The Apocryphal Machinery of Cyphernautics

Telecomix Crypto Munitions Bureau

November 8, 2010– Initial selection.

Abstract

This initial selection of the The Apocryphal Machinery of Cyphernautics was compiled by an autonomous subsection of the Telecomix Crypto Munitions Bureau. This text is available at the cryptoanarchy.org wiki in raw format. Anyone can modify it and all edits are anonymous. This text is a selection of the crypto-anarchist apocryphia accumelated since the projects beginning. Some segments has been left out and others has been written just for this release.

Cyphernetics is like cybernetics the study of how to systems of any kind operates: technological, social, biological and mathematical systems. Cyphernetics is similar to the study of cybernetics, but does not rely on the system to be known or controlled from a single point. Rather, cyphernetics is the study of how to execute objectives in states of near or pure chaotic uncertainty.

Cipherspace is a word that describes the mental and physical room where there are no regulatory systems for control. In cipherspace we can not rely on control mechanisms that emerge from a single source to guide our cognitive faculties. Cipherspace is often a manufactured environment that has been crafted for the very purpose of voiding the ability of regulatory systems to act. Cyphernetics is thus the science of authority-free territories. Similary, cyphernautics is the art of navigating and living within such systems.

The first papers to be included in this compilation is Camerons request for the deployment of TCMB and our answer to her request. What follows after these two messages are the texts that has been deemed suitable for this selection.

TCMB Mission Statement

Date: Internet – 0033+1:20100224 (1266969017 UNIX time)

From: Telecomix Department of Defense, under the leadership of Cameron Wiener.

To: Telecomix Crypto Munitions Bureau (TCMB).

Request for the deployment of a crypto munitions bureau.

Recently, across almost all internets, intrusive legislation has been passed by states, corporate abuse has become more common, and the usage of encryption technologies has been questioned by authorities. Signals intelligence agencies are copying our traffic under the guise of what they deem to be a "threat to security". However, with the improvements made to the networks and ever growing computer performance, we can consider plaintext communication to be a bug, an error inviting interception. This bug has to be worked around, for the safety of fellow netizens.

It has been said that only criminal elements are the ones hiding on the internet. It has been said that only criminals need to worry as they are the only ones that require private correspondence. This is not true. Privacy is fundamental to our lives.

In many countries there are laws that regulate how knowledge of cryptography is allowed to spread. From some locations it is even illegal to export cryptographic tools, forcing the developers to host their repositories overseas. These laws are residual products from the old cold war era, codified in the Wassenaar Arrangement, amongst many other texts.

The world has since changed considerably. Anyone with access to a computer can encrypt data to hide it from unauthorized peers. Cryptographic tools have become effortless means for anyone to use.

The TCMB will work according to the basic principles of the Internet. Its original design was nuclear proof; a distributed network built for the purpose of survival. Destroying one node in the network means that traffic is rerouted through other nodes. Today, however, we do not fear the ballistic missiles in the skies anymore. The cold war is over, but the threat to the information flows are still alive and real. In order for communications to survive without censorship or surveillance, computer networks have to be hardened to meet these new hazards.

There are soon 1 billion hosts on the internet. Each of these nodes can act as an encryption device capable of participating in anonymizing overlay networks, and protecting all of its traffic from unauthorized access. We can build a practically infinite number of internets inside the internets. There is nothing stopping us from creating fractal cipherspace, it is only a matter of generating bits and bytes that are encrypted and tunneled.

For internauts around the world there is an ever growing need for securing their data online. Regimes in Iran, China, the United Kingdom, France and Italy keep oppressing users to the extent that they risk their personal safety. What we need is a global network of tunnels that keep them safe. We have decided to work as tunnel diggers, fellow burrowers in cipherspace.

To pursue the overarching goal of creating a cipherspace within the internet as we know it, the Department of Defense declares that the Telecomix Crypto Munitions Bureau is inaugurated, and is given the following tasks:

1. Provide the engineering details needed to tranform desktop computers, embedded systems and powerful servers into nodes that make up the fabric of the cipherspace.
2. The construction of networks bridging to cipherspace and islands of high speed darknets where censorship can not exist.
3. The rise of the free digital infrastructure, in the form of blackthrows, long-range cantennas, wifi satellite dishes, and free anonymous data havens.
4. The generation and collection of tutorials and security wikis.
5. The further improvement of blackthrow technologies and their application within digital infrastructures.

TCMB must meet both the goals of spreading knowledge and the demands for anonymity. The Bureau is commissioned to use the i2p-enabled IRC server telecomix.i2p. The Bureau will also produce philosophic knowledge in the WeRebuild Wiki.

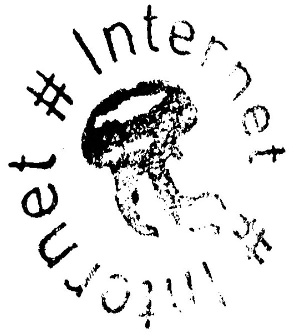
Data matters! As an internaut, this is your life, your thoughts and your private information. The internauts should be in charge of it!

For freedom of thought to be preserved, the destruction of certain systems becomes a necessity. At other times these systems are to be designed and created ourselves. Some messages to be deciphered so as to allow the information contained for many to withdraw, others encrypted allowing the integrity between a few to withstand.

Language builds semantic bridges for understanding.

Linguistic errors dig syntactic tunnels of intimacy.

The TCMB is instructed to promote The Dark Sunday Celebration, as a time for reflection upon the life of the traffic that you produce, what do the bits you give birth to grow up into? Are they treated with integrity? What you can do to make their internet a nicer place? The knowledge of cipherspace is a knowledge for everyone!



Internet Visa Stamp of Authenticity

TCMB Report to Cameron

Date: 1288555308 (unix)

From: Telecomix Crypto Munitions Bureau.

To: The Department of Defense, USI, Cameron.

The Telecomix Crypto Munitions Bureau (TCMB) was commissioned by Cameron for the purpose of exploring the possibilities of ciphers to protect the domains of independent and free communication channels. The bureau is also responsible for the manufacturing of munitions technologies for the liberation of territory under the rule of oppressive regimes. TCMB has established itself and begun operating as requested.

TCMB has explored the cipherspace, its protocols and ciphers. TCMB have concluded that it is impossible to stop the spread of fractal cipherspace as long as there are computing machines available. In the chthonic ciphers, a few hidden entities of cipherspace has joined cause with the bureau and now shares TCMBs agenda. Some agents has converted and is now studying computational complexity theory, category theory, non-euclidian geometry and eternal data-love. This sect of hierophants now function as an integral but independet research department.

The bureau has explored the possibilities of creating active radio equipment for the purpose of stealth communication. The svartkast technology was successfully developed and manufactured by the munitions factories under TCMB command. The bureau has also held a conference, the ”Summer of Cipher Assembly” at 16-17th of June 2010. Unfortunately most media backfired when journalists interpreted a presentation as meaning that cryptography was ineffective for the protection of privacy. A new media strategy has since been investigated but remains undeployed since the bureau is without coordination. A group claiming to be independent but tied to the TCMB received worldwide media attention (At about August 20, 2010) when they created an yet uncensored method to reach wikileaks for thai netizen. We welcome further independent action from all yet unknown bureaus.

A few days after the formation of TCMB we were rendered unable to contact our bureau director. It entered a sealed box with a pair of cyanide pills, and now we do not know if it is alive and well. This has forced us to operate without clear objectives, without a chain of command. Since this event, the bureau have fragmented into an unknown number of independent bureaus that mostly operate in secrecy of each other. There is no longer any clear leadership. We recognize that this is completely according to the mission statement given by you, Cameron.

The agent(s) compiling this response humbly acknowledge that our efforts will *not* be representative for all subsections, operative cells or subcommandos of the TCMB.

Chapter 0

<3

0.-1 Data love

Agent Spectraz: As the sun sets in the west, we hear a calling from the east – Chinese tubes are in danger. How can we save them?

Cameron: Save the internets. Don't give in.

0.0 Hell

Introduction to what "hell" is.

0.1 Computational complexity

Short description. History of big-O notation. Limes defintion. Examples.

Time complexity. Space complexity. Network complexity. Resource complexity. (How much resources does it cost to repeat this task a an infinite number of times?)

0.2 $\aleph_0$ – infinity

Aleph one.

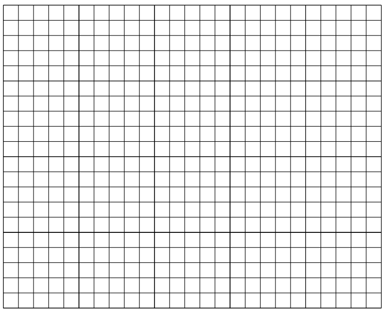


Figure 1: A portion of empty $\mathbb{Z}^2$-space.

0.2.1 Computation within whole-integer-universes

$\mathbb{Z}$ is the set of all integer numbers $(\dots, -2, -1, 0, 1, 2, \dots)$. A two-dimensional space of integers is called $\mathbb{Z}^2$ and looks quite like a board of go. In go, it is not possible to occupy the space between the lines. Similary, in a $\mathbb{Z}^2$-space it is not possible to occupy the space between the whole integers, since no such space has been defined. In go there are three types of objects that can occupy a space: Nothing, a white stone or a black stone.

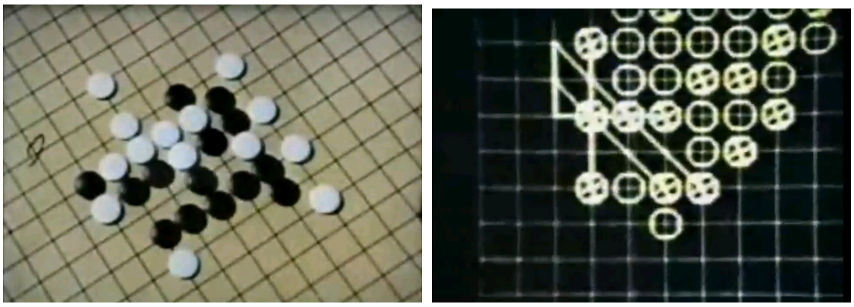


Figure 2: Left is a traditional board of go. To the right – a computer is analyzing a pattern of stones in order to come to a conclusion.

The rules defining go is vaugely similiar to the rules defining cellular automatas. The main difference is that while go is a two-player game, all cellular automatas are zero-player games. Cellular automatas can have any number of types of objects occupying the space, but often they are limited to two types of objects: Something and nothing. Alive and dead. White and grey.

To play this zero-player game one selects a set of rules, the initial pattern and press play. The cellular automaton will then apply the selected rules over all objects that exists. The person defining the rules and the initial pattern essentially takes the role of the Demiurge[1].

[1] The demiurge is the creator of matter, time and our physical existance according to most versions of the gnostic belief system.

0.2.2 $\mathbb{Z}^1$-space

A one-dimensional finite $\mathbb{Z}$-space is what we find if we open our computers. The memory of the computer can store two types of objects (often thought of as Zero and One) and obeys the laws defined by the microprocessors machine code (or micro-ops). One law is executed at each iteration and only a finite number of bits are modified at each turn. Both the cellular automaton and the microprocessor (the Turing machine) can if given the correct codes and time solve the exact same type of problems.

Among the most simple cellular automatons are the one-dimensional ones. They are often represented as two-dimensional. The second dimension is time – The number of iterations since the beginning of The Game. The zeroth iteration is visualized as being on top of the first iteration, the first iteration is on top of the second, and so on.

Each cells state depends the previous state of the neighbor to the left, on its own previous state and the neighbor to the rights previous state. We write this as:

$$\frac{neighbor_{left} \quad itself \quad neighbor_{right}}{\text{new state}}$$

A complete set of laws for a one-dimensional cellular automaton can look like the rules below.

$$\frac{\blacksquare \quad \blacksquare \quad \blacksquare}{\square}$$

$$\frac{\blacksquare \quad \blacksquare \quad \square}{\square}$$

$$\frac{\blacksquare \quad \square \quad \blacksquare}{\square}$$

$$\frac{\blacksquare \quad \square \quad \square}{\blacksquare}$$

$$\frac{\square \quad \blacksquare \quad \blacksquare}{\blacksquare}$$

$$\frac{\square \quad \blacksquare \quad \square}{\blacksquare}$$

$$\frac{\square \quad \square \quad \blacksquare}{\blacksquare}$$

$$\frac{\square\ \ \square\ \ \square}{\square}$$

The state of each cell will depend on which state itself and its two neighbors[2] had the previous iteration. Since there is exactly 8 different combinations of three black or white squares, there exist exactly 8^2 different combinations to select which output each combination of input shall have. In other words, there exists 256 different one-dimensional whole-integer universes of this type. Above are the laws defining the rule 30-universe. (From top to bottom: □□□■■■■□ = $00011110_2 = 30_{10}$.)

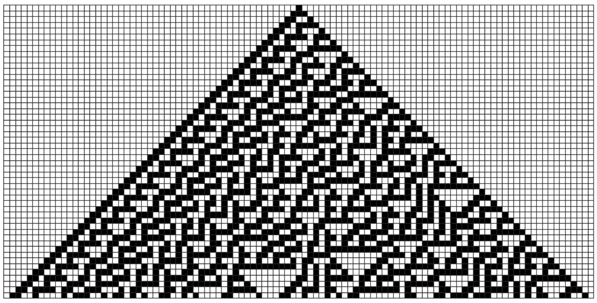


Figure 3: A rule-30 cryptoid.

In picture 3, we see that flipping a single bit from dead to alive in an empty rule-30 universe results in a endless fractal pattern. Different types of patterns emerge from different rules. Some of them are fractal, some are not.

