Inman**, Hast Du mal ein bisschen Bandbreite? Technology Review 02.09.2008

141 **CF**, Optimierung von P2P-Netzen, 08.09.2008

142 **WP**, Internetradio. Distribution und Reichweite

143 **WP**, Streaming-Server

144 **WP**, Download-Manager

145 **WP**, Portable Document Format. Verwendung und Eigenschaften

146 **WP**, Peer-to-Peer

147 **WP**, Filesharing

148 **CF**, Internet für Afrika, 27.12.2009

7. Verschlüsselte Welt

Kommunikationsnetze in ihrer heutigen Form gründen auf Vertrauen. Die transportierten Inhalte können prinzipiell überall im Netz abgefangen, kopiert, gelesen und manipuliert werden. Dagegen schützt die Verschlüsselung [149].

Die einfache Verschlüsselung betrifft die Inhalte in einer Datei, nicht aber ihre Kopfdaten (Header), in den der Urheber (Sender), der Empfänger und die wesentlichen Stationen beim Datentransfer gespeichert sind. Grundsätzlich muss zwischen der symmetrischen und der asymmetrischen Verschlüsselung unterschieden werden. Bei der symmetrischen verwenden Sender und Empfänger denselben Schlüssel, um die Nachricht zu ver- und schließlich zu entschlüsseln [150].

Die asmmetrische Verschlüsselung verwendet einen öffentlichen Schlüssel (public key [151]) zur Verschlüsselung, den der Empfänger beliebig verteilt. Die Nachricht lässt sich dann aber nur mittels eines privaten Schlüssels entschlüsseln (private key [152]), den der Empfänger unter Verschluss hält. Dieses Verfahren hat den besonderen Charme, dass die Partner unverzüglich verschlüsselt korrespondieren können, ohne sich zunächst über die Art und Weise der Verschlüsselung verständigen zu müssen.

Eine Verschlüsselung, die auch die Identität der Partner verschleiert, bedarf einer besonderen technischen Infrastruktur. Dabei werden am Netzknoten die Dateien komplett, also mit ihren eigenen Headern verschlüsselt und als solche in eine neue Transportdatei eingefügt. Die Transportdatei lässt nach außen nur erkennen, von welchem Router sie versandt wurde und an welchen Router sie gerichtet ist. Dieses Verfahren nennt man „tunneln“ [153]. Es ist nur in einem insoweit geschlossenen Netz möglich, in dem sich alle Stationen des Routings und das damit verbundene Protokoll kennen (zum Beispiel MPLS [154]).

Zur Anbindung häuslicher und mobiler PCs in Firmen- und sonstigen gesicherten Netzen dient das Virtual Private Network – VPN [155], wobei die Arbeitsplatzgeräte (Client) über einen besonderen Server (VPN-Gateway) mit den internen Netzdiensten korrespondieren. Die internen Zugangs- und Nutzdaten werden auf der Verbindungsstrecke zwischen Client und Gateway verschlüsselt und erst am Gateway wieder entschlüsselt. Auf diesem Prinzip beruht auch die SSL-Verschlüsselung [156], die vor allem beim E-Commerce und beim Homebanking [157] zum Einsatz kommt.

Alle Verschlüsselungen für den Datenverkehr in öffentlichen Netzen, wie das Internet, haben zwei prinzipielle Schwachstellen: Beim Verarbeitungsvorgang im Endgerät vor der Verschlüsselung [158] und an den Netzwerkknoten, die bei der Kommunikation durchlaufen werden. Hier ist es immerhin möglich, die Datenpakete abzufangen, zu kopieren und erst dann weiter zu leiten oder dass sich ein Man-in-the-Middle [159] direkt in die Kommunikation zwischenschaltet.

Overlay-Netze [160] für Unternehmen und die öffentliche Verwaltung nutzen deshalb ausschließlich durch ihre nummerische IP-Adresse und sonstigen Eigenschaften genau definierte Endgeräte. Wenn darüber hinaus eine asymmetrische Verschlüsselung genutzt wird, dann ist das Risiko, dass ein Angreifer mit abgefangenen Daten tatsächlich etwas anfangen kann, äußerst gering.

---

149 **CF**, Verschlüsselung. Tunnelung, 30.03.2008; siehe auch: **CF**, Geschichte der Geheimdienste und der Verschlüsselungstechnik, 24.11.2007; **CF**, unlesbare Texte, 08.10.2008.

150 **WP**, Verschlüsselungsmethoden

151 **WP**, Öffentlicher Schlüssel

152 **WP**, Geheimer Schlüssel

153 Siehe auch: **CF**, Tunneln mit Small Sister, 30.12.2008

154 **WP**, Multiprotocol Label Switching - MPLS

155 **WP**, Virtual Private Network - VPN

156 **CF**, Angriff auf gesicherte Verbindungen, 21.11.2009; **CF**, Kollisionsangriff gegen Webseiten-zertifikat, 15.02.2009.

157 **CF**, Sicherheit von Homebanking-Portalen, 22.03.2008

158 **CF**, Online-Angriff an der Quelle, 08.11.2008

159 **CF**, Botnetze. The Man in the Middle, Sommer 2007; Dieter **Kochheim**, Cybercrime, 2010

160 **CF**, Overlay-Netze der öffentlichen Verwaltung, 30.03.2008

8. Manipulierte Welt

Das Prinzip des Vertrauens und die mächtige Stellung der Autonomen Systeme – AS – ermöglichen es, Identitäten zu verschleiern, Netzinhalte zu zensieren und fremde IP-Adressen – jedenfalls vorübergehend – vom Internet auszuschließen.

