Erste Auflage 2009

gegenstalt.com

AxelRoch.de

Gestaltung und Satz: Mehi Park, mehi.kr
Umschlag: Mehi Park, Axel Roch
Lektorat: DerLektor.net
Druck: Albdruck, Berlin
Bindung: Stein + Lehmann, Berlin
Printed in Germany

ISBN: 978-3-9813156-0-8

Claude E. Shannon: Spielzeug, Leben und die geheime Geschichte seiner Theorie der Information

Axel Roch

gegenstalt Verlag

Inhalt

13 ● Kapitel Eins
Spielzeug

1.1 Throbac I — 16
1.2 7x8 Hoax — 17
1.3 Schaltungsspiel — 18
1.4 Caissac — 19
1.5 Gedankenlesende Maschine — 21
1.6 Theseus — 22
1.7 Nimwit — 23
1.8 3-Relay Kit — 23
1.9 Two by Two by Two Cube Cubes — 25
1.10 Wortspiele und Literatursynthese — 26
1.11 Ultimate Machine — 28

31 ● Kapitel Zwei
Mathematische Mobilmachung

2.1 Schaltalgebra — 31
2.2 Telefonzähler und Relaisrechner — 33
2.3 Mathematische Theorie der Genetik — 35
2.4 Skizze der Kommunikation — 37
2.5 Angriff oder Verteidigung — 39

43 ● Kapitel Drei
Kampf um den Kanal

3.1 Straightforward Attack — 48
3.1.1 Eingabe: ‘I’ — 50
3.1.2 Verarbeitung: ‘/’ — 52
3.1.3 …und Ausgabe als Kommunikation: ‘I/O’ — 54
3.2 Flug und Rauschen — 56
3.2.1 Irreguläre Bewegungen — 57
3.2.2 Autokorrelation — 59
3.2.3 Wiener/Bigelow-Prädiktor — 60
3.2.4 Statistik gegen Geometrie — 61
3.3 Antizipation der Antizipation — 65
3.3.1 Filterung der Gelben Gefahr — 67
3.3.2 Entscheidungsprobleme — 70
3.3.3 Flugzeuge als Signalquellen — 72
3.3.4 Zwischen Kontinuität und Diskontinuität — 76
3.4 Trajektorien als Nachrichten — 80

83 • Kapitel Vier
Sichere Signale

4.1 Projekt X — 85
4.1.1 Vo(co)der — 85
4.1.2 Sigsaly — 86
4.1.3 Kontinuierliche Unsicherheiten — 89
4.1.4 Signal Security Agency — 90
4.1.5 Alan Turing in New Jersey — 92
4.2 Schlüsseltechnologien — 97
4.2.1 Analoge Vernam-Chiffre — 98
4.2.2 Philosophie des Signals: PCM — 101
4.3 Mathematische Theorie… — 104
4.3.1 …der Kryptografie xor Kommunikation — 104
4.3.2 Neue Medien: Röhren und Radar — 106
4.3.3 SIGSEC — 110
4.3.4 Kryptografie und Physik: H — 113
4.3.5 …elektronischer Bewegung — 116
4.3.6 κ, χ, ψ, ϕ und φ — 118
4.4 Secret, nicht Top Secret — 120

125 • Kapitel Fünf
Security of Control

5.1 Fernforschung — 126
5.2 Ultimate Missile — 128
5.2.1 AAGM – Studie — 132
5.2.2 Nike – Major Electronic Job — 139
5.2.3 Secrecy of Control — 141
5.2.4 Magic Black Box — 143
5.2.5 Grundlagen und Grenzen: H, N, C und ε — 144
5.3 Dual, nicht Digital — 153
5.4 Post-War Post — 156
5.5 Steuerschleifen — 158

163 • Kapitel Sechs
Mathematical Theory of Little Juggling Clowns

6.1 Newton, Schnewton — 166
6.2 What hath God wrought? — 168
6.3 No-Drop/Club-Passing Diorama — 170
6.4 12-Clown Zoetrope — 172
6.5 W. C. Fields Memorial — 173
6.6 Superballs on Marble — 175
6.7 Massachusetts Institute of Jugglology — 178
6.8 Gedanken Juggling — 180
6.9 Clowns, Codes und Chiffren — 182
6.10 Shannons letzte Message — 190