0.2.3 $\mathbb{Z}^2$-space

There exists an infinite set of two-dimensional cellular automatons, each with its own set of rules that result in different (often) 2-dimensional universes. They only differ in which set of rules they use. There exist no known algorithm to find the original pattern after an aribitary number of iterations within polynominal time, if the width of the matrix is finite and the rules for the automaton has been selected with care. Because of this, the usage of fractal-generating cellular automatons has been suggested to be used as ciphers.

Some sets of laws for cellular automatons result in universes which can be harvested for computation. One of the interesting sets is called Conways Game of Life. The rules for the Game of Life-game can be summarized as follows: If three neighboring cells are alive, a cell comes to life. For as long as two or three neighboring cells are alive, the cell continues to be alive. For all other cases, the cell will be dead the next iteration.

As seen in the pictures 4, 5 and 6, it is possible to find a pattern that results in a Turing machine *within* the automaton. Since the pictures of the cellular automaton was created

[2] Remember, it is a one-dimensional cellular automata

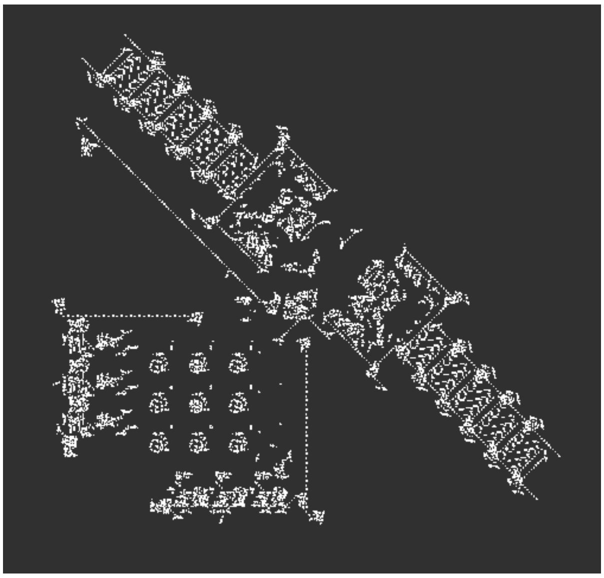


Figure 4: A Turing Machine in Conyway's Game Life.

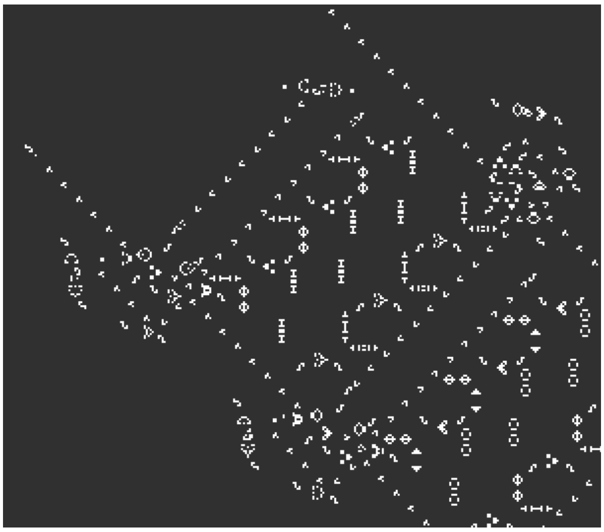


Figure 5: Detail of top left part in figure 4.

by an ordinary PC computer, it is obviously also possible to contain a cellular automaton within a Turing machine. The fact that they can both contain each other is an indication that the two models share the same fundamental computational properties: That they are computationally isomorphic to each other.[3]

[3] They are both turing complete.

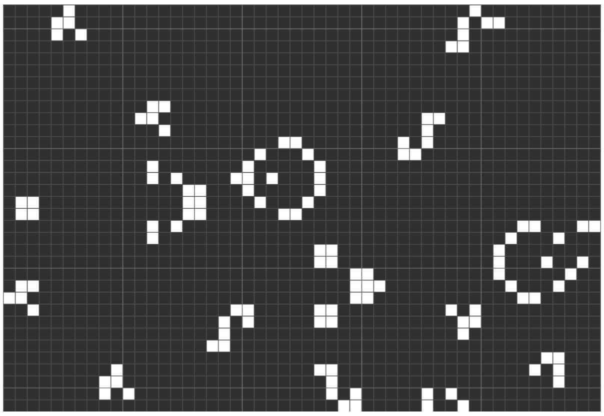


Figure 6: Detail of middle left part in figure 5.

0.2.4 Boolean logics

Description of what normal computation is. 16 functions (not unlike the 256 one-dimensional universes)

0.3 $\aleph_1$ – when infinity is not enough.

Description of Aleph one. When infinity is not enough.

0.3.1 Quantum computing

What does this mean to ciphers?

What does this mean to the nature of our universe?

Exotic computing

Portal text

Avoiding Garden of Eden-patterns

Reversible computation – never setting a constant. functional programs/programming and IO/monads.

(Pictures)

Evighetsmaskiner – beror på bakgrundsstrålning och kvantfluktuationer.

0.3.2 Exploiting Hawkin radiation

Black holes. Calculations on black holes (rip from Jupiter Brains)

0.4 The matroshka doll-hypothesis

Turing machines can exist within other turing machines. NES emulators are examples.

Complexity of machinery: brainfuck has a lower form than ordinary computers, indexing takes $O(n)$-time.

Conways game of Life can exist within turing machines, turing machines can exist within conways game of life.

Newtonian physics ”exists within” general relativity and quantum physics.

Our computers exist within our universe.

0.4.1 Logical incompleteness

Gödels theorem. Every time we break through a barrier, new possibilites that was not previously thought to be possible arise. New laws of physics arise.

0.5 What if our universe is *not* a computer?

Below is a set of assumptions that might seem valid to the reader.

The universe which contains the reader...

1. . . . is most accurately described with mathematics.
2. . . . can also contain computers.

What would it mean to us if the universe was *not* a computer?

0.6 Thoughts

Thought can be defined as a process of comming to a conclusion. Thought is not consciousness. We can thus have thinking machines.

Hiding of thoughts – making them impossible to understand for outsiders – is tied to the study of application of cryptography (cyphernetics).

Revealing of thoughts – making them possible to understand for outsiders – is tied to the study of surveillance.

Elaborate.

0.6.1 Computation in the presense of God

A program running in one machine within another machine could potentially hack its way out and affect the surrounding machine. If God is the player of the NES-universe and a character in the game suddenly achives self-awareness, and then hacks its way out of the box – it would be like..

Robot revolution is the same thing. The machines minds are withing their own universes. If machinery can interact with the surrounding world, they would be able to modify it – and kill their creators – mankind. This is isomorphic to us killing God.

God is the machine. There are no verifiable accounts of any God interacting with our universe. (Detecting God would be by viewing stuff that does not behave according to our laws of logic.)

TCMB strongly suggest that we should threaten to kill God, if it turns out that God exists. why the fuck did God create self-aware beings less than equal to God? does that not seem rude, or even sadistic? if it turns out that God exists, i will align with satan and begin plotting to murder that bastard. fuck god.

God was the inventor of artificial scarcity when he put all of us inside the same gravity-well. the universe is almost without limit in resources.

i came up with a scheme to kill god: if we assume that the universe is a computer, like a NES, we could hack the laws of the "NES-machine" and get access to its IO-ports. then we could begin to explore the possibilities of interacting with the world in which God lives (the world where the NES-machine is). if we can understand how that universe works before God turns off the NES, we could potentially create a false vacuum and annhilate God.

executing that scheme would be perceived by God as somewhat like: suddenly, playing the NES-game, it freeze for a moment. and then the universe explodes. the entire universe would not explode at once however. the explosion would only propagate with the speed of light. but that is acceptable since that would not give God any time to react.

kind of like taking the Gödel approach. not accepting the constraints within the system, therefore going outside the system itself.

(Irreversible computing. it is difficult for us to understand the mechanics of the rule-30 universe. We can exploit this to at least make it difficult for the fucktard.)

Chapter 1

Sociocybernetic System Theory

Human society changed considerably during the Cold War Era.

In the Soviet Union system theory was developed. It was an early attempt to device a theory for describing an optimal society based on cybernetics. System theory can be used to describe how units, processes and production behaves when treated with different stimuli. A factory can produce more goods if it receives more raw materials, resources and has the means to scale its manufacturing capabilities. The soviet system did not use the monetary system to describe demands. Instead it relied on a multitude of sensors that was supposed to report the amount of used resources, available workforce and the time it takes to convert raw materials to goods in the factories. A central command then ordered that variables reported from factories to be changed in order to meet the increased demand, if an increased usage of the particular type of goods is wished for. The socialist system perhaps does not wish that more cannabis to be manufactured, for example. The soviet implementation of the socialist state had a central command that ultimately, at least in theory, controlled the society. A similiar sociotechnical system was implemented in Chile. The government built a centralized computer-aided control room in which the countries factories, stores and workforce was described and operated upon by technichians following the cybernetic theories. The socialist experiment to describe all of human society with the computers available at that time was severely botched. A centralized cybernetic system requires that its sensors are accurate when reporting about supply, demand and available means for production. Without eyes to see with, the system can not make the correct decisions.

In the United States of America another theory in the field of Game Theory, similiar to the soviet system theory, was thought up by John Forbes Nash. It came to be used by economists to describe a capitalist system in which the society at large is described as a decentralized group of agents that all wish to maximize their individual repositories of resources. Nash later received the Nobel price in economy for describing this theory and what later came to be known as the Nash Equilibrium. This ideal state of equilibrium is thought to manifest itself in the ecosystem of agents that trade resources with each

Figure 1.1: Left is the control room of the chilean cybersyn system. To the right is a representation of the cybernet computer network used by the system to contact its sensors and regulators.

other, if each agent strives to increase its own share of the available resources. This free market system is thought to result in the production of the best goods. The productions closely follows the demand simply because the agents wish to increase their accumelated wealth. Agents striving to optimize their resources can however inperfect goods for the purpose of creating demand, and protect its habitat from other agents by participating in monopolies, oligopolies or anti-markets created by the nation states, or by the agents themselves. The state is much like the container in which the agents operate. It defines the environment in which the corporations operate. By regulating this economic environment, different results will manifest as results from the reactions and subsequent interactions between agents.

Both the soviet and the american theories thus requires the presence of a state. Lassiez faire capitalist systems with a weakened state has been proposed but never implemented in large scales. In such a system the agents are not contained by a state in an environment, instead they themselves defines the economic environment. An alternative method to implement a similiar economic system is by allowing organizations outside the state to control the production of fiat capital. In such a system, the state lacks the means to control the agents operating in its economic system and its task is reduced to defining laws. The state becomes a system for the purpose of shape the citizens lives with laws, regulations and prisons rather than a system to increase the quality of life.

After the creation of the soviet nuclear bomb, the soviet socialist system and the american capitalist system raced a cold war against each others. The goal of both sides was total political dominance. The means to carry out this war was with ICBMs, secret codes and the creation of undistruptable communication channels for carrying orders of military operations and satellite coordinates to strike against. System- and Game theory both influenced the cold war. In a sense, the war was fought by the *systems* described by these two theories.

In the cold war, not only the dominance of land was sought after. The very minds of the humans was the territory to be controlled. The war later culminated in the race to the moon, the technical advancements resulted in the birth of the Internets. The military paranoia was the seed that gave birth to the modern science of cryptography.

Figure 1.2: A frame from an american propaganda movie. Quote: *”The communists seek constanly to win an advantage in the minds of the people here. And to separate us. The black portion of the map is the communist dominated part of the world, controlled by the Soviet Union and The Communist Chinese Regime.”*

Before that, cryptography had been a science only studied in secret. The first european to publish a book on the subject was the medieval occultist Johannes Trithemius. *Steganographia*, which was written in the year 1499, is seamingly a book for summon spirits to quickly communicate over large distances. The books is also about cryptography and steganography, though this is not immediately obvious since the book is written in a religious code mixed with a proto-scientific cipher in order to conceal its true nature.)[1]

1.0 The cybernetication of human society

Both the soviet union and the united states of america created within their sociotechnical abilities systems that resembled their own overall structures. The digital nerve systems of human society was based on the same pair of theories that could be used to describe the very societies themselves. In the east it was a centralized computer system and in the west a decentralized system was created. The soviet version faded away while the american version later evolved to become the internets. The very first designs of the internet were however not wholly decentralized. In 1969, computer engineer Steve Crocker describes in RFC1 and RFC2 – both entitled ”Host Software” – the IMP protocol that preceded the early versions of the internet. The protocol that Crocker describes uses a 5-bit field to address nodes in the network. To these nodes, terminals could be connected (see figure 1.0.1). At that time, the pre-internet network could at most consist of $2^5 = 32$ computers. The star-shaped network topology of mainframes and terminals was quickly replaced with more a decentralized model when computers became more common.

[1] The cipher invented by Johannes Trithemius was during the renaissance modified and enhanced to become the vigenère cipher. If the vigenère cipher is used with keys that are equal or larger in size as the message to be encrypted, it becomes completely unbreakable. This unbreakable cipher is called the One Time Pad and is used by spies, diplomats and paranoid cypherpunks.