Überwachung, Spionage und Zensur im großen Stil sind immer dann möglich, wenn die dazu geeignete Technik an den Netzknoten eingesetzt wird, die ein geschlossenes, zum Beispiel nationales Subnetz mit internationalen Verbindungsnetzen verbinden [161]. So ist auch von den deutschen Verfassungsschutzbehörden darüber nachgedacht worden, Überwachungsmaßnahmen am deutschen Internetknoten durchzuführen [162]. Eine vollständige Überwachung müsste jedoch auch die 15 kleineren Internetknoten in Deutschland [163] und die Direktverbindungen der DTAG mit 5 internationalen Tier 1-Carriern [164] umfassen, so dass die Umsetzung allein schon an der Vielzahl der Verbindungsstellen scheitern würde. Andererseits sind groß angelegte Überwachungsprojekte seitens der USA geplant [165] und wie Echelon [166] lange Zeit betrieben worden. Jüngst ist auch aus Frankreich ein ähnliches Projekt bekannt geworden [167].

Ungeachtet der technischen Schwierigkeiten und dem Massenproblem bei einer Überwachung des Internets bleibt das Problem der Verschlüsselung. Bei einer Datenstromüberwachung können zwar Adressen mit bestimmten Ziel- und Empfängerangaben gefiltert und als Zensurmaßnahme gelöscht, verschlüsselte Daten dabei aber nicht ohne weiteres lesbar gemacht werden.

Besonders China ist in den letzten Jahren wegen breit angelegter Zensur- [168] und Überwachungsmaßnamen in die Kritik geraten. Dabei geht es um die Überwachung der internationalen Datenströme [169], um angebliche Hintertüren [170] im E-Mail-Dienst Gmail [171], um zensierte Suchergebnisse bei Google.cn [172], die gezielte Verfolgung von Regimegegnern mit Malware [173] und vor allem um Industriespionage [174]. Auch der jüngste Verfassungsschutzbericht spart nicht mit Kritik und berichtet über einen internationaler Angriff vom „GhostNet“, dessen Betreiber sich in China befinden sollen [175].

Dabei ist nicht jede Datenstromüberwachung unerwünscht und nachteilig. Die großen Provider filtern bereits seit Jahren offensichtliche Spam-Mails [176] und entlasten damit die internationalen Verbindungsnetze. Firmen- und Verwaltungsnetzwerke werden von Firewalls gegen unberechtigte Zugriffe und von Virenscannern gegen Malware geschützt. Jedenfalls der Malwareschutz läuft leer, wenn die eingeschleuste Malware verschlüsselt ist und deshalb nicht erkannt werden kann. Das ist der Grund dafür, dass eine Ende-zu-Ende-Verschlüsselung nicht in jedem Fall segensreich ist [177].

---

161 **CF**, omnipotente Überwachung, 29.03.2010

162 **CF**, Verfassungsschutz will Internet-Knoten abhören, 13.04.2008

163 **WP**, Tabelle regionaler Internet-Knoten in Deutschland

164 **CF**, horizontale und vertikale Verbindungen, 2007; **CF**, Grafik, 2007.

165 **CF**, Big Lauscher, 15.10.2007

166 **CF**, Onlinedurchsuchung. Omnipotente Technologien, 2007; **CF**, Diabolus geplant, 17.01.2008.

167 **CF**, Frenchelon, 12.07.2009

168 **CF**, Bilder gegen die Zensur, 04.09.2007

169 Great Firewall; siehe statt vieler: Julia **Fröhlich**, Internetzensur. Die virtuelle chinesische Mauer, focus online 01.08.2008.

170 **CF**, Backdoors in Standardsoftware, 2007

171 **CF**, Domänen, Google und China, 27.02.2010

172 Ebenda. Siehe auch: **CF**, Browser von dem Datenkraken, 04.09.2008.

173 **CF**, Social Engineering. Gezielte Manipulationen, 01.03.2009

174 **CF**, gefälschte Sicherheitsprodukte, 07.02.2010; **CF**, not amused, 23.10.2007.

175 **BMI**, Verfassungsschutzbericht 2009, 21.06.2010, S. 308.

176 Siehe: **CF**, Spam-Monitor von funkwerk, 21.06.2008;
WP, Spamfilter;
CF, Müllabwehr. Rechtliche Grauzone beim Filtern von Spam-Mails, 05.01.2008.

177 Der Virenschutz an der Firewall und auf dem Mailserver scheidet dabei aus und muss sich auf den Client beschränken.

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

BSI [178]

Die AS verwalten die nummerischen IP-Adressen, DNS-Adressen und Hostspeicher für ihre Kunden selber und unkontrolliert. Das machen sich die Schurkenprovider zu Nutze [179], umdie Standorte von Servern [180] und die Identität ihrer Kunden zu verschleiern (Whois Protection [181]) und um ihnen geschützte Umgebungen für illegale Inhalte (Drop Zone [182]) und Hackerboards zu schaffen [183].

Die AS melden den Zonenverwaltungen (RIR [184]) und damit auch den Routingtabellen für die Verbindungsnetze, welche anderen AS über sie zu erreichen sind. So können sie vorübergehend die an fremde IP-Adressen gerichteten Daten zu sich umleiten und damit die Adressen unerreichbar machen [185]. Dem liegt das Border Gateway Protocol – BGP [186] - zugrunde, nach dem die AS unkontrolliert die Netze und IP melden, die über sie erreichbar sind. Sein böswilliger Einsatz kann Man-in-the-Middle-Angriffe [187] und Domain-Übernahmen möglich machen, wenn der Angreifer große Anstrengungen unternimmt.

[178] **BSI,** Definition Kritische Infrastrukturen

[179] **CF**, Schurkenprovider, 11.04.2010;
CF, Schurken-Provider und organisierte Cybercrime, 13.07.2008.

[180] **CF**, anonyme Server, 11.04.2010

[181] **CF**, Whois Protection, 11.04.2010

[182] **CF**, heimlicher Betrieb, 11.04.2010;
CF, Drop Zones. Carder, 13.07.2008;
CF, Online-Warenhäuser, 22.11.2008;
CF, Gegenspionage wider 'ZeuS' und 'Nethell', 19.12.2008.