Vorwort

Die vorliegende Monografie ist eine Geschichte der Informationstheorie Claude Elwood Shannons. Die dafür umfangreiche Auswertung bislang unbekannter Primärquellen wäre ohne der Geduld und der Unterstützung vieler Institutionen und Personen nicht möglich gewesen. Etwas mehr als acht Monate intensiver Forschung in verschiedenen Archiven waren nötig, um die Entstehung der Informationstheorie zwischen 1940 und 1949 vergleichend und schrittweise rekonstruieren zu können. Mehr als die Hälfte dieser Zeit war ein vergebliches Suchen in Findmitteln, Karteikarten, Datenbanken und Akten ohne weiterführende Hinweise. Heute – im Rückblick – kann ich verstehen, warum die Geschichte der Informationstheorie bislang noch nicht geschrieben werden konnte: Die Heterogenität der Akten an den unterschiedlichsten Orten, die an den relevanten Stellen geradezu fragmentarische Systematik der Findmittel und die vergangenen Sicherheitsinteressen der Vereinigten Staaten von Amerika während des Kalten Krieges hatten es Historikern bislang noch nicht ermöglicht, die interessante, aber auch geheime Geschichte der Informationstheorie Claude Shannons einer interessierten Öffentlichkeit vorzustellen.

Ich kann mich noch gut an jenen Moment erinnern, als nach drei intensiven Wochen der Suche in New Jersey dann doch auf einmal ein Konvolut in Erscheinung trat. Schon beim Öffnen, noch bevor die ersten Seiten lesbar waren, wurde mir klar, hier tatsächlich historisches Neuland zu betreten: Der seltsame und eigenartige Geruch der Akten, in denen der Name Claude Shannon wiederholt und mehrfach auftaucht, ließ unwillkürlich darauf schließen, dass dieses Konvolut seit seiner Archivierung vor etwa 50 Jahren zum ersten Mal wieder eingesehen wurde. Offensichtlich ein echter Glücksfalls, denn in der Produktionshektik heutiger Medien- und Wissenschaftsgeschichte muss nach ein oder zwei Wochen frustrierter Suche in der Regel die Suche ergebnislos abgebrochen werden. Ich hatte aber irgendwie die Geduld, auch nach drei Wochen in jeder Hinsicht ergebnislosen Suchens an der gleichen Stelle doch nicht das Handtuch zu werfen. Die eigentliche archäologische Studie hatte damit allerdings erst begonnen. Ein erstes Ergebnis liegt nun mit dieser Monografie vor.

Dem eiligen Leser, der so schnell wie möglich und ohne Heranführung die Geschichte der Informationstheorie kennen lernen möchte, empfehle ich das fünfte Kapitel. Dem

Leser, der sich zudem für die Person oder das Leben Claude Shannons interessiert, sei weiter das einführende und das abschließende Kapitel anempfohlen. Letzteres führt auch in Shannons ironisch-kritisches Denken der 80er Jahre ein. Das zweite, dritte und vierte Kapitel gibt Auskunft zur unmittelbaren Vorgeschichte der informations-, kommunikations- und kryptotheoretischen Schriften bis 1945. Diese Kapitel sind für diejenigen Leser hilfreich, die Shannons Theorien als Fragestellungen und Ergebnisse der Forschung und Entwicklung seit dem Zweiten Weltkrieg lesen möchten. Nicht alle Fragen sind in den verschiedenen Kapiteln beantwortet worden. Shannon arbeitete 1951, 1957 und auch noch später für verschiedene Geheimdienste. Es ist zwar bekannt, bis zu welchem Grad und welche Themenkomplexe Shannon beispielsweise für die CIA und die NSA bearbeitet hatte, da sich aber bisher noch nicht mindestens zwei oder mehrere Quellen vergleichend auswerten ließen, bot sich eine vertiefte Darstellung in einer Monografie auch noch nicht an. Aus meiner Sicht sind die Schriften Claude Shannons bis 1949 dagegen nun ausreichend historisch bewertbar.