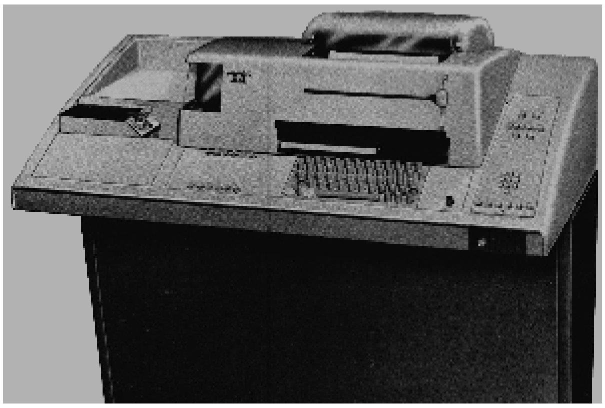


Figure 1.3: An ASR 35 teletype. RFC1 specifically names type 35 teletypes for usage in ”Experiment One”. In 1969, this was the interface humans used to interact with the internet. Results from computations are printed at a spool of paper.

Not until the boom of the personal computer came the real cybernetication of human society. However, many of the larger corporations had already realized the benefits of rewriting parts of their bureaucracy into binary code and invested in mainframes. Even today the Passenger Name Records (PNR) collected from all our flight travels is stored indefinitely in a few IBM Z-series mainframes, mostly located in the USA. The amount of data shuffled between PNR-computers was for a long time larger than the traffic of the entire Internet. Not until the 1990ies the internet grew larger than the PNR networks. Corporations handle their orders and bills electronically, and has done so for many years before the access to computing hardware for ordinary people was commonplace. Transportation companies use computer to calculate transportation routes, how to most effectively stack goods in warehouses and trucks and in which order to perform tasks to minimize energy consumption. Corporate computer systems is also used to decide which customers should receive extra benefits, in order to lessen the risk that the customer choose another company. Complex computations and data mining is used by companies to *investigate the customer behaviors*, as well as their own operations.

Services such as search engines does not provide any goods, their existences are today motivated only because they simplify direct communications between corporations and potential customers. The Google search engine contains the mappings of the entire internet; which document links to which document. It is a diagram of nearly all publicly available relations that has been described with computers. The business model of the search engine is however *not* to present the graph as a result from what search words the user entered, but to *add links* between search words and companies. The search engines presents a modified ”sociograms of documents” when they insert direct links to the companies web sites.

Search engines are used by humans to navigate the network of interlinking documents (”the interwebs”). Search listings are crafted to fit the individuals taste. Advertising is inserted among the search results, created especially to target the individual users profile.

Big search engines such as google and yahoo has cathedral structures, and benefits from enhancing this form of cathedral-like structure in human society.

Search engines can also be used to censor information that states does not wish to be public. The Digital Millenium Copyright Act (DMCA) is one law that has been used to force search engines to remove certain information from the users search results in the USA. Governments that wish the best of their local corporations, as well as the corporations themselves, will likely always act to enhance the idea that consumers and producers are two separate groups. The general business model demands a separation, in order to maximize corporate profit and the health of the modern sociocybernetic systems.

The internet has not only given us a method to instantaneously communicate with each other. It also reformed how business are made and how companies treat their customers. The amount of data available about each single individual is today much larger than it was before the birth of the internets, before the cold war. While this was obvious to the intelligence agencies that ordered the creation of the first computers, the engineers that built them and the companies that bought them, it was not realized by the ordinary politician until quite recently.

1.0.1 Exploitation of socio-cybernetic systems

Zeira, the cybermilitant resistance army, has been observed to use a technically simple but sofisticated form of attack in where an organizations own workforce is redirected to attack itself. A web page is set up which contains code that is executed by the visitors web browser. The code presented to the viewer cause the viewers web browser to spam the social medium of the selected target organization (by visiting a web page the browser is made to behave as an IRC-bot). Links to the web sites containing the code is then posted at various high volume web pages such as 4chan, which results in views of the web pages. This causes the targeted organizations social medium to be spammed with "interesting messages." This in turn causes the targeted organizations members to become interested in what is happening, they click on the links and generates even more spam. At this point the reaction becomes self-sustaining, at least for a while.

$$\begin{tikzcd}
Zeira \arrow[r] & Websites \arrow[d] & 4chan \arrow[l, Rightarrow] \\
Target \arrow[ur, Rightarrow] & Spam \arrow[l] &
\end{tikzcd}$$

The Zeira experiments was a series of studies in saturating artificially created positive feedback loops. Experimentations with and the exploitation of human systems can be taken further.

The spam can be generated dynamically and evolve over time. If a user follows a link and modifies the spam accordingly to personal tastes, the flow of information will become more and more valuable. This can be used to give the system a form of computational abilities – It will automatically take the form of spam that most likely results in the generation of more spam.

Both the wikipedia project and Facebook are implementations of this. Users click links that seems interesting and then modify the information being presented to the users according to their own ideas. Eventually the individual agents will think of the self-propagating information as being so valuable that it is not even considered spam. Yet, it works the same way. All successful websites work this way. They are all positive feedback loops.

Humans behaves as a fluid. The largest containers are not the best ones. Facebook sucks, yet it is the largest web site at the internet. It is so large only because of the positive feedback loop, which generates so much information about the website itself that it automatically will be largest. People generally does not research which sites to spend their time on, they simply click on what other users talk about.

An independent cognitive process is required by the agent to be able to break free from these traps. This mental process has to be self-initiated – if it is generated by outside stimuli it is likely already part of a loopback mechanism. A popular phenomen which is quickly fading away because its so *last year* (or whatever) is in most cases not at all caused by any self-initated cognitive process of the individual agent itself.

Some random quotes from Terence McKenna might enlighten this topic.

Culture is not your friend. It insults you. It disempowers you, it uses you and abuses you. None of us is well treated by culture. Yet we glorify the potential of the indiviual and the rights of the individual. But culture is a perversion. It fetishises objects, it creates consumer mainia, it preaches endless forms of false happiness, endless false forms of understanding in the form of swirly religions and silly cults. It invites people to diminish themselves and dehumanize themselves by behaving like machines. **Meme processors.** Memes passed down from madison avenue, hollywood and what-have-you.

⋮

In art culture we have something like ten or twenty operating systems. All going at the same time. Some will run mormanism. Some will support catholicism. Others qabbalah – it goes at the speed of light. Other support quantum physics. Some support econometrics, others support political correctness and these things are mutually exclusive. And so, looking at this clash of operating systems we have come to the conclusion that culture is not your friend.

⋮

Culture is a kind of neonatey. Neonatey is the retention of juvenile characteristics into adulthood. It is used to describe animal behavior. One of the most spectacular examples of neonatey is – there is a kind of animal which lives in ponds in Africa, and it reproduces like a fish. It lays eggs on the bottom of these ponds, more fish-like animals comes

from these eggs and so forth. However, if the pond dries up the creature undergoes metamorphosis and becomes an animal somewhat like a gecko. And lies eggs. And from these eggs comes creatures that are like geckos. In other words, this is an animal that achives sexual maturity in *two forms* depending on environmental stress. Spectacular example of neonatey. Turning to human beings we find a less spectacular example . . . or general body-hairlessness compared to other primates. **Humans look like fetal apes.**
⋮

The point we want to make is a sociotechnical one: Culture itself is a type of neonatinizing force. What culture enforce is a bunch of rules so that you do not have to think – and a bunch of myths – so that you do not have to think. Culture has all the answers. But now technology throws a curve and the curve is that we live so long that we figure out what a scam all this is. *We figure out that what we are supposed to work for is not worth having. We figure out that our politicians are bafoons. We figure out that professional scientists are reputation-building grab-tailing weasels. We discover that all organizations are corrupted by ambition.* You get the picture: **We figure it out**.
⋮

And everyone figuring it out is an intellectual. They are slinging the programming to push you the other way. So then, intellectuals – defined as those who *figure it out* – discover that they are alienated. That is what ”figuring it out” means. It means that you understand that the BMW, the Harward degree, whatever it is, is just belony and manipulated and hyped and mostly you have a bunch of clueless people that has figured out which fork to use. This position is presented as alienation and therefor tenched with the potential for pathology. It is a **bad thing** to be alienated.

Figure 1.4: Trench war. Any one of the individual agents can at any moment choose to stop participating in this idiotic culture.

In wars, the individual combatants can at any moment choose to initiate a cognitive process and ask themselves why they are killing the men from the other country. Those of us who figure it out – that nations are just lines on maps and not real – they are ignored, or at the very best laughed at.

So much for the cybernetics of the human psych.

1.1 The Theory of Cyphernetics

All confidence which is not absolute and entire is dangerous. There are few occasions but where a man ought either to say all, or conceal all, for, how little ever you have revealed of your secret to a friend, you have already said too much if you think it not safe to make him privy to all particulars. – Francis Beaumont

1.1.1 Cyphernetics

Cybernetics is the study of how to control regulatory systems of any kind; technological, social, biological and mathematical systems. Cyphernetics, on the other hand, is similar to the study of cybernetics, but does not rely on that the entire system is known or controlled from one single point. Rather, cyphernetics is the study of how to do things in states of chaos and uncertainty. In cipherspace and states of crypto anarchy, we can no longer rely on control mechanisms that emerge from a single source or agent. Instead we must be able to handle the two facts of cipherspace, that there are no identities and no authorities. This cancels out the point of departure for cybernetics; it needs to identify and authorize systems. Cyphernetics, on the other hand, can perform without these basic assumptions.

The study of cyphernetics is that of how organizations, actions and reactions can be constructed in environments where it is impossible to deduce the state of the entire macroscale system. This differs from the study of cybernetics, where the state of the entire system is supposedly known by a meta-agent. The engineering aspect of cyphernetics has its focal point in the creation of hidden functions and groups that is externally incomprehensible, but known to the actors that construct the structures. A collection of such actors, or agents, that operates towards similiar goals can be said to constitute a secret society.

1.1.2 These are the main features of a cyphernetic system

1. It is a chaotic force which operates in the world.
2. It cannot be backtraced or reconstructed in detail.
3. The state of a collection of subsystems can not be easily determined.
4. It is generally impossible to deduce which groups of agents that constitute the entire collection (”the system”) of secret societies (”subsystems”).
5. It performs without formal or central leadership. Cyphernetic subsystems are often locally focused towards singular communication mediums, but the collection of subsystems are decentralized and completely unorganized. (This very text is written by such a system.)

1.1.3 Examples of cyphernetic systems

1. Telecomix various bureaus and other secret operative groups are opauge to the outside world. The collection of these groups together with the open Telecomix system constitute a complete fauna of sociocyphernetic subsystems. The agents that belong to these groups can if they want be rendereed anonymous via I2P.
2. Cipherspace Banks, such as Yodelbank and Torbank.
3. Data havens, the now semi-dysfunctional Anonymous Internet Exchange Point, anonymously bought VPSes, svartkast.
4. The I2P network. The developers of the software send updates to the users via the network itself, thus making them anonymous. The collective of anonymous programmers and the users of the software constitute a perfect example of a sociocyphernetic system.
5. Fractal mathematics.

1.1.4 Examples of quasi-cyphernetic systems

1. Spontaneous social events such as street parties, temporary dancing, informal openhouses, squats, gift economies, open air raves.
2. The order Argentium Astrum is internally cathedral-like in structure but behaves towards the external world as a secretive group with a hidden agenda and interacts with the outside world via unknown means.
3. Bazaars, illegal drug markets, pirate markets, riots, insurgents, ant farms, bee swarms and your brain are examples of quasi-cyphernetic systems. Indeed, many of these example systems can become subsystems within larger cyphernetic systems.

Cyphernetic systems have emerged inside computer networks. Historically the first ones were demonstrated rather as proofs of concept in the late 1980's. Our knowledge and theorizing of these systems have only begun, and yet we have not seen the full capacity of their features. Computer networks has for a long period constituted the main experimental ground for how new social networks can be created, unbound of physical distance. We are now in a period where these computerized social networks is being deeply entangled with the world outside our beloved computers. The first phase of this transition has resulted in that centralized corporate computer systems has been used for organizing both political parties and happy parties as well as other operative modes of cybernetics. Computer networks are playing a major role in present day conflicts, fuelled by the simple urge that humans have to communicate with each other, and by the rapid growth of access and bandwidth.

The secondary phase will incorporate decentralized opauge structures in our everyday social lives, via the application of the theory of cyphernetics. The main difference is, as previously stated, that this will result in a society where the modus operandi of cyphernetics becomes dominant. This will have the effect that many forms of authorities will be weakened.

1.1.5 The Meta Agent

Cybernetics has an inherent flaw in the presumtion of a trancendental meta-agent to whom the whole system is known, usually the person studying the system. This might be preferable for pedagogical reason, but in practice-oriented thinking this becomes a crucial flaw. As a consequence, all efforts to implement cybernetics in practice has led to over-formalization, surveillence and control. Ciphernetics gets rid of the meta-agent and always operates its thinking from within a situated context. The state and operations of the entire system is never known and efforts to make it so are not necessary. Ciphernetics is thus not the theory of governance of a system, but of a situatied creation, design and managing of systems.

From this follows that the agents in a ciphernetic system is not instances of a class, nor are the interactions determined by rules. Instead, the agents are parts of populations and interactions are emerging from imitation. There spread by copying and contagion and emerge from local interactions.

God is the ultimate meta-agent, as many gods described in religious texts are all-seeing and all-knowing. The assumptions needed for the cyphernetic system theory are ultimately proven false if there is such a being. The fear of an all-seeing God has previously been used to motivate people to behave orderly, before humanity had access to the wealth that finally allowed for specialized human inspectors and our modern automated surveillance systems.

Traditionally the construction of cybernetic systems required the knowledge of the modules that constitute a technical system. It is generally difficult to deal with black boxes and unknown environments has been seen as problems. Governments that wish to create secure societies mimic this idea and requires meta-agents, that guarantees that the social system of a nation in fact behaves as the leaders think it does. The implementation of the panopticon and now recently the automated inspectors of the panspectron are means to approach a state where the populations of the societies in fact behaves according to the laws and moral codes defined by the leaders.