[183] **CF**, neue Hacker-Boards schotten sich ab, 23.05.2010

[184] **WP**, Regional Internet Registry - RIR

[185] **CF**, IP-Adressen ohne Beweiswert, 16.05.2010

[186] **WP**, Border Gateway Protocol - BGP

[187] **CF**, böswillige BGP-Manipulationen, 10.07.2010

Nicht mehr einzelne PCs, sondern zunehmend Router, Firewalls und andere Sicherheitseinrichtungen, die in Unternehmen oder Verwaltungen Systeme schützen sollen, geraten ins Visier der organisierten Kriminalität.

BSI [188]

Die internationalen Kommunikationsnetze bauen auf Redundanz und gewährleisten damit ein hohes Maß an Ausfallsicherheit [189]. Sie lassen sich nicht einfach abschalten, aber durch gezielte Angriffe empfindlich stören. Das gilt besonders für die zentralen Verwaltungstechniken und die Netzknoten, an denen das Routing stattfindet.

Wenn die Signalverwaltung für ein intelligentes Netz mit seiner Datenbank ausfällt, dann können deren Aufgaben von einer redundanten Einrichtung übernommen werden. Dadurch erhöht sich jedoch die Verarbeitungslast des Ausfallsystems. Beim Ausfall mehrerer Komponenten bricht im schlimmsten Fall das Signalisierungsnetz zusammen. Das Kommunikationsnetz fällt dann insgesamt aus.

Der deutsche Internetknoten DE-CIX ist auf mehrere räumlich getrennte Standorte in Frankfurt am Main verteilt. Im Katastrophenfall blieben bei seinem Ausfall eine Vielzahl von internationalen Verbindungsnetzen für die Internetkommunikation unerreichbar.

Der Ausfall mehrerer Seekabel kann zu empfindlichen Einschränkungen führen [190], auch wenn sich die Kommunikation über Ersatzstrecken (oder Satelliten) abwickeln lässt.

Überlastungen, Störungen und einzelne Ausfälle lassen keinen Totalausfall der Kommunikationsnetze erwarten, wohl aber Teilausfälle, vorübergehende Störungen und Performanceeinbußen. Sie können die Verlässlichkeit Kritischer Infra-

[188] **BSI**, Nationaler Plan zum Schutz der Informationsinfrastrukturen (NPSI), BSI 18.08.2005; S. 5.

[189] Siehe: Stefan **Dierichs**, Wie verlässlich ist das Internet? if(is) 15.03.2006; weitere Veröffentlichungen des Instituts für Internet-Sicherheit

[190] **CF**, 4 Seekabel im Nahen Osten gestört, 05.02.2008; **CF**, TAT-14 beschädigt? 24.03.2008.

strukturen (Krankenhäuser, Stromversorgung, Polizei) erheblich beeinträchtigen, weil sie meistens nicht über eigene Netze verfügen, sondern durchweg auf angemieteten Netzen von privatwirtschaftlichen Carriern betrieben werden. Das macht abhängig und birgt das prinzipielle Risiko eines Ausfalls infolge Schlamperei, mangelnder Kontrolle und kaufmännischem Unvermögen.

Dem widersetzt sich die Bundeswehr, indem sie eine "Vernetzte Operationsführung" - NetOpFü [191] - eingerichtet hat, die aus autonomen, sich selbst synchronisierender Einheiten besteht [192], die selbst bei unterbrochenen Kommunikationsverbindungen handlungsfähig bleiben sollen.

Die zunehmende Abhängigkeit von Kommunikationsnetzen in fast allen anderen Bereichen der Öffentlichkeit macht eine genaue und ständige Risikobewertung und die Schaffung von Ausfallsicherungen erforderlich [193]. Dem widmet sich zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik – BSI – mit ihrem Arbeitsschwerpunkt „Kritische Infrastrukturen“ [194]. Dessen ungeachtet scheint ein breites Problembewusstsein in Staat und Wirtschaft zu fehlen. Das könnte sich bei üblichen Störfällen oder böswilligen Angriffen rächen (DoS [195], Cyberwar [196]).

Die größte Bedrohung stellen derzeit internetbasierte Angriffe auf Computersystemeund mobile Kommunikation deutscher Wirtschaftsunternehmenund Behörden dar … Zugleich scheint sich die internationale Finanz- und Wirtschaftskrise negativ auf die Sicherheitsstrukturen deutscher Unternehmen auszuwirken. Viele Unternehmen sehen sich gezwungen, Kosten einzusparen; Personalabbau im zweistelligen Prozentbereich ist keine Seltenheit. So kürzen sie Mittel für Sensibilisierungsmaßnahmen sowie zur Prävention und Abwehr von Wirtschaftsspionage. Insbesondere bei Schulungsmaßnahmen und sicherheitsrelevanten Investitionen, z.B. für IT und Informationssicherheit, wird gespart. Unternehmen ignorieren oder unterschätzen nachrichtendienstliche Aktivitäten und betrachten das eigene Know-how als nicht gefährdet. Umfassende Sicherheitskonzepte unter Einbeziehung der IT und des menschlichen Faktors werden vernachlässigt. Die Folgen können für Wirtschaftsunternehmen äußerst kontraproduktiv sein.

BMI [197]

[191] Ulrike **Heitmüller**, Die Bundeswehr auf der Suche nach der besten Vernetzung, c't 02.01.2009

[192] Detlef **Borchers**, Mit Datennetzen zur Bundeswehr aus autonomen selbstorganisierenden Einheiten, Heise online 15.05.2006

[193] Dabei kann es sich zum Beispiel um Richtfunkstrecken handeln, die hinreichend leistungsfähig und erschwinglich sind und die eine verschlüsselte Übermittlung zulassen.

[194] **BSI**, Schutz Kritischer Infrastrukturen. Moderne Gesellschaften sind auf eine zuverlässige Infrastruktur angewiesen

[195] **CF**, verteilter Angriff, Sommer 2007

[196] **CF**, Schatten des Krieges. Digitale Bürgerkrieger, Cyberwar und Kritische Infrastrukturen, 11.01.2009; **CF**, gefälschte Sicherheitsprodukte. Anmerkungen, 07.02.2010.