Das erste und das letzte Kapitel der vorliegenden Monografie sind verschriftlichte Auszüge aus zwei Vorträgen, die ich im Juli 2007 und im Mai 2009 gehalten habe. Den ersten auf Einladung durch Prof. Dr. Hartwig Steusloff am Fraunhofer-Institut für Informations- und Datenverarbeitung IITB in Karlsruhe im Rahmen der CHIL-Konferenz – Computers in the Human Interaction Loop. Den zweiten Vortrag habe ich für Prof. Dr. Manfred Faßler zum 60. Geburtstag im Rahmen des Symposiums zur Anthropologie des Medialen an der Goethe-Universität Frankfurt gehalten. Die Kapitel zwei, drei, vier und fünf sind leicht erweiterte Auszüge einer Dissertation, die an der Ludwig-Maximilians-Universität München, Fakultät für Mathematik, Informatik und Statistik, angenommen worden ist. Titel der Dissertation: Eine Geschichte der Informationstheorie Claude Elwood Shannons (1938-1949), Datum der mündlichen Prüfung: 13. Oktober 2009. Prof. Dr. Menso Folkerts und Prof. Dr. Martin Wirsing gilt dafür mein ausdrücklicher Dank. Für inhaltliche Kommentare und hilfreiche Kritik danke ich diesbezüglich Prof. Dr. Dr. h.c. mult. Friedrich L. Bauer und ganz besonders Dr. Rudolf Seising.

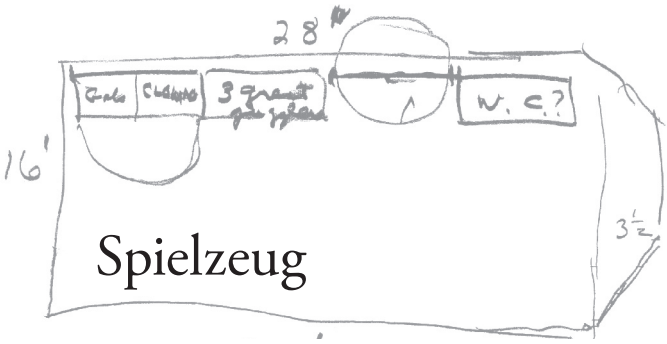
Die Forschungsaufenthalte vor Ort, zunächst als Visiting Scholar, dann als Research Assistant und später als Research Scholar, sind durch die Johns Hopkins University und das Massachusetts Institute of Technology ermöglicht worden. Die unverhältnismäßige Geduld der Mitarbeiter in den verschiedenen Archiven gab meiner historischen Forschung das konkrete Material, hier sind mit einer Danksagung wenigstens Marjorie Ciarlante für NARA, Sheldon Hochheiser für AT&T sowie Joseph Brooks für die Library of Congress zu nennen. Für lange und kurze, immer aber wichtige Gespräche, die

mich zu weiteren Primärquellen führten, danke ich insbesondere Betty Shannon, Prof. Dr. Peter Elias, Prof. Dr. Jacob Ziv, Prof. Dr. Erhard Schüttpelz, Dr. Friedrich-Wilhelm Hagemeyer, Dr. Jim Reeds und Dr. David Kahn. Ohne das Heinrich-Klotz-Stipendium, gestiftet von der Gesellschaft zur Förderung der Kunst und Medientechnologie e.V. und verliehen durch den Vorstand des ZKM | Zentrum für Kunst und Medientechnologie in Karlsruhe, Prof. Dr. h.c. Peter Weibel, wäre es mir nicht möglich gewesen, die Forschungsergebnisse als Dissertation einzureichen und in einer Monografie darzustellen. Den toleranten und herzlichen Kollegen an der Rijksuniversiteit Groningen, insbesondere Prof. Dr. Liesbeth Korthals Altes und Dr. Barend van Heusden, danke ich für die Integration meiner medienhistorischen Forschungen in den akademischen Betrieb. Mein ausdrücklicher Dank gilt weiter dem Heinz Nixdorf MuseumsForum in Paderborn. Norbert Ryska und Dr. Jochen Viehoff haben das Projekt durch viele Kenntnisse erweitert und in der Produktion unterstützt. Ab dem 6. November 2009 widmet das HNF Claude Shannon eine Sonderausstellung: Codes und Clowns – Claude Shannon – Jongleur der Wissenschaft. Bei der Korrektur des Manuskripts haben mir Regina Passier und Birte Schonhaus geholfen. Die Bilder sind reproduziert mit freundlicher Genehmigung von Betty Shannon, Douglas Ramsey, dem MIT und dem HNF/Jan Braun. Gestaltet ist das Buch von Mehi Park. Die Zitate auf der Buchrückseite hatte sich Claude Shannon für öffentliche Vorträge notiert und zusammengestellt. Er rückte damit seine Informationstheorie in einen viel allgemeineren und weiteren historisch-theoretischen Zusammenhang, als es diesem Buch jemals hätte gelingen können.