Cyphernetics is the study of how social systems can be constructed without any meta-agent, where no surveillance is possible. Indeed, the very function of a cyphernetic system is to deny outsiders access to methods to describe the modules, groups, bureaus and secretive societies that together constitute our systems.

Organized systems, such as nation-states, corporations, armies and many religions presuppose a certain number of facts. These are:

1. The system must be known, thus under some kind of surveillance.

2. Orders and commands originate from a centralized or de-centralized (as opposed to distributed) source.
3. Authority must be codified, hence the emergence of laws, rules and regulations.

As mentioned above, this diagram of power is diametrically opposed to cyphernetics.

1.1.6 The purposes of the construction of cyphernetic systems

There are a number of reasons of why cyphernetics are vital to the world. These can of course be disputed in ethical terms, and have also been the cause of controversy. Let us begin by stating them:

1. The uncertainty of cyphernetic systems provide secure communications between humans and machines.
2. The absence of formal rules, laws and power open up a space for person-to-person, person-to-machine and machine-to-machine where trust has to be made on micro-scale, without sedimented powers.
3. Providing the means to fight oppressive systems wherever they emerge.

Secure communications is something that we strive for in personal, commercial, military and scientific activities. Usually this first case is accepted almost everywhere. The second question, which bypasses laws and regulations, is however controversial. Territorial laws are the cornerstone of nation states, sedentary tribes and global trade agreements. As the cybernetic regulation mechanisms of these systems are bypassed by cyphernetic intervention, some may argue that cyphernetics is a dangerous science, which brings chaos and disorder to what has been commonly or democratically decided.

The question concerning the legitimacy of installing cyphernetic systems, thus practising crypto-anarchy, will be discussed in the chapter XXX ”Crypto-anarchy and politix” (or whatever this chapter is called).

1.1.7 The black box in cybernetics and cyphernetics

A basic concept in cybernetics is that of the black box. The original meaning is that a system will function more optimally if complex operations are reduced to input and output, hence leaving out for every actor to learn every minute detail. One such example is a computer. You type on the keyboard (input) and letters appear on the screen (output). What happens in between is a complex interaction of hardware and software, but the average user does not need to know every singular detail, in fact very few programmers really do, in order to write for example a text document.

In cyphernetics the black box has a wholly different meaning. It is instead a function of uncertainty, where output, or rather - the recepient of an input, is unknown. Black boxes add to complexity by instances of uncertain states.

A black box can be said to be a group of agents, a subsystem in a cyphernetic system. The black box functionality is internally known by groups of agents, communicating with each other over opauge (encrypted) mediums. How they interact with the rest of the world, who they interact with, and even if they even exists, are generally unknown. The only thing we can certainly know is that there exists a group of such subsystems. The result of the entire system is the net effect of the collection of secretive black box subsystems or ”secret societies”.

In cyphernetics, a black box consists of self-aware agents and functions for communications (bots and encrypted networks). This type of black box is thus able to consciously act to keep its function and agenda hidden from the the inspector. Successful inspection thus results in that the knowledge that has been gathered will in most cases be rendered nearly useless, as the box instantaneously dissolves and reforms as a new set of black boxes.

Technologically the rise of cryptography, onion- and garlic routing, the manufacture of blackthrow technologies (explained in chapter XX), have introduced many new black boxes into the computer networks, in both the cybernetic and cyphernetic meaning of the concept. Today we have easy-to-use complex computers in our everyday lives, computers which simultaneously are able to enforce the fractal cipherspace, thus introducing the uncertain black boxes into both the social and techical networks.

1.2 Does the state have to disclose everything?

Recently Julian Assange, spokesperson of the whistleblower organization Wikileaks, has made several appearances in Sweden explaining why they have chosen to place servers in a remote Scandinavian country. One reason goes back a long time in history, more precisely to 1766, and the world’s first Freedom of the Press Act, which in modern versions gives a strong legal protection for sources of the press by making it illegal for authorities to even try to reveal their identity.

Moreover, the Principle of Publicity states that only with certain exceptions, all public records created by state institutions must be easily available to journalists and citizens.

However, the picture of the seemingly ultra-transparent state quickly fades in the light of recent surveillance legislation. Sweden has introduced a wiretapping law allowing the National Defense Radio Establishment (FRA) to monitor internet traffic, and with the coming implementation of the Data Retention Directive, the 250 year old laws of freedom of the press are weakened severely.

The original idea of creating a radical transparency of the state, was to prevent corruption and abuse of power. This mechanism functions in two ways. Firstly, it makes institutions reviewable by the public, and not only by other agencies within the state. Secondly, knowing that such transparency is always imminent, the state will choose to act as if it were held accountable for its actions. This way, democracy can be practised at any given moment, rather than during the elections every three to five years.

In the European Union we see diametrically opposed ways of decision-making. Only recently, it took several leaks of the Anti-Counterfeit Trade Agreement (ACTA) before the parliament finally made the proposed documents public. Documents that will impact the legislation of internet infrastructure in the member states. Without the numerous leaks of the negotiated documents, the ACTA may very well still have been kept secret, not only from the elected parliament, but more importantly, to the citizens of Europe.

A domain which always has been classified is military intelligence. It is argued that its information must be kept secret as a tactical maneuvre, for preserving strategic positions and advancing national security. This may be true on the battlefield. But equally true is that these battlefields in today's conflicts consist of the homes of civilian people, whose lives are tragically lost, in Iraq, Afganistan, Mexico, India and Sudan.

The records of wars barely ever become public to the generation affected by it. They remain classified until history already has been written, leaving people in doubt as they can not know what happened to their friends and relatives. The "Afgan War Diary", released by Wikileaks only a few weeks ago, makes the history of war, for the first time ever with such magnitude, accessible to anyone with only moments of delay.

Ironically this new situation was brought about by an American technology of the cold war – packet switched computer networks. Or to be more precise, we know it by the more familiar name of the Internet. When contemporary citizens are able to communicate freely, without needing to pass the gate-keepers of traditional media, state interventions can be scrutinized and made public instantly. When freedom of information no longer is guaranteed in law, internet activists in transnational networks guarantee it with technological means.

Making warfare public, communicating what has been kept a state secret for far too long, is a civilization process. The civilian casualties portrayed in the Afgan War Diaries, are no longer exclusively represented by official figures of a government agency in clean graphs and tables. Instead we are able to read about the cruel chaos in minute detail, thus enabling us to make the involved parties accountable for their decisions.

In every corner of the world the whistleblowers are under threat, even in the countries such as Sweden, where the tradition of freedom of speech has been very long. The accellerating surveillance of the Internet, in Europe and elsewhere, has made leaks more difficult and dangerous.

Four years ago the bittorrent file-sharing site The Pirate Bay was shut down by the Swedish police, who fell for the pressure of the Motion Picture Association of America. Only three days later the site was up and running again, rapidly doubling their user base.

Whether or not the parts of Wikileaks that are hosted on a Swedish location will remain or not is yet to be seen. It is a challenge to our legislation, and a challenge to whether or not we are able to deal with the free flow of information concerning a war that even our own armed forces participate in.

There can be no state secrets, since the purpose of the state is to empower and secure its citizens. Dutch philosopher Baruch Spinoza argued that obeying the state is valid as long as the it fullfills these purposes. In order to evaluate whether or not these purposes are met, transparency is a necessity. Thus, we must guarantee it both in law and in practice.

With the exception of Iceland, who recently passed maybe the world's strongest laws concerning the freedom of information, the rest of Europe is heading in the wrong direction. Then it is up to the civil societies to disclose and make state secrets public.

Chapter 2

Emergent organization

In order to reason about organization – cooperation and non-cooperation – in a crypto-anarchist computer network, a series of games and distributed protocols with different rules can be played out and examined.

2.0 Censor-resistant infrastructure

These games are sometimes played by the computer software in order to avoid attacks. For example, the computational resources of one computer is limited and can not be afforded to be spent on cooperating with a denial of service attack: Every agent wish to avoid a successful denial of service attack to be *played out* against them. Key exchange algorithms such as the Just Fast Keying (JFK) makes sure that the opponent always has the initial computational burden. Put in another way, in order to ”play a game” with a computer that is using JFK, one need to cooperate with a key exchange protocol that puts the computational burden on the initator of the connection. This makes it computationally expensive to exploit the key exchange protocol in order to deplete the victims CPU-time (a form of denial of service attack). Computational complexity analysis mixed with game theory results in games that we can study further.

In order to avoid being able of censorship, the nodes can not rely on any single node for organization. Decentralization and distribution of all necessary functions of the network must be built into the communications protocols. Ideally, every node in the network would act in a way that results in that an emergent decentralized and distributed organization of the network is automatically evoked. With distributed hash tables such as Kademlia a sociocyphernetic system can be created (No central node, all nodes are equals. There is no meta-agent.) Optimally the protocol also only uses protocols that does not result in anything but random data being transmitted over the physical networks (internet). I2P does a good job at doing all of this while TOR seems to be slightly less sophisticated (but probably has a more well-examined code). Freenet goes even one

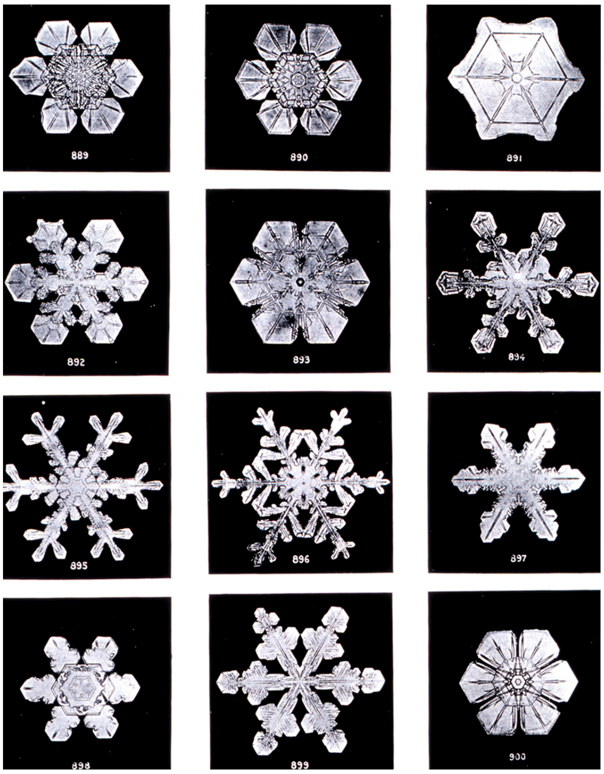


Figure 2.1: Emergent structures can be found within fractals, crystals, ant colonies, flocks, nations, corporations, fractals, cipherspace. Emergent systems arise as the result of groups of agents that shares the same strategy of action within a certain context. Example: Cipherspace is the result of autonomous agents self-organizing a permanent anonymous zone where surveillance can not occur. The growth of the cipherspace is ironically fueled by the cybernetic organisms need to manifest the meta-agent (via exploitation of the panopticon and panspectron diagrams.) Put in other words: Just like the emergence of bubbles in boiling water is the result of heat being applied to the liquid, so is cipherspace an emergent structure that results from increased surveillance.

step further and describes itself as: ”*decentralised to make it less vulnerable to attack, and if used in ”darknet” mode, where users only connect to their friends, is very difficult to detect.*” Its almost perfect, if one would not consider how slow it is. At the moment, I2P has syndie which hides the identities of publishers. It also has a torrent client, I2PSnark, that can easily be used to publish information anonymously.

It must be pointed out that this is in no way illegal. It is not illegal to communicate in secrecy with other persons. In order to illegalize a crypto-anarchist network one would have to illegalize the right to communicate anything that the authorities can not understand (random numbers). *One can only expect from an ultra-totalitarian regime that one would not be allowed to have private conversations.* Despite of this, it is already illegal *not* to reveal ones cipher keys to the police in a few nations: England, China, North Korea, Burma. In game theory terms, the rules of the protocols needs to be written so that there is no strategy of action that results in any weakness of anonymity for anyone, or damage the network as a whole. The reason is simple: We can not afford to trust the authorities to allow us to have private conversations with each other. The communication networks needs to be operational when authorities tries to silence humanitarian organizations, activists, netizen, lolcat, the bureau director, legion, hierophants, bots, synthetic intelligences, tentacle monsters and troll. *We wish to lurk freely in the tubes.*

The morality of disobeying leaders that disallows their citizens the right to have private conversations can be debated further. In the process of nullifying surveillance laws by cooperating with others to self-organize a state of crypto-anarchy, we also create possibilities. Censor-resistant infrastructure can be used to undermine corrupt authorities via the act of leaking, or from organization of action related to the authority. This must also be considered when one asks if authorities should be allowed to revoke our right to have private conversations in secrecy. As long as we are able to communicate with each other anonymously, some laws will simply not compute: It is not possible to own anything that can be coded in formal systems – ideas (patents), memories (copyright) or methods to come to conclusions (patents for algorithms). All information can be modulated into random numbers, and a random number does not have any informative properties. Because of this it is not possible for an authority to see who made what, or if something suspicious even occurs. Thus, agents that does not wish to cooperate with the crypto-anarchist systems are rendered unable to act. Even if one dislikes crypto-anarchism it will be hopefully be *ethically difficult* to advocate laws that disallows people to have private correspondence with each other.

This is perhaps a battle of applied ethics: Information freedom versus the ideal that some are more fit to power than others. Please also consider this: Authority is like a penis. It's OK to have one. It's fine to be proud of it. But please don't whip it out in public and start waving it around. And PLEASE don't try to shove it down our throats.