[197] **BMI**, Verfassungsschutzbericht 2009, 21.06.2010, S. 309.

Im April und Mai 2007 gab es einen großen DDoS-Angriff, der auf viele Regierungswebsites in Estland gerichtet war. Ermittler gehen davon aus, dass der Angriff durch die Umsetzung des „bronzenen Soldaten“ veranlasst wurde, einem Denkmal für einen unbekannten russischen Soldaten im Zweiten Weltkrieg. Estnische Behörden hatten beschlossen, das Monument vom Zentrum Tallins auf einen vorstädtischen Militärfriedhof zu versetzen. Dieser Beschluss löste unter der Bevölkerung Tallins Unruhen aus, bei denen eine Person getötet wurde. Später, kurz vor dem Jahrestag des Sieges (zur Beendigung des 2. Weltkriegs, der in Estland am 9. Mai gefeiert wird), begann ein mehrere Tage andauernder DDoS-Angriff. Viele große estnische Websites standen während dieser Zeit nicht zur Verfügung. Unter Sicherheitsexperten herrscht die Meinung vor, dass dieser Angriff von einer Gruppe von Einzelpersonen durchgeführt und von deren patriotischen Gefühlen angeheizt wurde. ... Es konnten keine Hinweise auf eine Beteiligung der russischen Regierung an diesen Angriffen gefunden werden, und selbst wenn es eine Verbindung gäbe, würde diese mit sehr großer Wahrscheinlichkeit nicht entdeckt werden. Nach dem Vorfall beschuldigten sich beide Seiten gegenseitig der Cyber-Angriffe.

Muttik [198]

... nach einem Pressebericht des israelischen Online-Magazins ynetnews.com ist eine islamistische Hackergruppe namens "Team Evil" von Marokko aus in das System des israelischen Registrars DomainTheNet eingedrungen und hat diverse Domains "entführt" und den Besucherstrom auf antiisraelische Webseiten umgeleitet.

domain-recht [199]

9. Cyberwar

Bekannt gewordene Cyberwar-Angriffe gehen bis auf den Kosovo-Krieg zurück [200] und besonders diskutiert wurden die Angriffe gegen estnische Regierungsseiten aus dem April und Mai 2007, wobei auch das Finanzsystem vorübergehend ausfiel. Dort, in Estlands Hauptstadt Tallinn, errichtet die NATO ein Zentrum zur Abwehr von Cyberangriffen mit (lächerlichen) 30 Mitarbeitern [201]. In den von McAfee veröffentlichten Länderberichten [202] hat sich auch Igor Muttik [203] mit dem DDoS-Angriff auf estnische Webseiten (und zwei russischen Städten [204]) auseinander gesetzt. tecchannel bezeichnet den Vorfall als eine *schlecht koordinierte Netz-Prügelei* [205].

McAfee sieht jedoch eine zunehmende Tendenz zu destruktiven kriminellen, politischen und militärischen Auseinandersetzungen im Internet. Den Anfang machte McAfee's Zweite große europäische Studie über das Organisierte Verbrechen und das Internet [206]. Sie lieferte die erste Typenbeschreibung für die Internetkriminalität und stellt nach meinem Eindruck den ersten Versuch dar, die Cybercrime im Zusammenhang mit den handelnden Personen zu bewerten [207]. Im Dezember 2008 folgte der Bericht zum Thema Virtuelle Kriminalität [208]. Er verweist auf die Zunahme staatlicher Auseinandersetzungen im Internet (Cyber-

198 Igor **Muttik**, Die Wirtschaft und nicht die Mafia treibt Malware voran, McAfee 12.02.2008

199 **Domain-Recht**, TLDs - Neues von .il, .nl und .london, Newsletter 446 vom 15.01.2009

200 Florian **Rötzer**, FBI und amerikanisches Militär im Cyberwar-Rausch, Telepolis 08.10.1999

201 **CF**, NATO-Zentrum zur Internet-Kriegsführung, 17.05.2008.

202 **McAfee**, Ein Internet, viele Welten, 12.02.2008; siehe auch: **CF**, McAfee. Analysen zu globalen Sicherheitsbedrohungen, 11.04.2010.

203 Siehe Kasten links oben.

204 **CF**, Ende der Anonymität im Internet, 18.12.2007; "Anonyme Nutzer im Netz wird es bald nicht mehr geben", channelpartner.de (ursprünglich: tecchannel 07.12.2007)

205 NATO plant Zentrum zur Internet-Kriegsführung, tecchannel 15.05.2008

206 **McAfee**, Zweite große europäische Studie über das Organisierte Verbrechen und das Internet, Dezember 2006

207 Siehe auch: **CF**, der Basar, 11.04.2010

208 Bericht von McAfee zum Thema Virtuelle Kriminalität, McAfee 08.12.2008

Im Mai 2008 gesellten sich Belgien und Indien zur wachsenden Anzahl der Länder, die Opfer von offenbar aus China stammenden Angriffen wurden. Vermutlich aufgrund der Tatsache, dass sich in Brüssel (Belgien) die Hauptsitze von EU und NATO befinden, gingen in Belgien E-Mails mit Spyware an das Außenministerium ein. Auch Indien berichtet, dass seine staatlichen und nichtstaatlichen Netzwerke ständig von Computerangriffen betroffen sind.

McAfee [209]

Im August 2008 wurde gegen die Infrastruktur von Georgien ein koordinierter Computerangriff gestartet, der die Webseiten der georgischen Regierung einschließlich des Außenministeriums kompromittierte. Die georgische Regierung gab an, dass die Unterbrechung durch Angriffe verursacht wurde, die von Russland im Zusammenhang mit dem Konflikt zwischen den beiden Staaten um die Provinz Südossetien durchgeführt wurden.