Axel Roch
Groningen, im Oktober 2009

Id facit exiguum clinamen principiorum
Nec regione loci certa nec tempore certo
Lukrez

Heraklit ist der erdenklich radikalste Pazifist:
Er war gegen die Dinge überhaupt,
weil sie aus dem Blödsinn des Krieges hervorkommen,
und das hat Hegel (man würde sagen absichtlich) verschwiegen.
Aber es ist gut, sich daran zu erinnern.
Flusser



Spielzeug

Ein Besuch im Hause Claude Elwood Shannons am Mystic Lake in Winchester, Massachusetts, hinterließ bei jedem, der dazu die glückliche Gelegenheit hatte, einen unheimlichen Eindruck. Nicht nur weil das Haus seiner Familie einmal der Ur-Ur-Enkelin eines Präsidenten der Vereinigten Staaten, Thomas Jefferson, gehört haben soll. Auch nicht, weil Shannon während des Zweiten Weltkriegs an einer geheimen und sicheren Telefonverbindung zwischen Franklin D. Roosevelt und Winston Churchill, Washington und London, mitgearbeitet haben soll. Der unheimliche Eindruck entstand vielmehr angesichts einer entropischen und anti-entropischen Vielfalt an Maschinen, Apparaten, Automaten und Artefakten, die Claude Shannon gesammelt oder gebaut hatte. Er verbrachte einen erheblichen Teil seines Lebens mit nutzlosen Spielereien. “I am always building totally useless gadgets, some of which you can see around here, just because I think they’re fun to make.”

In seiner Garage in Winchester sammelte Claude Shannon exotische Räder. Er interessierte sich für Steuerung und Balance auf Einrädern. Einräder mit verschiedenen Durchmessern und Radbreiten, sehr dünnen oder flachen Reifen; Einräder mit Sitzen in einer Höhe bis zu drei Metern; Mini-Einräder mit etwa 10cm Durchmesser und ohne Sitz, deren Pedale direkt an der Radachse befestigt sind; Einräder mit Sitzen innerhalb des

Rads; kuriose Dreiräder; Hochräder; motorisierte, mit Benzin betriebene Springstöcke; exotische Tandem-Fahrräder für 2, 3, 4 oder *n* Personen; vertikale Tandems, deren Sitze parallel zur Fahrtrichtung angebracht sind; etc. Shannon kehrte das Prinzip des Fahrrads um: Nicht eine Person mit zwei Rädern, sondern ein Einrad für zwei Personen, ein Tandem-Einrad. Wie lassen sich solche Einräder für 2, 3, 4 oder *n* Personen konstruieren? Shannon selbst baute sich ein Off-Center Unicycle. Das ist ein Einrad, dessen Radachse nicht im Mittelpunkt des Rades liegt. Der Fahrer wippt dadurch automatisch auf und ab. Wie viele Bälle können Zirkuskünstler auf solchen Einrädern jonglieren? "I have always been interested in the circus arts – juggling, unicycling and the like."