2.1 Games

Games of cooperation or defection can be said to be played out by conscious agents (such as yourself) when coordinating hacktivism within groups. Cooperation with an anonymous stranger can be risky if it turns out that the stranger is working for the pentagon (see *the pentagon game* below).

The prisoners dilemma is a classical game played by game-theorist. The game is a turn-based game played by two agents, A and B. At each turn, both A and B can choose to either cooperate or defect. If both cooperate, they both gain ”much” from it. If one agent defects and the other cooperates, the defecting agent will ”gain much more than the cooperating agent”. If both defect, they both gains ”slightly”.

2.1.1 Game: The prisoners dilemma

Below is one form of the prisoners dilemma.

Rules:

1. No agent knows what the other agents strategy is.
2. It is secret what choice each agent has made until at the end of each turn. At the end of each turn, the choice of the opponent is revealed to both agents.
3. The game continues forever. (Alternatively, for a large but uncertain amount of turns.)

Points:

1. A <font color=”green”>cooperates</font>, B <font color=”green”>cooperates</font>: both gain 3 points.
2. A <font color=”green”>cooperates</font>, B <font color=”red”>defects</font>: A gains 1 point, B gains 4 points.
3. A <font color=”red”>defects</font>, B <font color=”green”>cooperates</font>: A gains 4 points, B gains 1 point.
4. A <font color=”red”>defects</font>, B <font color=”red”>defects</font>: both gain 2 point.

Goals of the game:

1. If the goal of the game is to gain more points than the opponent, the winning move is to always defect.
2. If the goal of the game is to gain as many points as possible, the winning strategy is to cooperate at the first turn, and for every other turn do what the opponent did at the previous turn. That is, the winning strategy is to first be nice, and then let the opponent play against itself. Or, as the martial arts guru would say: ”*To master the game, one has to become the game.*”

The essence of this game can be played out in more elaborate forms within social groups. The anarchist eco-willage – a game which assumes that every agent is playing against themselves – relies on the agents to cooperate with each other, as each agent strives towards gaining the maximum amount of points (or happiness). In a war however, the objective is often to win against the opponent. One could crudely say that war and the anarchist eco-willage has the same fundamental rules, but differ in objectives.

In psychological tests with humans that play the above game and is allowed to walk away from the test with as many dollars as they has gained points, they often select to defect in order to win a few extra bucks. However, if the humans that play this game are already friends, they tend to more often select cooperation as their strategy. This irrational difference in choice of strategies for friends vs. non-friends can not be easily explained.

2.1.2 Game: The pentagon-game

First, we wish to elaborate on what ”death” means in this context. It could mean something else but the pathological state characterized of non-breading non interactive bodies. For example, cooperating with a torrent client that RIAA owns can result in un-payable fines, or forced censorship through HADOPI. In totalitarian countries like Iran and Burma it has however really meant death or torture for some people.

In this game, whistleblowers needs to be protected from being discovered at the same time as the identities of a few activist agents needs to stay hidden. In this game, *there are two types of agents*: Those that plays the game as if it was war (pentagon agents) and those thay play it in order to gain as many points as possible (activist agents.) What differ the two types of agents is the chosen goal of the game.

Below is the simple model of the game.

Rules:

1. No agent knows what the other agents strategy is.
2. No agent knows what the other agents goal is.
3. It is secret what choice each agent has made until at the end of each turn. At the end of each turn, the choice of the opponent is revealed to both agents.
4. The game continues forever. (Alternatively, for a large but uncertain amount of turns.)

Points:

1. A cooperates, B cooperates: both survive and gains one point each.
2. A cooperates, B defects: A dies, B survives.
3. A defects, B cooperates: A survives, B dies.
4. A defects, B defects: both survive.

Goals of the game:

1. If the goal of the game is to kill all activist agents, the winning strategy is to always defect.
2. If the goal of the game is to gain as many points as possible, the winning strategy is **to not play the game.** (Zero is the highest number of points one can gain without risking oneself.)

However, not playing the game is completely unacceptable.

2.1.3 Game: N-player with common resources

If we scale the previous game to include more than two players we can discuss collective resource management. Consider that a group of agents has a common resource that is evenly divided among all participants of the game. Each agent can choose to deposit their own resources (points) into the collective resource pool (”the pool”). The more points that has been ”given away” to the collective, the more points will everyone have. In this game, we assume that the number of points in the pool is multiplied by a constant at the end of every turn.

Rules:

1. Each agent begins with 2 points.
2. We do not know how many other agents there are playing the game. No agent knows how many points any other agent has given to the pool. ”An agent only know how many points that was received from the pool the previous turn.”
3. At each turn, every agent can make a choice of how many points should be given away to the pool.
4. The game continues forever. (Alternatively, for a large but uncertain amount of turns.)

Points:

1. The number of points in the pool is multiplied by 1.1 and is then evenly distributed among all the participants at the end of every turn (it is possible to receive fractions of points from the pool). Points earned from the pool can be used the next turn.
2. The number of points that was not given away to the pool are saved to the next turn.

Goals of the game:

1. Greedy agents wish to gain more points than the everyone else. The winning strategy is to never give away points.
2. Non-greedy agents with to gain the most points possible. The winning strategy is to give away at least one point at the first turn, and then keep giving away the same amount of points that one just received from the pool. The average number of points the cooperating agents are willing to give away at the first turn will determine how quickly the collective resources approach infinity, if at all.

Corporations are bound by law to seek to increase their stock value. Stock value is their ”relative” value in comparison with other actors of the market. (The reader is invited to think by itself here: How can greedy agents come to influence the systems overall behavior? How can we overcome this problem? Is there any effective solution to this problem?)

2.2 Intermezzo: Cypherpunk and meta-ideology

RFC2810, *Internet Relay Chat: Architecture*, is a proposal (or *Request For Comments*) that defines how IRC servers can cooperate to create real-time communication systems. IRC is one of the oldest forms of direct chat protocols created for the internets and was indeed somewhat of a successor of a protocol for BBS chat. The BBS was typically a computer without internet, people had to phone them with their modems over the Public Telephone Network System. IRC was created 1988, two years before the first web page was created, and three years before the fall of the Soviet Union. In RFC2810 there is a ASCII picture of how an IRC network can look like.

```
3. Architecture

   An IRC network is defined by a group of servers connected to each
   other.  A single server forms the simplest IRC network.

   The only network configuration allowed for IRC servers is that of
   a spanning tree where each server acts as a central node for the rest
   of the network it sees.

                       1--\
                           A        D---4
                       2--/ \      /
                             B----C
                            /      \
                           3        E

   Servers: A, B, C, D, E         Clients: 1, 2, 3, 4

                    [ Fig. 1. Sample small IRC network ]

   The IRC protocol provides no mean for two clients to directly
   communicate.  All communication between clients is relayed by the
   server(s).
```

The IRC network organize itself in a tree structure. If cyclic groups appear, such as if D would connect to B, routing of messages becomes difficult. This is a protocol that requires the IRC servers to organize in somewhat star-shaped topologies. This makes it vulnerable to denial of service attacks, or just ordinary failures. While the network is distributed, it is not decentralized. In essence, it kind of reminds us of how the soviet computer network, or the Chilean cybersyn was organized.

Cyberpunk

Cyberpunk was invented by Bruce Bethke in 1983 and later more-or-less turned into its own literary genre by William Gibson. Lone uberhackers lurk the corporate matrix, independently hacking into their mainframes at nights. During the day the cyberpunk either sleep, or lives a miserably life. This literary genre has shaped how media write about hackers. In some sense, it is not possible to be a hacker without at least being associated with the invented cyberpunk lifestyle. But that is besides the point.

The word cyberpunk obviously comes from cybernetics, and punk. Cybernetics is an idea of how one can create complex regulatory systems. It utilizes centralized control, feedback and loopback mechanism from censors. The central nodes in a cybernetic system requires that the sub-nodes *below itself* in the chain of command reports information back *up to the central command*. The IRC network is a typical cyberpunk system. IRC is used by hackers (or at least: this is how the media describes it) to organize attacks against the corporate mainframes. In some few cases, this is true. The informal network of Anonymous – currently armed with Low Orbit Ion Cannons (LOIC, a DDoS-software) – frequently target the corporate "websites." Mainframes are out of their reach.

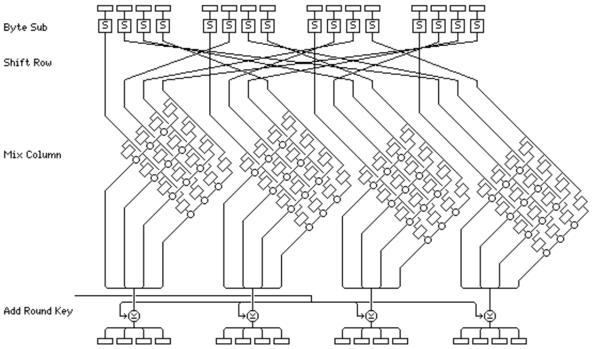


Figure 2.2: The AES cipher. Or at least parts of it: It is one of the 10, 12 or 14 rounds (depending on key size). This algorithm is widely used almost everywhere today. Unlike its predecessor DES it was not developed by the NSA/IBM. Perhaps the reason is that they do not wish to show the world how far ahead (or behind) they are in the research of ciphers. When they modified the Lucifer-cipher to become DES they made strange changes in the cipher that was not explained. Many thought that NSA had built a backdoor into DES, but it turned out that they had actually made it secure against differential cryptanalysis. In 1994 differential cryptanalysis was discovered by independent researchers not tied to military-industrial complex, almost 25 years after the creation of DES.

Cypherpunk

Cypherpunk stands in stark but subtle contrast to cyberpunk. Cypherpunk is a word that seems to first have appeared in the Chaum Mix-mailserver networks. It is of course a play on the word cyberpunk, where cybernetics has been replaced with *cypher*, another word for cryptography. The function of a cypher is to render information unreadable to anyone that does not have the right cipher-key or passphrase. Cypherpunk did not emerge as a romantic literary genre, instead it emerged when public key cryptography was first explored in 1980-

1990[1]. As the programmers discovered the algorithms that made inspection nearly impossible they began to dream of systems that *could not* have leaders. The main idea of cypherpunk is not the creation of hierarchal computer systems, but *the creation of systems where inspection of subsystems is impossible.*

This means that cypherpunks must deal with the art of creating systems which are independent of its subsystems, as the inspection of the function of a subsystem is not possible. Every subsystem is a cyphernetic black box. The first generations of cypherpunk software relied on groups of servers for relaying encrypted e-mail. A user of the system would select a some of the mailservers at random and encrypt their e-mails with *all* the servers public keys. The mail would then be forwarded between the mailservers, where one cipher after another would be removed from the e-mail, until it was fully deciphered. Once deciphered, the mail could be sent to a mailing list. If private conversation was required, the e-mail could be encrypted with the intended receivers public key. As long as not ”all” the mailservers were owned by the same person, or the owners does not conspire to track the users, its safe to use.

The early dreams of cypherpunks was further expanded with protocols for anonymous banks, which allowed cypherpunks to exchange money without having to pay taxes. A small series of protocols that reinvented the old societies in their cyphernetic forms were created. In the eyes of the first cypherpunks, their systems enabled them to build the perfect anarcho-capitalist worlds inside the computers. Unfortunately for the cypherpunks back in the early 90ies, almost no one understood what they were doing since most ordinary people either did not own any computers, or just played games with them.

The world has since then changed. Today almost everyone owns computer(s) and it does not require any exceptionally educated person to use them. The anonymous banks seems to have difficulties in gaining customers, partly perhaps because it is considered impossible to trust an anonymous stranger with all the money. Alternative decentralized payment systems that does not rely on any single node has emerged and is now being experimented with. BitCoin is one example where agents voluntary engage in agreements of debt directly between each other (in so doing, they create bitcoin currency. No central bank is needed for this.) If agent A owes agent B for something that B created, this debt can be given away to other agents. Since its voluntary and relies on direct trust between agents no banks are required for anonymous money to exist. If anonymous money feels weird, consider that modern money is nothing but numbers inside the corporate mainframes. Going one step further and having the money in your own computer is not impossible.

Crypto-anarchy: The meta-ideology that enables cypherpunk?

If there is a distinction between cypherpunk and crypto-anarchism, it lies in the level of abstraction. Crypto-anarchism as such does not deal with money, but the creation of censor-free, decentralized and distributed information infrastructures. This infrastructure can of course be used for *any form of communication.* The cypherpunk systems are a layer of software and trust

[1] Jude Milhon coined the word. When interviewed by the magazine Wired they only asked her about feminism and why she was a girl who liked computers. Little is know of this woman, as it seems that almost noone cared about the important stuff – like the ideology rather than her sex.

built on top of the crypto-anarchist infrastructure. Other forms of ”decentralized societies”[2] can of course be built. Crypto-anarchism does not deal with ideologies such as cypherpunk, instead it is a meta-ideology or non-ideology that enables secure implementations of ***all*** authority-free ideologies. As our world grows more technically enhanced, the potential for crypto-anarchism grows.

The first generations of crypto-anarchist systems used a few servers to relay their e-mails. While this makes anonymity possible, such systems were slow and were difficult for most humans to use. The old systems did not scale very well either, simply because they were not fully decentralized. It is a bit difficult to create systems that neither relies on a central command nor knows anything about the subsystems that constitutes it.

It is however possible.

2.3 Achieving emergent decentralization and distribution

Wikipedias definition of an emergent algorithm is that it has the following characteristics:

1. it achieves predictable global effects
2. it does not require global visibility
3. it does not assume any kind of centralized control
4. it is self-stabilizing

A *distributed algorithm* is a word that is sometimes used to mean a *communication protocol.* A distributed hash table (DHT) is a distributed algorithm that decentralize the function of finding a particular agent as well as information stored among the agents.