McAfee [215]

war) und fordert eine koordinierte, grenzüberschreitende Strafverfolgung [210]. Den vorläufigen Schluss bildet Paul B. Kurtz [211], ebenfalls von McAfee:

Die Grenze zwischen Internetkriminalität und Internetkrieg verschwimmt heute immer mehr, weil manche Staaten kriminelle Organisationen als nützliche Verbündete betrachten. Einige Nationen zeigten bereits, dass sie bereit sind, Angriffe auf gegnerische Ziele durch kriminelle Organisationen und Privatpersonen zu tolerieren, zu fördern oder sogar gezielt einzusetzen. [212]

Auch der Bundesverfassungsschutz spricht insoweit von einer deutlichen Zunahme der "elektronischen Angriffe" zum Zweck der Spionage und vor allem der Industriespionage [213]. *Besonders gefährlich sind elektronische Angriffe auf Netzwerke und Computersysteme deutscher Wirtschaftsunternehmen und öffentlicher Stellen* [214].

9.1 allgemeine Definition

Betrachten wir den Cyberwar als eine gezielte, zerstörerische Auseinandersetzung mit den Mitteln und gegen die gegnerischen Infrastrukturen der Netzkommunikation, so umfasst der Begriff nicht nur militärische Akteure, sondern auch politische Aktivisten, Unternehmen und die organisierte Cybercrime.

Cyberwar in diesem Sinne ist der strategische Einsatz der Informations- und Kommunikationstechnik mit dem Ziel, Gegner und Opfer existenziell zu schädigen, also nicht nur ihre Datenverarbeitung und Netzkommunikation zu stören oder auszuschalten, sondern ihre Funktionstüchtigkeit insgesamt.

Dabei unterscheide ich wegen der Akteure zwischen kriminellem und staatlichen Cyberwar und wegen der Interventionstiefe zwischen Kaltem und Heißem Cyberwar. Die Akteure sind austauschbar, so dass sich die Unterscheidung zwischen Kriminalität und Staat weniger auf die Personen, als auf die verfolgten Zwecke bezieht.

Beiden Formen geht es in der „kalten Phase“ darum, geheime Informationen zu gewinnen, fremde Infrastrukturen zu infiltrieren und auszukunden, ohne dabei offen in Erscheinung zu treten.

Die kriminellen Varianten davon sind schon jetzt die Malware und die Botnetze. Die von ihnen infiltrierten Server, Router und Endgeräte verhalten sich wie die Schläfer im Kalten Krieg. Sie sind möglichst unauffällig und warten auf das Signal

---

209 Bericht von McAfee zum Thema Virtuelle Kriminalität, McAfee 08.12.2008

210 **CF**, virtuelle Kriminalität 2008, 13.12.2008

211 **CF**, Analysen zum Cyberwar, 11.01.2010

212 Paul B. **Kurtz**, Bericht zum Thema Virtuelle Kriminalität 2009. Virtueller Internetkrieg wird zur Wirklichkeit, McAfee 06.11.2009

213 **CF**, Verfassungs- und Wirtschaftsschutz, 25.05.2009; **BMI**, Verfassungsschutzbericht 2008, Vorabfassung 19.05.2009, S. 285

214 **BMI**, Bundesinnenminister Dr. Thomas de Maizière stellt Verfassungsschutzbericht 2009 vor, 21.06.2010

215 Bericht von McAfee zum Thema Virtuelle Kriminalität, McAfee 08.12.2008

Der Krieg im Gaza-Streifen wird auch im Internet geführt. So verbreitet die israelische Armee ihre Propaganda unter YouTube und israelfreundliche Hacker verunstalten Webseiten mit Hamas-Propaganda [216]. Nicht ohne Gegenwehr. Die iranische Hackergruppe Ashiyane Digital Security Team zog kurzfristig eine Webseite des israelischen Geheimdienstes Mossad [217] aus dem Verkehr und hackte andere, vor allem israelische Webseiten [218].

"Help Israel Win" ist eine Initiative israelischer Studenten, die sich gegen Hamas-freundliche Webseiten im Internet richtet [219]. Sie wirbt um Unterstützer, die von ihrer Webseite ein Programm herunterladen können, mit dem feindliche Seiten blockiert werden sollen.

Was dieses Programm macht, ist nicht ganz klar und wahrscheinlich weniger patriotisch als die Geschichte drum herum. Nach ersten Analysen könnte es sich um eine Botsoftware handeln, die die Computer der Unterstützer zu Zombies macht. Danach verbindet das Programm PatriotInstaller.exe den Computer, auf dem es installiert ist, mit einem Internet Relay Chat-Server und anderen Websites. Überdies ermöglicht es das Herunterladen einer weiteren Datei, die als TmpUpdateFile.exe installiert wird.

Die Initiatoren bestätigen, dass das Programm als Trojaner benutzt werden könne ... Nach Angaben auf der Webseite haben bereits über 8200 Internetnutzer das Programm installiert; die Entwickler betonen, es ließe sich wieder ohne Probleme entfernen. Die Update-Option verwende man nur, um Fehler zu beheben, aber nicht um Schadprogramme zu installieren ... Nach dem Krieg werde man das Projekt beenden. Jeder könne dann das Programm wieder entfernen.

Die geäußerte Vermutung, es handele sich um Botsoftware, liegt nahe. Mit ihr lassen sich DDoS-Angriffe durchführen und diese sind ein brutales und probates Mittel gegen "feindliche" Angebote im Internet.

Es gibt nur wenige andere Methoden, um "Gegner" auszuschalten und alle benötigen hackerhandwerliches Geschick. Neben dem Hacking in den Webserver, auf dem die Seite betrieben wird, käme besonders das Poisoning in Betracht, wobei DNS-Server verbogen werden müssten, damit die Seite nicht mehr erreichbar ist und ihre Besucher auf andere (nachgemachte) Seiten umgeleitet werden.

Cyberfahnder [221]

zum Aktivwerden [220].