Das allererste Einrad baute Shannon 1951. Ein klassisches Einrad mit Bananensitz und etwas mehr als einem Meter Durchmesser. Shannon balancierte damit, gleichzeitig drei Bälle jonglierend, in den 50er Jahren durch die Gänge seines Arbeitgebers in New Jersey, den Bell Telephone Laboratories. Die Sensation für Mathematiker und Ingenieure war perfekt. Ralph Hartley benutzte 1928 in seiner Theorie der Information noch die Metapher des Fahrrads, um den Unterschied zwischen analoger und diskreter Signalübertragung zu veranschaulichen. Shannon, nachdem er seine Theorie der Information 1948 publiziert hatte, fuhr Einrad und jonglierte dabei mit mehreren Bällen. Shannon inszenierte damit seine Variante der Informationstheorie: Kodierung und Fundamentaltheorem. Das Einrad ist Shannons Metapher für Kodierung, das Jonglieren veranschaulicht die Anstrengung, möglichst viele Nachrichten gleichzeitig in einem Kommunikationskanal zu übertragen…

Shannons Einrad

Selbstverständlich konnten alle seine drei Kinder, die Söhne Andy und Rob und seine Tochter Peggy, sowohl jonglieren als auch Einrad fahren. Auf dem allerersten Einrad-Treffen in Amerika, der Unicycle Invitational 1971 in New York City, gewannen zwei seiner Kinder, Andy und Peggy, 12- und 17-jährig, den ersten und zweiten Preis in der Kategorie Trickradfahren. Sie balancierten auf ihren Einrädern mit nur einem Fuß.

Mathematische Mobilmachung

Motley's the only wear.
Shakespeare

Lange bevor Claude Elwood Shannon seine Theorie der Information entwickelte und damit auf fundamentale Weise Grundlagen und Grenzen technischer Kommunikation neu definieren konnte, schenkte ihm seine Ausbildungsumgebung höchste Aufmerksamkeit. Er war, so die Beobachtung seiner Zeitgenossen, ein echtes mathematisches Genie. Der Präsident des Massachusetts Institute of Technology schrieb 1939 über den 23-jährigen, gerade graduierten Studenten: "I appreciate what you say about Mr. Claud[e] E. Shannon who certainly shows signs of being a mathematical genius. Dean [Vannevar] Bush had spoken to me several times about him."[1] Shannon fiel durch eine Doppelbegabung auf. Er hatte 1936 an der University of Michigan einen BSc in Mathematik und einen BSc in Elektrotechnik erhalten. Das zeigte sich 1938 nochmals bei seinem Master of Science, "A Symbolic Analysis of Relay and Switching Circuits", in dem er Mathematik und Elektrotechnik, Software und Hardware verbinden konnte.

2.1 Schaltalgebra

Ein Aushang an der University of Michigan soll Claude Shannon 1936 auf einen Job am MIT aufmerksam gemacht haben. Vannevar Bush, Dekan des Department of Electrical

Kampf um den Kanal

Even the most intense strata are
riddled with lines of flight.
Deleuze / Guattari

Lange vor dem Angriff japanischer Flugzeuge auf Pearl Harbor im Dezember 1941 hatte sich Amerika politisch, militärisch und zivil auf den bevorstehenden Krieg eingestellt. Vannevar Bush formulierte als eine der größten Sorgen der nationalen Sicherheit die technischen Möglichkeiten angreifender Flugzeuge. Er antizipierte Probleme in der Flugabwehr. Die Verteidigung musste wissenschaftlich modernisiert und an eine neue technische Bedrohung angepasst werden: "Anti-aircraft is not receiving the attention it should have."[1] Hochfrequenzradio, also Radar, konnte ein Flugzeug entdecken, aber noch lange nicht abschießen. Es fehlte "[a] precise and rapid *control* of guns"[2]. Die Amerikaner lasen am 16. Dezember 1941 in der New York Times, dass Radar und Leitsysteme längst kombinierbar waren: "[The German Anti-Aircraft Defense has solved] the problem of hooking up the radio locators, used to detect the enemy planes, with the ground guns."[3] Die Deutschen hatten ab 1940 das Radarsystem Würzburg in Serie produziert, welches nicht nur Flugzeuge detektieren, sondern auch Flugabwehrfeuer koordinieren konnte.

Die Erforschung der Methoden zur Steuerung der Flugabwehrgeschütze in Amerika bedurfte zunächst selbst einer organisierten Steuerung mittels nationaler Institutionen.