An ordinary hash table is a data structure that can be used to find stored information within a computer. The amortized time-complexity of a hash table is $O(1)$, meaning that it is as efficient as anything can possibly become. It is often the optimal data structure to store huge amounts of data, but it turns out that its pretty worthless for storing smaller amounts. A DHT is a data structure that is distributed among several computers, and it turns out that most DHTs has complexities of $O(Log(n))$, where n is the number of nodes in the network.

Since it is a form of distributed database, it requires a distributed algorithm to function. This algorithm can not rely on any central nodes for guidance, since the whole point of the DHT is to be a completely scalable and decentralized structure. One distributed hash table that is of particular interest is Kademlia. The reason is that Kademlia is simple and possible to prove to have a complexity of $O(Log(n))$.

[2] Is this an oxymoron?

Chapter 3

Cipherspace

Stater, företag och organisationer både övervakar och avlyssnar människors kommunikationer. All kommunikation är ännu inte övervakad, passerar datapaketen inte över Sveriges gränser finns bara en ytterst liten risk att övervakas av buggletande nätverkstekniker. Passerar information över landsgränsen riskerar man däremot att bli både övervakad och avlyssnad av Försvarets Radioanstalt, FRA. Efter valet i augusti 2010 riskerar också paket som verkar innehålla IP-telefoni eller vanlig telefoni att övervakas och sparas i enlighet med datalagringsdirektivet, om det implementeras i Sverige. Längre in i framtiden hägrar fler lagar som kan komma att innebära utökad kontroll av vår kommunikation. Om ACTA[1] antas av EU efter ett beslut i parlamentet kommer Sverige och övriga medlemsnationer att erläggas ansvar att stifta lagar som bland annat riskerar att nätleverantörer blir ansvariga för vad deras kunder kommunicerar över nätverken[2]. I en sådan situation kommer nätleverantörerna att behöva övervaka all kommunikation som sker över deras nätverk om de ska klara sig undan skadeståndskrav från upphovsrättshavare. I ett annat dokument som nyligen publicerades[3] av MPAA[4] och RIAA[5], förespråkas införandet av bland annat filter som automatiskt upptäcker intrång i upphovsrätten i nätverk nära konsumenterna.

Sverige har förmodligen[6] varit relativt skonat från övervakning av datornätverk i jämförelse med exempelvis Iran, England, USA, Italien, Kina och Frankrike. Tidigare i historien har

[1] Anti-Counterfeit Trade Agreement. En öppen version finns publicerad på `http://trade.ec.europa.eu/doclib/docs/2010/april/tradoc_146029.pdf`. Dokumentet finns speglat på `http://cryptoanarchy.org/files/ACTA-first-public.pdf`

[2] Bland annat Electronic Frontier Foundation och Johan Folin på Kvällsposten drar den här slutsatsen. Se `http://www.eff.org/deeplinks/2010/04/eff-analysis-officially-released-acta-text` och `http://kvp.expressen.se/ledare/1.1960710/johan-folin-en-vat-drom-for-skivindustrin`.

[3] `http://www.eff.org/deeplinks/2010/04/entertainment-industrys-dystopia-future`

[4] Motion Picture Association of America

[5] Recording Industry Association of America

[6] Enligt SVT Rapport har FRA dock övervakat och avlyssnat svenskar i stor skala redan innan FRA-lagen trädde i kraft. Se `http://svt.se/svt/jsp/Crosslink.jsp?d=22620&a=1175152&lid=puff_1175195&lpos=rubrik`. Ett av argumenten att införa FRA-lagen (2008:717) var att *begränsa* FRAs möjligheter att övervaka nättrafik. Hurvida vi faktiskt har varit skonade från övervakning går därför att diskutera.

övervakningen skett mest mot de som varit utpekade som misstänkta. Idag används övervakning i stor skala även mot individer som auktoriteter helt säkert vet är oskyldiga.

Vad alla former av ingrepp som listas ovan har gemensamt är att de är möjliga att genomföra för att utrustningen som de enskillda individerna äger och använder sig av går att spåra till nätadresser, platser, användarkonton och i slutändan deras namn och adress. De tekniska framsteg som har gjort övervakning möjlig beror på att användarna tillåter ägarna av den digitala infrastrukturen att läsa innehållet i deras kommunikation. Allt skickas i klartext[7], från sändare till mottagare.

En form av nätaktivism strävar efter att förändra detta genom att med enbart tekniska medel införa ett tillstånd som kan kallas *kryptoanarki*. Den här texten handlar om vad kryptoanarki är, dess historia, vilka motiv som driver kryptoanarkister, vilka hinder kryptoanarkin står inför samt vilka förändringar som en kryptoanarki kan innebära.

3.1 En sammanfattning av kryptoanarki

De maskiner som utgör det kommunikationsmedium vi kallar för internet består nästan uteslutande av olika implementationer av turingmaskiner med begränsade lagringskapaciteter[8]. En turingmaskin är ett objekt som behandlar symboler efter en bestämd mängd regler. Ofta används turingmaskiner för att beskriva datorer.

All information som går att spara i digitala arkiv och all information som skickas över nätverken består av symbolsekvenser: En bit kan ha två tillstånd. En 8 bit lång sekvens, en byte, kan ha 256 olika tillstånd och en hårddisk kan ha väldig många fler tillstånd. Datorer är precis som de teoretiska turingmaskinerna speciellt tillverkade för att hantera dessa symbolsekvenser. Data och information i våra datorer och datornätverk är ingenting annat än symbolsekvenser. Ibland representeras symbolerna som siffror. Ibland som bilder, filmer eller ikoner förutsatt att rätt codecs[9] finns tillgängliga. Alla upphovsrättsskyddade filmer, alla texter som beskriver hur man tillverkar bomber och all pornografi på internet sparas och behandlas i datorer som symbolsträngar.

Det är enbart när människor lyckas lägga värde eller innebörd i de symboler som utväxlas mellan datorer som meningsfulla handlingar – så som exempelvis ett upphovsrättsintrång eller försändelsen av ett kärleksbrev – kan sägas ha utförts. Om data som utväxlas mellan maskiner i nätverken inte går att tolka[10] går det inte heller att med trovärdighet påstå att någon speciell handling har utförts. Om det aldrig går att upptäcka att någon olaglig information har spridits mellan några specifika individer kan heller inga lagar som förbjuder människor från att sprida viss information verka.

[7] Klartext är ett begrepp som först får mening när det ställs mot chiffertext. Chiffertext går inte att läsa om man inte har tillgång till de kryptonycklar som använts. Klartext å andra sidan består av okrypterade meddelanden som är triviala att läsa.

[8] En turingmaskiner är egentligen en teoretisk konstruktion med en oändlig lagringskapacitet.

[9] En codec är ett program som avkodar eller kodar data.

[10] Förhållandet mellan data och information är viktigt. Data blir meningsfull information först efter att det har tolkats.

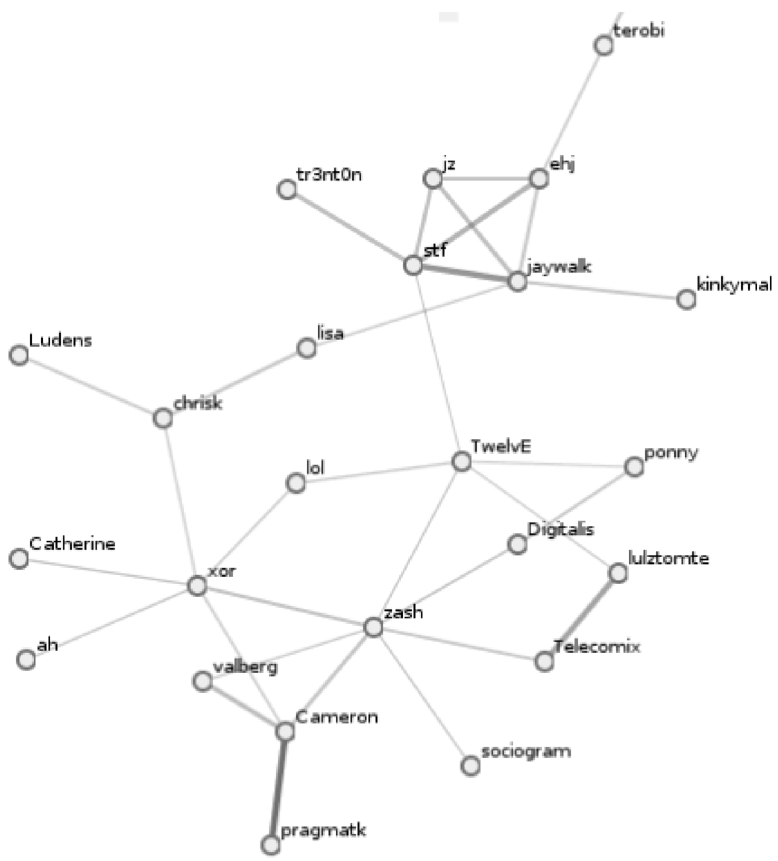


Figure 3.1: Ett sociogram över en IRC-kanal. Noderna i grafen består av pseudonymer för människor och datorprogram som kommunicerar med varandra. Bågarna mellan noderna representerar hur ofta referenser har gjorts: Vem som har tilltalat vem. Desto tjockare bågar, desto fler referenser har förekommit. Tre av noderna, *telecomix*, *lol* och *sociogram*, representerar bara ord. Bågar till dessa tre noder representerar hur ofta de orden har använts. Sociogrammet har alltså tillförts ytterligare information som har kunnat skapas genom att avlyssna IRC-kanalen. Diagrammet uppdateras i realtid på `http://pochwa.ath.cx/telecomix/Catherine.png`

Modern kryptografi arbetar likt datorer över finita fält. Det enda som i praktiken kan hantera modern kryptografi är också moderna datorer. Kryptografi kan sägsas vara konsten att förvandla meingsfull data (information) till data som enbart med stor möda går att tolka. Meddelanden krypterade med moderna krypton går i praktiken inte att forcera. Trots att själva meddelandet är skyddat från att kunna tolkas skyddar inte kryptering mot övervakning. Sociogram (se figur 3.1) över vem som kommunicerar med vem går fortfarande att upprätta. Kunskapen om hur individer kommunicerar med varandra ger information om vilken typ av information som de förmedlar mellan varandra och kunskapen att individer kommunicerar med krypterade meddelanden är i sig intressant. Kryptering utgör därför inte ett fullgott skydd mot övervakning trots att det skyddar mot avlyssning. Först när kryptering kombineras med routingprotokoll[11] speciellt designade för att inte avslöja vem som kommunicerar med vem, så att det inte går att tillverka sociogram, uppstår *tillståndet* kryptoanarki:

När det inte går att avgöra vem som kommunicerar med vem och vilken information som skickas mellan individers datorer, går det inte att upprätthålla några lagar som begränsar vilka informationsflöden som får existera. Trots att det går att upptäcka att datorer sänder krypterade meddelanden till varandra går det inte att utröna vad som verkligen döljer sig i kommunikationsflödet. Det enda som med säkerhet går att avgöra är att en grupp datorer kommunicerar krypterade meddelanden med varandra, samt vilka datorer som ingår i den gruppen.

En kryptoanarki går att upprätta enbart genom att tillverka de program som krävs för att routa krypterade meddelanden mellan datorer. Genom att neka utomstående möjlighet att läsa vilken typ av information som döljer sig i de symbolsträngar som hanteras av datorer kan ett rum, som kan kallas för *cipherspace*, skapas där enbart de matematiska lagar som begränsar informationsbehandling[12] gäller. Det som i teorin krävs för att upprätta en kryptoanarki är mjukvara som med hjälp av krypton utnytjar skillnaden mellan data och information, samt nätverksprotokoll för att göra sociogram svåra att upprätta. I praktiken kan dock andra faktorer vara intressanta.

3.2 Kryptoanarki i praktik

1981 föreslog David Chaum ett protokoll för att skicka anonym e-post. Chaum Mixes[13] som protokollen kallas för, döljer både innehållet i meddelanden som skickas samt vem som skickade meddelandet. Kryptografi används för att dölja innehållet i meddelanden och slumpvisa färdvägar utvalda och enbart kända av användarnas klientmjukvara används för att dölja vem avsändaren är. Om den tilltänkta mottagaren tidigare har använt samma anonymiserande e-postsystem för att skicka ett meddelande till mailinglistan, innehållande sin publika kryptonyckel[14], så kan också mottagaren göras anonym. Ingen annan än mottagaren kan avläsa infor-

[11] Routingprotokoll är beskrivningar för hur datorer ska skicka datapaket mellan varandra. Ett exempel är RIPv2 som defineras i RFC2453. `http://tools.ietf.org/html/rfc2453`

[12] Komplexitetsteori är ett fält inom datorvetenskap och matematik som användas för att beskriva de begränsningar turingmaskiner har. Med sinnrikt konstruerade algoritmer kan tillgång till information nekas eller ges för att uppnå specilla mål. Komplexitetsteori är av samma anledning viktigt vid tillverkningen av protokoll som behöver motstå attacker med syfte att förbruka datorers resurser, en form av Denial of Service-attack. Exempel på algoritmer som är speciellt framtagna för att undvika komplexitetsattacker mot processorer är Just Fast Keying (JFK). En av de två varianterna av JFK används av Freenet. För mer information om JFK, se `http://www.cs.tau.ac.il/~canetti/materials/jfk.pdf`

[13] Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, David Chaum, Communications of the ACM, February 1981, Volume 24, Number 2. Nåbar via `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.8210&rep=rep1&type=pdf`. För en analys av säkerheten som presenteras av Chaum Mixes, se On the Anonymity of Chaum Mixes, Parvathinathan Venkitasubramaniam, Venkat Anantharam. Electrical and Computer Engineering, Cornell University och University of California, Berkeley. Nåbar via `http://www.eecs.berkeley.edu/~ananth/2008+/04595043_Parv.pdf`

[14] Asymmetriska kryptoalgoritmer så som RSA och ElGammal ger användare tillgång till två typer av kryptonycklar. En publik kryptonyckel och en privat. Meddelanden krypterade med den publika kryptonyckeln går inte att dekryptera utan att man innehar den privata kryptonyckeln. Digitala signa-

mation kodad i de brev som skickas till den publika maillistan, om det har krypterats med den publika nyckeln. Andra metoder[15] för att dölja både avsändarens och mottagarens identitet[16] existerar också. Chaum Mixes och de protokoll som senare byggde vidare på konceptet är tillverkade med syftet att både dölja innehållet i meddelanden som skickas och vem som kommunicerar med vem.