9.2 Kalter Cyberwar

Die vorgestellten Stellungnahmen gehen davon aus, dass sich die Formen des staatlichen und des kriminellen Cyberwar kaum unterscheiden, was nicht zuletzt darauf zurückführen sein dürfte, dass sich die staatlichen Akteure bevorzugt krimineller Organisationen und ihrer Fachleute bedienen.

Dies vorausgesetzt ist es angezeigt, die Grundlage der Methoden des Cyberwar in den kriminellen Methoden zu suchen, die von der Cybercrime bekannt. Das dürfte in der Kalten Phase ein Gemisch aus dem Hacking, dem Ausspähen und Abfangen von Daten, dem Social Engineering (Aushorchen und Überreden von Personen, Auswertung öffentlicher Quellen und schließlich Ausspähen geheimer Informationen) und der Einsatz technischer Mittel sein. Darunter verstehe ich Abhörtechnik (Keylogger, Datenweichen, getarnte

[216] Gaza-Konflikt: Der Krieg im Internet, Heise online 09.01.2008

[217] Alfred **Hackensberger**, Mythos Mossad, Telepolis 30.11.2008

[218] Gaza-Konflikt …, ebenda.

[219] Israel im Cyberwar mit einem Trojaner helfen? Heise online 09.01.2009

[220] Das Vorbild dafür sind die modernen Botnetze, die die infiltrierten Zombies nur wenig belasten, damit sie dem Botnetz möglichst lange erhalten bleiben. Siehe: Dieter **Kochheim**, Cybercrime, 2010, S. 83.

[221] **CF**, Schatten des Krieges. digitale Bürgerkrieger, Cyberwar und Kritische Infrastrukturen, 11.01.2009

Eingabegeräte), kompromittierte Router an Netzknoten und die Art Software, zu der sich die Malware für Botnetze allmählich entwickelt: Zu autonomen Agenten, die auf Schlüsselereignisse warten und bei deren Eintritt damit beginnen, zu protokollieren oder anderweitig aktiv zu werden.

Ihr Konzept stammt aus den Sechziger Jahren und wurde als „Daemon“ [222] unter Unix [223] realisiert. Es sind im Arbeitsspeicher schlummernde Hintergrundroutinen, die auf bestimmte Anforderung warten und dann zum Beispiel einen Drucker (oder einen anderen Dienst) rufen und zur Verfügung stellen. Ihre kriminelle Variante wird seit ein paar Jahren als Phishing-Malware eingesetzt [224]: Die Malware wartet darauf, dass der Anwender PayPal oder ein anderes Portal zum Onlinebanking oder -einkauf aufruft und klinkt sich dann in den weiteren Prozess ein.

Seit einigen Jahren wird damit experimentiert, solche Agenten gezielt zur Informationsbeschaffung in offenen Netzen einzusetzen [225]. Ihr Einsatzort sind die Netzknoten (Router, Firewalls) und Hostspeicher, die sie nach brauchbaren Informationen durchforsten. So funktionieren bereits im Ansatz die Crawler [226], also die Suchbots, die von den Betreibern von Suchmaschinen zur Durchforstung von Host-Speichern eingesetzt werden.

Zur kalten Phase gehören auch gezielte Provokationen und DoS-Angriffe, um zum Beispiel intelligente Netzkomponenten zu infiltrieren (Buffer Overflow [227]). Schafft es der Angreifer, Arbeits- oder Zwischenspeicher zu überfluten, dann hat er die Chance, Programmcode zu injizieren, der unkontrollierte Prozesse einschleusen kann. Diese Methode wird heute vom Prinzip her von den infiltrierten Webseiten verfolgt, die Schadcode in die Browser der Besucher einschleusen [228].

Diese und andere Provokationen können den Zweck haben, zu erproben, ob der Gegner auf sie vorbereitet ist, wie er reagiert und vor allem wie schnell. Schon 2006 haben sich zwei konkurrierende Unternehmen mit Spamabwehr und DoS-Angriffen bekämpft, wobei das israelische Sicherheitsunternehmen auf der Strecke blieb [229]. Auch in der Hackerszene sind Hacking und DoS-Angriffe zwischen konkurrierenden Gruppen Gang und Gäbe [230]. Die größten politischen Dimensionen hatten bislang der DoS-Angriff auf Estland und die Malware-Angriffe gegen Regimekritiker in China während der Olympischen Spiele 2008, auf die eingangs eingegangen wurde.

Bei einem DoS-Angriff kommt es darauf an, dass zu einem festgelegten Zeitpunkt ein Zielsystem von sehr vielen Anfragen gleichzeitig bombardiert wird. Das kann durch eine Vielzahl von Gleichgesinnten und viel einfacher durch kompromittierte Rechner geschehen, denen durch Hacking oder durch Malware eine Schadroutine eingesetzt wurde. Einfacher ist es jedoch, dazu Botnetze zu verwenden, die zu jedem kriminellen und zerstörerischen Zweck einfach und schnell umkonfiguriert werden können.

Deshalb ist es gut denkbar, dass es den Kontrahenten im Kalten Cyberwar ganz besonders darauf ankommt, möglichst mächtige Botnetze für den Ernstfall zu rekrutieren. Dazu müssen die Kriegsparteien entweder selber Botnetze aufbauen oder die heutigen Betreiber schon jetzt einkaufen. Dazu eignet es sich am besten, ihnen Schutz zu bieten und sie schon jetzt unbehelligt zu lassen. Wenn man sie dann braucht, sind sie noch den einen oder anderen Gefallen schuldig oder sehen sich plötzlich der Strafverfolgung ausgesetzt, weil sie nicht so parieren wie sie sollen.

---

[222] **WP**, Daemon

[223] **WP**, Unix

[224] Dieter **Kochheim**, Cybercrime, 2010, S. 105.