Sichere Signale

The heart of modern army communications
is the vacuum tube.
Llewellyn, Bell Labs, 1944

1943 erhielt Claude Shannon eine neue Aufgabe im Bell System. Er sollte nicht mehr nur Flugzeuge mittels Filtertheorie und Mathematik abschießbar machen, sondern Nachrichten mit mathematischen Methoden verschlüsseln, Daten und Signale also nicht nur verarbeiten, sondern auch sicher machen. Bis zu welchem Grad konnte ein Feind nicht nur Flugzeuge, sondern auch Nachrichten abfangen? Wie ließen sich mehr oder weniger verschlüsselte Nachrichten in den Kanälen der Kommunikation mehr oder weniger sicher übertragen? Welche mathematischen Grundlagen eigneten sich für theoretische als auch praktische Kommunikationssicherheit? Shannon bekam eine völlig neue Aufgabe: den Schutz der Nachrichten vor feindlicher Interzeption, d.i. theoretische Kryptografie.

In den Bell Labs entstanden im Verlauf des Zweiten Weltkriegs neue Techniken der Kommunikation und mit diesen die Problematisierung der theoretischen Sicherheit. Shannon beschäftigte sich deshalb während zweier Phasen, 1943 und 1945, mit Kryptologie. Im Mai 1943 legte er eine interne Studie vor, Titel: "Analogue of the Vernam System for Continuous Time Series". 1945 folgte eine weitere intensive Studie, Titel: "A Mathematical Theory of Cryptography". Der erste Bericht ist eine kleine, die Entwick-

Security of Control

No nation was ever more
remote-control conscious than the United States.
Spencer, NDRC, 1945

Seit Juni 1940 hatte das NDRC die Aufgabe, zivile Wissenschaften und Streitkräfte auf taktischer Ebene zu verbinden. Nach dem Angriff auf Pearl Harbor empfahl James Conant, Mitbegründer des NDRC, die Einrichtung einer weiteren Kommission. 1942 gründete sich daraufhin mit der zusätzlichen Empfehlung des Kriegsministers Henry Stimson das Joint Committee on New Weapons and Equipment (JNW). Den Vorsitz übernahm Vannevar Bush.[1] Ausschließlicher Gegenstand waren nicht Probleme oder die Antizipation derselben an der taktischen Front, sondern neue Waffentechnologien und deren Wechselwirkung mit strategischer Kriegführung. Zivile Wissenschaften hatten somit nach englischem Vorbild auch einen Kanal zu den Streitkräften auf strategischer Ebene.[2]

Das JNW war im Wesentlichen administrativ, da es über keinerlei Budget verfügte. Vannevar Bush hielt zudem die Kommission für nicht sehr effektiv, doch brachte sie unterschiedliche Leute an einen Tisch, "especially in subcommittees when such subjects as guided missiles were considered."[3] Das JNW richtete für neue Waffen, beispielsweise Radar oder Raketen, Kommissionen ein, die die Aufgabe hatten, die Methoden dieser Waffen zu evaluieren. Lenkwaffen spielten dabei eine besondere Rolle. Als 1944

Mathematical Theory of Little Juggling Clowns

What is the Matrix?
Control…
Morpheus

"The next time you see a juggler watch his hands – they carry a message." Nicht nur elektromagnetische Wellen oder Impulse in elektronischen Schaltkreisen, nicht nur die technischen Medien der Ingenieure, sondern auch die taktilen Hände der Jongleure kommunizieren Nachrichten. Es fällt junggeselligen Wissenschaftlern und Ingenieuren lediglich schwer, solche Nachrichten auch zu dekodieren, so jedenfalls Shannon: "The next time you see a juggler watch his hands – they carry a message. With all the action elsewhere, this may be as difficult to do as a similar suggestion to young sailors seeing their first hula dance." Wie können Medien und Computer nicht nur Daten übertragen, Signale verarbeiten, intelligente Spiele meistern, sondern auch physikalisch Bälle werfen, balancieren, dribbeln oder fangen?

Shannon interessierte sich in den 80er Jahren für komplexe sensomotorische Fähigkeiten, d.h. für Interfaces zwischen Mensch und Maschine, also für die mediale Steuerung von Daten, Prozessen, Ereignissen oder Objekten in Bewegung. "As machines get more complex, this flow of man to machine communication increases enormously."[1] In