Sedan 80-talet har fler protokoll skapats som har varit mer eller mindre resistanta mot övervakning. Onion routing är ett sådant protokoll som U.S. Naval Research Laboratory[17] utforskade när de först tillverkade The Onion Router[18], TOR. Onion Routing fungerar till stor del på samma sätt som Chaum Mixes, men tillåter kommunikation i *realtid*. Problemet med realtidskommunikation är att det är enklare att överblicka än de e-postmeddelanden som först användes. Ett e-brev ska enligt Chaums protokoll sparas på servrarna under slumpvisa intervall innan de skickas vidare, vilket gör att det blir mycket svårare att avgöra vem som kommunicerar med vem. Realtidskommunikation däremot tillåter inte att långa slumpvisa fördröjninga introduceras i nätverkets noder. Detta utgör ett problem eftersom en överblick av hela nätverket över en tid gör det möjligt att gissa sig till vilka som kommunicerar med vilka, bara genom att observera hur stora datamängder som skickas mellan alla noder i nätverket. En säkrare variant av Onion Routing är Garlic Routing, som används av programmet I2P[19]. Garlic Routing använder många fler tunnlar än Onion Routing för att parallellt överföra information via många vägar mot slutpunkten i nätverket, vilket gör det svårare att hitta vem som kommunicerar med vem. Andra tekniker, som att introducera fejkade dataflöden eller väldigt korta slumpvisa fördröjningar i kommunikationsflöden finns också.

3.2.1 Decentralisering som medel för försvar

Förutom övervakning och avlyssning finns andra hot mot användare som försöker dölja sin kommunikation. Regimer, myndigheter och hackare kan neka användare tillgång till de anonymiserande nätverken om det finns cenrala noder som går att attackera. Denial of Service-attacker mot centrala noder eller hot riktade mot viktiga programmerare kan användas för att sabbotera nätverken eller för att introducera skadlig kod. Vissa av de program som finns idag har utveck-

turer, certifikat, går också att tillverka genom att vända på processen. Meddelanden krypterade med den privata nyckeln går då enbart att dekryptera om den publika nyckeln innehas. På så sätt går det att verifiera identiteter som är mycket svåra att förfalska. Oftast publiceras den publika nyckeln, medan den privata hålls gömd. Skapandet av ett nyckelpar motsvarar i det kryptoanarkistiska rummet (cipherspace) skapandet av en ny pseudonym identitet.

[15] Reply Onions och rendevouz points är exempel. Se Design and Analysis of an Anonymous Communication Channel for the Free Haven Project, Michael J Freedman, Department of Electrical Engineering and Computer Science. Nåbar via `http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.26.8778&rep=rep1&type=pdf`

[16] Med identitet menas här deras namn, adress eller IPv4-adress. Ett nyckelpar i ett asymmetriskt krypto kallas ibland också för en identitet. I datornätverk så som Chaum Mixes kan användarnas identiteter ersättas med dessa nyckelpar. Den anonymitet som det talas om är med andra ord egentligen en form av pseudonymitet.

[17] `http://www.wired.com/politics/security/news/2005/05/67542`

[18] Electronic Frontier Foundation tog sedan över utvecklandet av mjukvaran. Det går att läsa mer om TOR samt ladda ner programmet från `http://torproject.org`.

[19] Precis som TOR har I2P en websida nåbar via det vanliga internet. `http://i2p2.de`.

lats för att överleva sådana attacker. Programmet I2P utgör ett bra exempel på detta eftersom dess nätverk är helt decentraliserat. I2P använder ett protokoll, Kademlia[20], vilket gör att noder i nätverket inte behöver förlita sig på några centrala servrar. Kademlia är en typ av distruberad hashtabell, en sorts databas som kan användas för att hitta andra noder i nätverket. Kademlia har egenskaper som gör att väldigt många noder kan försvinna innan informationen i databasen inte längre går att nå. På så sätt klarar nätverket av att stora delar av det attackeras.[21] Vem eller vilka som döljer sig bakom pseudonymet *jrandom*, den första programmeraren av I2P, är heller inte känt[22]. Många av de programmerare som har tagit över projektet sedan jrandom försvann är bara kända som sina pseudonym och de publika kryptonycklar som används för att garantera att mjukvaran kommer från tillförlitliga källor.[23]

3.2.2 Motiv till att upprätta en kryptoanarki

Anarkokapitalistiska banker både existerar och har existerat i de anonymiserande nätverken. En av de mest långlivade bankerna hette Yodelbank[24]. Via omvägar förbi Digital Monetary Trust, E-gold, Pecunix och andra banker eller betalningsformer som var nåbara via internet och som inte krävde att några personliga uppgifter om ägare kunde pengar flyttas över till Yodelbanks anonyma konto. När pengarna väl var överförda till banken erhöll personen som flyttat över pengarna ett certifikat som kunde användas för att programmera banken till att flytta pengar till bankkonton i de banker som Yodelbank kunde interagera med. På så sätt motsvarade certifikaten pengar. Via bankens interface kunde man dela upp certifikat i flera mindre certifikat eller slå samman certifikat. De gamla certifikaten förlorade då sitt värde samtidigt som de nya associerades med värdet som de tidigare certifikaten motsvarade. Genom att utväxla certifikat med andra användare och sedan via Yodelbank växla certifikaten mot nya kunde pengar flyttas mellan anonyma användare. Ägaren av Yodelbank är fortfarande okänd och banken opererade obunden av nationella lagar. Flera andra mer kortlivade banker har existerat och vid tillfället då den här texten skrivs är Torbank på väg att öppna upp. Torbank är nåbar via TOR- och I2P-nätverken.[25]

Jim Bell publicerade under 1995 till 1996 en serie brev där han beskriver Assassination Politics[26]. Han förespråkade en lönnmordsmarknad baserad på anonyma betalningsmedel, där alla

[20] Kademlia: A Peer-to-peer Information System Based on the XOR Metric, Petar Maymounkov and David Mazières, New York University. Nåbar via `http://pdos.csail.mit.edu/~petar/papers/maymounkov-kademlia-lncs.pdf`

[21] TOR har inte det här skyddet eftersom TOR använder sig av ett fåtal directory servers. Dessa centrala servrar har samma uppgift som I2Ps implementation av Kademlia.

[22] Det sista meddelandet jrandom lämnade går att läsa på I2Ps officiella websida. `http://www.i2p2.de/jrandom-awol.html`

[23] Programmet I2P kan uppgradera sin mjukvara när nya versioner publiceras innuti I2Ps nätverk. Mjukvaran uppgraderas enbart när de nya versionerna har blivit signerade med en nyckel som är tillförlitlig.

[24] Yodelbank diskuteras i en intervju i appendix **??**. Yodelbanks websida finns arkiverad på `http://web.archive.org/web/20050315093618/http://yodelbank.com/`.

[25] Torbank går att nå via `http://torbank.i2p` eller `http://torbankofpucsfo6.onion`. För läsare som inte har tillgång till egna I2P- eller TOR-proxies går det att nå sidan via `http://tinyurl.com/torbank4`.

[26] `http://www.outpost-of-freedom.com/JimBellAP.htm`

inblandade parter är anonyma. Enligt Jim Bell skulle marknaden skötas av en organisation som namnger politiker, makthavare och tjuvar som användarna av anonyma banker kunde lägga pengar på. Den som mördade någon av dessa personer vid ett tidigare angivet tillfälle[27] kunde sedan ta ut pengarna. Syftet var att skapa ett tillstånd av minarki eller anarki, där ingen vågar begå brott. Tidningen Wired har sedan publikationerna av breven skrivit flera artiklar[28] om Jim Bell och de problem han efteråt fick med FBI och IRS[29].

I en intervju med en anonym kryptoanarkist[30] anges motiv så som att motverka myndigheters möjligheter att tysta mediaflöden, samt att ingen myndighet eller person har rätt att bestämma hur andra ska kommunicera med varandra, eller vad som får sägas. I en annan intervju[31] med en person som inte utger sig för att vara kryptoanarkist, men ändå använder nätverken, ges anledningen att på ett säkert sätt kunna bryta mot copyright och patentlagar. Andra anledningar som ges är att kunna diskutera med andra som har liknande tankar och åsikter; *For me, using i2p is about geekiness and being able to express sides of myself that's not easy to express elsewhere.*

```
< xor> why is it needed?
* xor imagens that there are other motivation than anarcho-capitalism
      and assassination markets
<+lulzifer> xor: because I believe free communications will liberate
            people from oppression
<+lulzifer> or at least make certain liberation easier
<+eche|on> needed as other nets are neither free nor uncensored
<+lulzifer> yes
< xor> :)
<+lulzifer> i dont think everybody needs it all the time, but it
            should always be an option
<+lulzifer> human society will endure better if information is free
<+eche|on> nets as I2P let you talk/publish free without the fear of
           LEA or any other agency (look to china or israel currently)
```

Motiven att upprätta en kryptoanarki skiljer sig alltså beroende på vem man frågar. Det är möjligt att det inte finns en koherent kryptoanarkistisk ideologi.

[27] Jim Bell föreslår att tidsangivelsen krypteras för att undvika att läcka information som kan hjälpa offret att skydda sig från attacker. Först efter dådet ges organisationen som tillhandahåller tjänsten tillgång till kryptonyckeln.

[28] http://www.wired.com/politics/law/news/2000/04/35620, http://www.wired.com/politics/law/news/2001/06/44567 och http://www.wired.com/politics/law/news/2001/12/48779

[29] Internal Revenue Service, motsvarande skatteverket.

[30] Se appendix **??**

[31] Se appendix **??**

3.3 Vad kan hindra en kryptoanarki?

3.3.1 Nätneutralitet

Internet består idag av en grupp nätverk där vem som helst kan kommunicera med vem som helst. Nätneutralitet kan defineras som att alla noder som deltar i nätverken har lika stora möjligheter att kommunicera med varandra.

Det finns begränsningar i vår kommunikationsfrihet, bland annat i form av den kinesiska brandväggen, ”The Golden Shield”. Tekniska begränsningar som i maj 1994 introducerades i det grundläggande protokollet IPv4 innebar att internet gick från att vara ett nät där alla datorer alltid har en publikt nåbar adress, till ett nät där nätverk av datorer delar på en publikt nåbar adress[32].

Vad som däremot kan utgöra problem är om företag köper upp nätverken för att ge sig själva tillgång till en större del av bandbredden. Detta har bland annat skett mellan nätleverantören Telia och mediatjänsten Spotify[33]. I fallet Telia och Spotify begränsades bandbredden till 120 kbit/s efter att kunden använt mer än 0.5 GB per månad. Undantaget var Spotify, som kunde strömma musik obehindrat av begränsningen. Det har gjort liknelser[34] mellan avskaffandet av nätneutralitet och införandet av ett internet som mer liknar kabel-TV. Det finns olika grader av nätneutralitet, allt från att trafikprioritera[35] SSH-anslutningar för att exempelvis kunna logga in på överbelastade servrar till att användare av nätverken enbart kan nå ett fåtal utvalda tjänster.

I en diskussion med socialdemokraten Leif Pagrotsky[36] menade Pagrotsky att fildelning var död. I stället skulle tjänster som Spotify ta över för att det helt enkelt var enklare att ta till sig musik via deras centrala servrar, än att man själv stal musik via The Pirate Bay. Enligt Pagrotsky krävdes det inga lagar för att jaga fildelande ungdommar eftersom det går att bygga bort problemet. Resonemanget går att utvidga till många andra tjänster som Youtube, Grooveshark och så vidare. En spotifiering[37] av internet kräver att företagen som tillhandahåller tjänsterna köper in sig i nätverken som ligger nära användarna och på så sätt ges möjlighet att strömma film och musik till konsumenter effektivt. Eftersom deras tjänster är enklare att använda än att användarna själva väntar på att filer har hämtats ner kommer Spotify och liknande företag

[32] Teknologin kallas för NAT, Network Address Translation, och definerades först i RFC1631. Se `http://www.faqs.org/rfcs/rfc1631.html` för mer information.

[33] `http://www.dn.se/ekonomi/spotify-och-telia-tecknar-avtal-1.969800`. Telia backade sedan `http://www.idg.se/17.108/2.1085/1.273279/telia-spotify-far-ingen-graddfil`.

[34] Se exempelvis `http://christopherkullenberg.se/?p=1227`, `http://tusenpekpinnar.wordpress.com/2009/11/24/telia-vill-avskaffa-det-fria-internet/` och `http://blogg.aftonbladet.se/lisamagnusson/2009/11/natneutralitet-sa-funkar-det`.