[225] Gordon **Bolduan**, Von Agenten gesucht, Technology Review 25.08.06

[226] **WP**, Webcrawler

[227] **WP**, Pufferüberlauf

[228] Besonders instruktiv sind die beiden Beiträge, die die c't jetzt in der neuen Reihe „Tatort Internet“ veröffentlicht hat:
Thorsten Holz, Alarm beim Pizzadienst, c't 13/2010, S. 184 (Drive-by-Download von einer infizierten Webseite);
Frank Boldewin, Zeig mir das Bild vom Tod, c't 14/2010, S. 186 (infizierte Doc-Datei).

[229] Alfred **Krüger**, Den Teufel mit dem Beelzebub austreiben, Telepolis 21.05.2006

[230] **CF**, neue Hacker-Boards schotten sich ab, 23.05.2010

Die Macht dazu haben staatliche Einrichtungen und mafiöse Strukturen.

Organisierte „Krieger“ könnten auch Strategien verfolgen, die bei der Netzinfrastrukur selber ansetzen, so dass Netzknoten physisch angegriffen oder so sabotiert werden, dass bestimmte Kabelverbindungen verhindert oder umgeleitet werden.

In der „heißen Phase“ können alle diese Maßnahmen dazu führen, einen Zeitvorteil für andere destruktive Aktionen zu erlangen. Ergänzt werden sie wahrscheinlich von nachrichtendienstlichen und konspirativen Methoden, die von extremistischen Gruppen bekannt sind.

9.3 Heißer Cyberwar

Erst in der Heißen Phase des Cyberwar dürften neben den bekannten Methoden der Cybercrime ganz verstärkt terroristische und militärische Einsätze zu erwarten sein.

„Heiße Krieger“ könnten zum Beispiel versuchen, Router an Netzknoten so zu manipulieren, dass sie kein zielgerichtetes Routing betreiben, sondern wie Hubs wahllos die eingehenden Daten in alle angeschlossenen Netze gleichzeitig verteilen. Schaffen sie es, mehrere Router zu kompromittieren, dann kann es zu einem Echo-Effekt kommen, bei dem sich die Router – wie bei einem DoS-Angriff – gegenseitig abschießen.

Militärische Cyberwar-Strategien dürften sich eher gegen die technische Infrastruktur richten und das Ziel haben, die gegnerische Logistik und Wirtschaft zu stören oder auszuschalten [231]. Schon jetzt wird kräftig aufgerüstet mit Robotern, selbständigen Systemen, vernetzten Soldaten [232] und Weltraumwaffen [233]. Das sind aber Nebenaspekte.

Strategische Überlegungen dürften anders aussehen: Ein Nadelöhr der internationalen Telekommunikation erstreckt sich über den Suezkanal entlang dem gesamten Roten Meer. Ein unauffälliges Schiff, das den üblichen Schifffahrtsrouten folgt, könnte mit einfachen Wasserbomben empfindliche Kabelschäden hervorrufen, ein zweites, das vor Hongkong kreuzt, Indien fast ganz vom Netz abkoppeln und ein drittes in der baltischen Bucht Russlands Hauptverbindungen zum internationalen Netz ganz empfindlich stören.

Wie sensibel Netzkomponenten und -dienste auf technische Ausfälle und ungewöhnliche Ereignisse reagieren, zeigen verschiedene harmlose Beispiele aus der Vergangenheit. Die Auslobung eines VW Golf, der zuvor dem zum Papst gewählten Kardinal Ratzinger gehört hatte, führte zu einem riesigen Öffentlichkeitsinteresse und schließlich zum Ausfall von eBay [234]. Ein Fehler im DeNIC-Rechenzentrum ließ unlängst weite Teile der deutschen .de-Domänen für Stunden ausfallen [235]. Schon 2001 fiel tagelang ein Rechenzentrum des Webhosters Strato aus technischen Gründen aus [236] und 2003 erfolgte ein DoS-Angriff gegen das Unternehmen, der ebenfalls zum Ausfall führte [237].

Beispiele für verheerende Kaskadeneffekte in vernetzten Systemen zeigen mehrere Ausfälle der Stromversorgung. Im August 2003 führten Softwarefehler in acht Staaten im Nordosten der USA und in Teilen Kanadas zuM Stromausfall [238], die *planmäßigen Abschaltung der Höchstspannungsleitung über die Ems zur Durchfahrt des Kreuzfahrtschiffes Norwegian Pearl* [239] führte zu Ausfällen und Kapazitätsengpässen in Deutschland und seinen westlichen Nachbarländern und 2005 brachen 50 Strommasten unter Eislasten zusammen, so dass im Münsterland tagelang der

---

231 Carolin **Welzel**, Vom Kalten Krieg zum Cyberwar, politik-digital.de

232 Wehrwirtschaft: bessere IT für "kleine Kriege", Heise online 08.01.2009

233 Wolfgang **Pomrehn**, China: Satelliten-Knacker geehrt, Telepolis 11.01.2009

234 **CF**, verteilter Angriff, Sommer 2007

235 Fehlerhafte Nameserverdaten-Aktualisierung legte Domain .de lahm, Heise online 15.05.2010

236 Strato-Domains nach wie vor offline, Heise online 29.03.2001

237 Ausfall wegen DDoS-Attacke beim Webhoster Strato, Heise online 19.07.2003

238 Software-Fehler verursachte US-Stromausfall 2003, Heise online 13.02.2004

239 E.ON führt Stromausfall auf "menschliche Fehleinschätzungen" zurück, Heise online 15.11.2006

Strom ausfiel [240].

9.4 Risikobewertung und Ausfallsicherung

Die Bewertung solcher hypothetischen Gefahren muss erfolgen, um die Risiken zu bewerten und geeignete Gegenmaßnahmen zu entwickeln.

Das sind vor allem Strategien zur Ausfallsicherheit durch Redundanz, wobei die Ausfallsysteme so eingerichtet werden müssen, dass sie räumlich weit getrennt und im Katastrophenfall nicht beide in Mitleidenschaft gezogen werden. So macht es wenig Sinn, zwei Verbindungsstrecken eines lokalen Netzes zu anderen Verbindungsnetzen kilometerlang durch denselben Kabelkanal zu führen. Ein unbedarfter Baggereinsatz kann beide Verbindungen kappen.

Hinzu kommen alle Maßnahmen zur klassischen Zugangssicherung. Das betrifft auch den Standort wichtiger Kommunikationstechnik. Wer weiß, wo die damals noch staatliche Post ihre Ämter betrieb, hat gute Chancen, die örtlichen Schaltstellen der DTAG zu entdecken. Die Konzentration des deutschen Internetknotens an einem Ort ist unter Sicherheitsgesichtsgesichtspunkten eine Katastrophe. Das gilt ebenso für das blinde Vertrauen auf die Zuverlässigkeit privater Carrier als Grundlage für den Netzbetrieb bei kritischen Infrastrukturen.

Neben physikalischen und technischen Ausfallsicherungen bedarf es politischer Strategien zur Bekämpfung desintegrer informationstechnischer Systeme. Wegen dieses Begriffes lehne ich mich an das Urteil des Bundesverfassungsgerichts zu den Voraussetzungen und Grenzen der Onlinedurchsuchung an [241]. Staatliches Handeln hat es durch die Schaffung eines ergänzenden Grundrechts auf das Vertrauen auf die Integrität informationstechnischer Systeme beschränkt[242], ohne darauf anzusprechen, dass genau diese kriminelle Praxis von Malware und Botnetzen im großen Stil betrieben wird.

9.5 Bekämpfung von Cybercrime und Cyberwar

Ganz wesentliche Werkzeuge in einem Cyberwar werden einsatzspezifische Malware und funktionstüchtige Botnetze sein, um kommerzielle, politische oder „echte“ Kriegsgegner und ihre lebenswichtigen Infrastrukturen anzugreifen. Daraus ist meines Erachtens zu schließen, dass der erste Schritt zur Bekämpfung des Cyberwar in der Bekämpfung der Cybercrime besteht. Deshalb bedarf es – nicht nur national – neuer Maßnahmen gegen destruktive Programme (Malware), gegen ihre Urheber, ihren Verbreitern und schließlich ihren Nutzern. Sie müssen mehrere Stoßrichtungen haben: Verbot und Strafbarkeit von Malware, Schaffung von Einrichtungen und Instrumenten zu ihrer präventiven und repressiven Verfolgung und eine internationale Zusammenarbeit, die einerseits keine „sicheren Häfen“ wegen der Strafbarkeit zulässt und andererseits die gemeinsame aktive Bekämpfung optimiert.

Ebenso bedarf es der internationalen Ächtung destruktiver Malware, von Schurkenprovidern, die anonymisierte Hostdienste zur Verfügung stellen, und von Botnetzen sowie einer Charta werden, in der die Staaten auf die Nutzung dieser Dienste verzichten.

Diese politischen Forderungen sind neu und unpopulär. Sie gehen weit über das hinaus, was mit der Cybercrime Convention [243] und dem ständigen Rummachen am Urheberrecht mühsam auf den Weg gebracht wurde. Das Cybercrime-Abkommen wird die internationale Zusammenarbeit bei der Strafverfolgung erleichtern und zum Beispiel das Freeze-Verfahren einführen [244]. Darüber hinaus müssen die Strafverfolgung und die

---

[240] Warum die Masten knickten, faz.net 29.11.2005

[241] **CF**, Vertraulichkeit und Integrität informationstechnischer Systeme, 01.03.2008;
CF, Bundesverfassungsgericht: Onlinedurchsuchung, 05.04.2008.

[242] **CF**, Gestalt und Grenzen des neuen Grundrechts, 05.04.2008

[243] **Europarat**, Übereinkommen über Computerkriminalität

[244] Vorläufige Sicherung „laufender“ Verkehrs- und Inhaltsdaten im Ausland mit anschließendem Rechtshilfeersuchen. Das Verfahren eignet sich nicht rückblickenden Aufklärung von Straftaten.

Cybercrime-Prävention wahrscheinlich in einem Programm [245] zusammengeführt werden, auch wenn damit die Grenzen zwischen repressiver Strafverfolgung und polizeilicher Prävention verwischt. Ein solches Vorgehen ist aus der Verfolgung der Organisierten Kriminalität erprobt und hat sich als erfolgreich erwiesen.

Das Projekt muss die Cybercrime analysieren, Methoden zu ihrem Erkennen und ihrer Bekämpfung entwickeln. Diese strategische Aufgabe wird bereits jetzt vom Bundeskriminalamt und der Landeskriminalämtern wahrgenommen, die ihre Schwerpunkte jedoch allein aus polizeilicher Sicht und ohne Einbindung der Strafverfolgung setzen. Getrennt davon müssen die repressive Strafverfolgung und die präventive Vorbeugung, die trotz ihrer Selbständigkeit und einer notwendigen, auch personellen Trennung koordiniert und eng zusammen arbeiten können. Die personelle Trennung ist nicht nur deshalb nötig, um die Gewaltenteilung zu erfüllen, sondern auch, um klare Verhältnisse im Hinblick auf die Verwertbarkeit von Informationen und ihrer Offenbarung zu schaffen. Dazu wird auch § 96 StPO neu bewertet und gefasst werden müssen.

Mit der erfolgreichen Bekämpfung der Cybercrime verbinde ich die Chance, terroristische und staatliche Cyberwar-Aktivitäten zu erschweren, weil die Akteure nicht mehr einfach auf die erprobten kriminellen Strukturen und Techniken zugreifen können.

Den Cyberwar kann man damit nicht endgültig verhindern.

---

[245] Programm im Sinne des Projektmanagements ist eine beständige Organisation mit einem bestimmten, aber allgemein gehaltenen Ziel. Die Umsetzung erfolgt durch Projekte. Diese sind auf jeweils eine konkrete Aufgabe ausgerichtet, deren Erreichen zeitlich befristet ist.