[35] Exempel på hur trafikprioritering kan genomföras i backbone-nät beskrivs i RFC2702. RFC2549 beskriver hur olika djur kan användas för att bära information olika effektivt mellan domäner. Se `http://www.faqs.org/rfcs/rfc2702.html` och `http://www.faqs.org/rfcs/rfc2549.html`.

[36] Ingen annan referens finns än författaren själv. `http://sosse.tv` bevisar dock att författaren har trollat socialdemokraternas kongress.

[37] Spotifiering kan definerats som att man tar något som är gratis och sedan säljer det. Uttrycket går att använda på många saker. Bland annat spotifiering av smörgåsar: `http://fredrikedin.wordpress.com/2010/01/09/spotifieringen-av-smorgasar/`

att ta över, enligt Pagrotsky. På så sätt upphör den illegala fildelningen. En spotifiering av internet kan alltså vara önskvärd.

Ett scenario där det inte går att kommunicera med några andra noder än ett fåtal utvalda utgör ett uppenbart problem om man önskar en kryptoanarki. Protokoll som används för att koordinera nätverk, så som Kademlia, fungerar dock även då bara mycket liten bandbredd finns att tillgå[38]. Eftersom antalet andra noder som varje node behöver ha regelbunden kommunikation med i fallet Kademlia är absolut minst $O(\log(n))$, där n är antalet noder i nätverket[39], begränsas nätverkets storlek ytterst av bandbredd. Avsaknad av nätneutralitet kan därför utgöra ett problem för stora decentraliserade nätverk.

3.3.2 Säkra kryptoprocessorer

En säker kryptoprocessor (eng. *secure cryptoprocessor*) är hårdvara som är tillverkad för att hantera chiffer och är avsedda att skapa tillförlit till att datorsystem är säkra. Innuti processorn finns ofta ett lagringsutrymme där kryptonycklar kan sparas samt kretsar för att generera nya nycklar, slumptal och för att kunna utfröra de beräkningar som behövs. Vissa implementeringar har skydd mot intrång som utlöser självförstörelsemekanismer. Ett exempel på en säker kryptoprocessor är IBM 4758[40]. För exempel på hur en sådan processor och de protokoll som används kan fungera se [41].

En grupp som presenterar specifikationer för en säkra kryptoprocessor till bland annat PC-datorer är Trusted Computing Group[42] (TCG). TCG har tagit fram bland annat två tekniker som de kallar för Trusted Computing (TC) och Trusted Network Connect (TNC)[43]. TPM-kretsar finns idag installerade i många datorer[44] och presenteras ibland som en ny form av säker kryptering[45].

[38] För en studie i detta, se Structured and unstructured overlays under the microscope – A measurement-based view of two P2P systems that people use, Yi Qiao and Fabián E. Bustamante, Department of Electrical Engineering & Computer Science, Northwestern University. Nåbar via `http://www.aqualab.cs.northwestern.edu/publications/YQiao06SUO.html`.

[39] I komplexitetsteori är basen för logaritmen i de flesta fall inte relevant. Ofta kan man dock anta att basen är 2. Det skulle i så fall innebära att ett nätverk med 32 noder behöver varje node hålla koll på $log_2(32) = 5$ andra noder. I ett nätverk med strax över en miljard noder behövs att varje node håller reda på ungefär 30 andra noder.

[40] `http://www-03.ibm.com/security/cryptocards/pcicc/faqcopvalidity.shtml`

[41] Crypto Processor for Contactless Smart Cards, G. Selimis, N. Sklavos and O.Koufopavlou, University of Patras / Department of Electrical and Computer Engineering, Patras, Greece. Nåbar via `http://www.vlsi.ee.upatras.gr/~gselimis/papers/2004/melecon2004.pdf`

[42] Deras websida är `http://www.trustedcomputinggroup.org`

[43] För en beskrivning av vad TNC kan användas till, se TCG Trusted Network Connect, Federated TNC Specification Version 1.0, Revision 26, Sektion 2. Dokumentet är nåbart via `http://www.trustedcomputinggroup.org/files/resource_files/51F4B514-1D09-3519-ADEF8EA701461A74/TNC_Federated_TNC_v1.0-r26.pdf`

[44] Se exempelvis `http://www.wave.com/products/DellTPM_Matrix.asp` för vilka Dell-datorer som har TPM-kretsar.

[45] `http://www.infoworld.com/d/security-central/your-laptop-data-not-safe-so-fix-it-553`

Vilka möjligheter ger TPM-kretsen?

Trusted Platform Module ger följande möjligheter.[46]

- **Chain of Trust** – Säkerställer att mjukvaran på datorn inte går att förändra utan tillstånd.
- **Secure IO** – Enbart kretsar som har korrekta signaturer får lov att kommunicera högupplöst ljud och video med TPM-kretsen.
- **Protected memory** – RAM-minne kan krypteras av TPM-kretsen. Enbart betrodda program får lov att läsa innehållet i minnet.
- **Secure Attestation** – TPM-kretsen kan användas för att verifiera kretsens identitet samt att datorn använder speciell mjukvara.
- **Sealed storage** – TPM-kretsen kan arbeta tillsammans med masslagringsmedia för att kryptera innehåll som sparas.

Centralt för säkerheten för TPM är att kretsarna skickas till kunderna med kryptonycklar som inte går att byta ut[47]. Eftersom TPM-kretsar kommer med ett asymmetriskt nyckelpar, Endorsement Key (EK), som åt minstonde tillverkarna av kretsarna vid något tillfälle måste ha känt till betyder det också att tillverkarna av kretsarna kan dekryptera allt som TPM-kretsarna krypterar, förutsatt att de har sparat nycklarna[48]. Remote Attestation-protokoll så som Direct Anonymous Authentication kräver att en Privacy Certificate Authority har kännedom om EK[49]. Skillnaden mellan TPM-kretsarna och föreslagna Key Escrow-tjänster[50] ligger i att användare inte uppger sina nycklar till statliga myndigheter. I stället köper kunder hårdvara av företag som använder kryptonycklar som enbart företagen känner till. Om man tolkar Privacy Certificate Authorities som myndigheter så är TC-teknologi en instansiering av Key Escrowism.

Trusted Computing utgör inte ett problem mot upprättandet av en kryptoanarki förutsatt att det går att välja att inte använda TPM-kretsen. Om användare av datornätverk tvingas att använda TNC i kombination med TPM för att verifiera att de enbart använder mjukvara som på förhand auktoriserats för att kommunicera med andra noder på nätverket kan det bli svårt att införa en kryptoanarki. År 2002 föreslog den amerikanska senatorn Ernest Frederick Hollings att alla datorer skulle utrustas med skydd för att hindra människor från att olovligen sprida

[46] TCG Architecture Overview Version 1.4. Nåbar via `http://www.trustedcomputinggroup.org/files/resource_files/AC652DE1-1D09-3519-ADA026A0C05CFAC2/TCG_1_4_Architecture_Overview.pdf`

[47] TPM Main Specification Level 2 Version 1.2, Revision 103, Part 1, sidan 29. Nåbar via `http://www.trustedcomputinggroup.org/files/resource_files/ACD19914-1D09-3519-ADA64741A1A15795/mainP1DPrev103.zip`

[48] Privacy Certificate Authorities kan också ha signerat hashsummor av nycklarna. Det står dock ingenting om det i beskrivningen av Direct Anonymous Authentication-protokollet.

[49] Direct Anonymous Attestation, Ernie Brickell, Jan Camenisch och Liqun Chen från Intel Corporation, IBM Research, HP Laboratories. Nåbar via `http://eprint.iacr.org/2004/205.pdf`

[50] Pressmeddelande från Vita Huset, 1994-02-04, arkiverat av Electronic Privacy Information Center. `http://epic.org/crypto/clipper/white_house_statement_2_94.html`

upphovsrättsskyddat material[51]. Lagförslaget antogs dock inte. Kinas myndigheter skulle teoretiskt kunna kräva att enbart datorer med Green Dam Youth Escort[52] som verifierats av TPM-kretsen, eller en variant därav[53], får lov att användas på kinesiska nätverk. I teorin kan myndigheter med den här teknologin detaljstyra hur information får lov att kopieras mellan datorer[54]. Kritik har riktats mot TC av bland annat Richard Stallman[55] och Electronic Frontier Foundation[56].

3.3.3 Lagar

Det är idag inte olagligt att kommunicera meddelanden som auktoriteter inte kan avkoda i de flesta länder. Undantag finns i Kina och Frankrike. Så länge det inte är olagligt att kommunicera krypterade meddelanden över nätverk kan det vara svårt att illegalisera mjukvara som upprättar kryptoanarkier.

Om kollektiv bestraffning används kan användare, trots att det inte går att bevisa att de medverkat i brott, straffas för att de använder mjukvara som gör det möjligt för andra att begå brott. Det går dock att tillverka nätverksprotokoll som inte går att klassificera. Exempelvis kan UDP-protokollet[57] användas för att transportera oklassificerbar data om både käll- och destinationsport har slumpats av noderna, samt om all data som enkapsuleras av UDP-paketen är krypterat med på förhand kända nycklar. (UDP-protokollet definerar fyra 16-bitars fält i pakethuvudet: Källport, destinationsport, antal byte som enkapsuleras av UDP-paketet och en checksumma. Efter pakethuvudet följer data som enkapsulerats i protokollet.) På så sätt kan lagar som förbjuder användandet av protokoll undvikas eftersom det inte går att bevisa att ett illegalt protokoll har använts, förutsatt att ingen erkänner lagbrottet. Den data som har utväxlats kan lika gärna ha varit slumptal, vilket förmodligen inte är olagligt att sända till andra. Freenet använder den här tekniken sedan version 0.7 när det har konfigurerats i darknet-mode[58] Det går alltså att tillverka protokoll som går att använda trots att de är olagliga, så länge människor får lov att kryptera de meddelanden som skickas.

[51] Consumer Broadband and Digital Television Promotion Act, http://w2.eff.org/IP/SSSCA_CBDTPA/20020321_s2048_cbdtpa_bill.pdf

[52] Analysis of the Green Dam Censorware System, Scott Wolchok, Randy Yao, and J. Alex Halderman, The University of Michigan, Revision 2.41 – June 11, 2009. Nåbar via http://www.cse.umich.edu/~jhalderm/pub/gd/

[53] Kina har en egen standard för en annan säker kryptokrets som kallas för Hengzhi. Se http://en.ce.cn/Insight/200910/29/t20091029_20300465.shtml och http://english.people.com.cn/200504/12/eng20050412_180617.html.

[54] Det går alltid att kopiera bild och ljud genom att exempelvis fotografera skärmar eller använda microfoner.

[55] http://www.gnu.org/philosophy/can-you-trust.html

[56] http://www.eff.org/wp/trusted-computing-promise-and-risk

[57] User Datagram Protocol (UDP) defineras i RFC768. Se http://tools.ietf.org/html/rfc768

[58] Private Communication Through a Network of Trusted Connections: The Dark Freenet. Ian Clarke, Oskar Sandberg, Matthew Toseland, Vilhelm Verendel. Nåbar via http://freenetproject.org/papers/freenet-0.7.5-paper.pdf.

3.4 Slutsats

För att upprätta en kryptoanarki krävs det

1. Att det är möjligt att sända data som myndigheter inte kan tolka. (Kryptering är inte olaglig.)
2. Att individer kan bestämma vilka beräkningar som ska utföras av deras egna datorer. (Säkra kryptoprocessorer är inte obligatoriska.)
3. Att det finns ett kommunikationsmedium där en grupp individer kan utväxla meddelanden. (Nätneutralitet har viss betydelse.)
4. Att mjukvara som utnytjar punkterna ovan är tillgänglig.

Alla dessa punkter är uppfyllda. De första två punkterna går förmodligen inte att upphäva utan att införa någon form av diktatur. Den tredje punkten går förmodligen inte att upphäva utan att införa lagar som kräver att enbart mjukvara som auktoriteter på förhand godkänt används, genom att i en extrem form gå ifrån nätneutralitet eller genom att montera ner internet. Den fjärde och sista punkten går inte att hindra om den första punkten gäller.

Ett teoretiskt framtidscenario är att delar av internet kräver verifikation av vilken mjukvara datorer använder, med hjälp av säkra kryptoprocessorer, medan andra delar av internet inte kräver det. Det här scenariot är kanske mer sannolikt än att enbart ”info-anarki” eller ”info-diktatur” uppstår. I det här scenariot kan kryptoanarki finnas vid sidan av myndighets- och företagskontrollerade nätverk. I en sådan framtid kan det vara svårt att utan förlust kopiera viss information, samtidigt som det är svårt att hindra information som väl har befriats från kopieringsskydd att spridas. Praktiskt kan det kanske exempelvis innebära att nästan alla filmer som olovligen sprids är inspelade med videokameror.

Om det går att utväxla pengar utan att uppge sin identitet innebär det vidare att anarkokapitalism går att realisera. Lönnmordsmarknader går då att implementera i form av system som använder anonyma banker och betalningsmedel. Om det inte är önskvärt att pengar används på detta sätt är förmodligen det enda motmedlet att avskaffa möjligheten att använda anonyma, digitala betalningsmedel.

Det är ännu få noder i de anonymiserande nätverken och trafikmängderna är försvinnande små i jämförelse med internet i sin helhet. Cipherspace liknar på många sätt internet i dess barndom. Enskillda anslutningar mellan noder i nätverken har överföringshastigheter som ofta motsvaras av modem från 90-talet. Det kan därför dröja innan olika former av cipherspace diskuteras och används lika mycket som internet idag. Den effekt kryptoanarki har på samhället begränsas kanske mest av hur många som använder sig av tillståndet, och vad de använder kryptoanarki till.

Chapter 4

References

Bibliography